SECURING AIR TRAFFIC

Case CBRN Terrorism

Edited by Timo Hellenberg, Pekka Visuri and Lars Nicander

Assisted by Maarit Elo-Valente

Aleksanteri Institute
University of Helsinki
2011

With financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission - Directorate-General Home Affairs

Published by Aleksanteri Institute, University of Helsinki
Cover design by WSOY
Printed by WSOYpro Oy, Helsinki, March 2011
ISBN 978-952-10-6868-3 (nid.)
ISBN 978-952-10-6869-0 (PDF)

Contents

Contributors

Marina Andeva, PhD Candidate in Transborder Policies for Daily Life, MA in Communication and European Policy Making at the University of Trieste, Italy, BA in National and International Law at the University of Skopje, Macedonia. Junior Researcher at I.S.I.G. Research fields: cross-border cooperation, immigration, minorities and European policies.

Martti Annanmäki, M.Sc (Physics) acts as a consultant at STUK (Radiation and Nuclear Safety Authority, Finland). He is retired from STUK after a career of 36 years, during which he served in various positions the last one being the Quality Manager. His expertise, apart from quality related affairs, covers natural radioactivity. His publications include scientific and other articles mainly on natural radioactivity related topics. As a consultant he participates in various international service projects mainly funded by EU financing instruments (PHARE, TACIS etc.). Earlier experience in international projects covers e.g. projects in Latvia, Lithuania and Belorussia.

A.A. Cohen, L.L.B., Ph.D., is on the Board of Advisors of the Institute for Analysis of Global Security (IAGS). He is also a member of the Editorial Board of Central Asia and the Caucasus (Stockholm) and of Caspian Crossroads, and is a Member of the Council of Foreign Relations, the International Institute for Strategic Studies (London), and a number of other professional organizations. He advised Burson Marsteller, a pre-eminent public affairs firm, and a number of government agencies and private companies on a wide range of policy issues. Dr. Cohen earned his Ph.D. and M.A., Law and Diplomacy, from The Fletcher School of Law and Diplomacy at Tufts University. Dr. Cohen is a recognized and widely published authority on international security policy, on domestic and foreign policy, the rule of law, and crime and corruption in Europe, Eurasia, and the Middle East.

Emilio Cocco, PhD, is senior lecturer of Sociology of the Territory and the Environment at the University of Teramo since 2005; research fellow at the Department of Theories and Policies of Social Development. Several grants and fellowships 2003-2006, as well as research visits 2002-2006 in Croatia, the United Kingdom, Sweden and Finland. Research interests: social theory; border studies; nationalism, regionalism and territorial development; cross-border cooperation in maritime regions; urban studies; tourism, travelling and mobility.

Daniele Del Bianco, PhD, is a senior researcher at ISIG - Institute of International Sociology of Gorizia and lecturer in Sociology at the University of Trieste. His main fields of research and study are: border studies, cross-border cooperation and institutional and civil society cooperation in crisis management. His publications include ProAdrias – Protecting the Adriatic Seaways (2008) and Training Modules on cross-border and inter-territorial cooperation (2010) published by the Italian Prime Minister Office and the Council of Europe.

Timo Hellenberg, Dr. Pol. Sc., is a senior scientist with experience in intergovernmental cooperation for disaster reduction and emergency management. His many publications include "Challenging Disasters – Natural Disaster Reduction in the Context of Intergovernmental Relations" (Kikimora Publications, 2002). He is CEO of the Hellenberg International Ltd and holds a post of senior fellow at the Aleksanteri Institute of the University of Helsinki. In 2003 he served as a Special Advisor to the Prime Minister of Finland.

Pertti Jalasvirta is the Managing Director and owner of Jalasvirta Inc. Medical Croup and Suojasauma Ltd.; a Nordic based European manufacturing and medical supply and Service Company. He has thirty years of professional experience in government affairs, resource management, and administrative management, and planning and organizational development in military medicine, field hospital relations and CBRNE processes. He is also a highly decorated Medical Service Corps Reserve Warrant Officer and is currently responsible for the development and testing of new medical processes and emerging technologies for the Finnish Defence Forces.

Timo Lairio, Lieutenant colonel (retired). Depot Commander at safety depot 1995-2000, Staff commander at Engineer Regiment 2000-2005, CBRNE-sector director at Suomen Terästekniikka Oy 2006-2008, and CBRNE adviser at Jalasvirta Group Oy since 2009. Author of CBRNE Protection Guide, 2001; Complementary Guide: CBRNE Materials, 2002; and others. DVDs: CBRNE-Equipment from Finland, 2006; Light-weight CBRNE Reconnaissance and Extinction Vehicle, 2008; CBRNE Symposium's Outdoor Exhibition, 2009; Project Hangar, 2009; and Project Aether, 2010.

Jan Leijonhielm, Senior Intelligence Advisor at the Centre for Asymmetric Threat Studies (CATS), SNDC. Manager of Russian and Early Warning Studies at FOI (Swedish Defence Research Agency) since 1998. Earlier in Military Intelligence and Head of Economic Intelligence (at Stockholm East Economic Studies Institute) 1980-89. Author of several books and studies on Russian economy, raw materials, defence budgets and intelligence, especially early warning methods.

Lars Nicander is the Director for The Center for Asymmetric Threat Studies at the Swedish National Defence College. Between 1997 and 2002 he was appointed as Secretary of the Cabinet Working-Group on Defensive Information Operations. Mr. Nicander is a political scientist and has served in various positions within the Swedish national security environment. He is an elected member of the Institute of Strategic Studies in London (IISS) and a Fellow of The Royal Swedish Academy of War Sciences.

Magnus Normark, Senior Analyst for the Center for Asymmetric Threat Studies (CATS) at The Swedish National Defense College. His area of expertise is CBRN-terrorism and proliferation of weapons of mass destruction. Co-editor of "Unconventional Weapons and International Terrorism" published by Routledge in January 2009. Senior analyst and program manager at Swedish Defence Research Agency (FOI) on counter proliferation and CBRN threat assessments. Earlier experience includes 12 years as an analyst within the intelligence community on proliferation and WMD related issues.

Hannu Rantanen, Lic.Phil., is a Senior Research Scientist in Information Technology at the University of Kuopio, Finland. He has more than 20 years' experience in the safety and security field and is currently employed by the Emergency Services College, where he is involved in research activities dealing with complex emergencies. His main areas of expertise are the use of information technology in emergency response and large scale international emergencies.

Heikki Silvennoinen, Engineer in Industrial Management and Economy. His area of expertise is fixed and portable CBRNE detection devices, decontamination processes and emergency management. His earlier experience includes 16 years of international CBRNE trade and technical specialist tasks. He has participated in several CBRNE and defence related R&D projects. He has engaged in studies at the School of Business and Economics, University of Jyväskylä.

Mikko Valkonen, Dr. Nucl. Phys. is project consultant at Finnish Radiation and Nuclear Safety Authority, STUK. He is a retired Senior Adviser of Corporate Security at Teollisuuden Voima Oyj (TVO), and is Special Teacher on Corporate Security at Aalto University TKK since year 1997. His key qualifications include security and emergency preparedness of nuclear power plants and corporate security. His international co-operation consist of audit in Armenian Nuclear Power Plants for IAEA and several meetings and seminars in Sweden, Germany, Denmark, Norway, Canada and USA etc. He has published on Nuclear Physics and several Finnish security papers.

Pekka Visuri, Dr. Pol. Sc. is project researcher at the Aleksanteri Institute. He is a retired Army colonel, worked 15 years as researcher at the Finnish Institute of International Affairs in Helsinki, and as adjunct professor at the National Defence University in Helsinki, specialized in security policy and strategy. His publications include Suomi kylmässä sodassa (Finland in the Cold War. Helsinki: Otava, 2006), Suomi ja kriisit (co-editor with Tuomas Forsberg et al, Engl. Finland and Crises, Helsinki: Gaudeamus, 2003) and Maailman muutos ja Suomi (Engl. Change of the World and Finland, Helsinki: WSOY, Docendo, 2011).

Preface

On a Finnair Airbus 340 passenger flight from Hong Kong to Helsinki, the idea for a new type of threat scenario first started to emerge in my mind. From the beginning, it was clear that a multidimensional project like this would have to involve both the owners and operators of the European critical infrastructures, governmental institutions, supported with extensive multi-disciplinary studies on emerging new threats of chemical, biological, radiological or nuclear materials. At the time, our multinational team of experts was concluding a similar type of project, P*oseidon – Preventing Terrorism in the Baltic Sea Region*, which was introduced as a successful best practice model at the Council of the European Union, Working Party on Terrorism, in Brussels on 15th April 2009.

This collection of articles is based on *Project Aether – Air Passenger Transport Security in Case of CBRN Terrorism*. It lasted two years, 2009-2011, and it was generously financed by the European Commission Directorate-General Home Affairs. We owe special gratitude to the Commission for its profound support and practical cooperation, which made possible this two-year-long project between several partners from different national backgrounds. The project was conducted in Hong Kong (SAR), Europe and the United States. It involved 18 project and advisory partners and dozens of government representatives from Finland, Germany, Hong Kong (SAR), Italy, Sweden and the United States.

The objective of the project and this report has been to investigate situational awareness and decision making at the national and European Union level in the case of a complex CBRN (chemical, biological, radiological and nuclear) threat-related crisis situation on board an airplane. The project also sought to identify prevention capacity and to develop solutions against threatening use of CBRN material. The aims have been achieved through a scientific analysis and simulation of an open-ended scenario with several development lines.

The Aether scenario is based on illegal and threatening trafficking and use of chemical, biological, radiological or nuclear (CBRN) materials by extremists. The scenario is scheduled to take place on a passenger flight from Hong Kong to Helsinki. The case includes terrorism with the demonstrative use of CBRN material and potential for a wider escalation of the crisis. The plane Airbus 340 carries together circa 300 passengers and aircrew of several nationalities. The triggering moment of the scenario takes place when the passengers start to have mounting health problems in the Russian airspace. The crew informs Finnair and the Finnish air control of the problems on board.

Once the plane is landed at the Helsinki Airport, the evacuation operation takes place and a field hospital is prepared to take care of the victims. The Finnish Government, as well as the EU level, are notified and have meetings immediately. The first goal – besides the medical emergency measures - is to find out whether a terrorist strike has taken place, who is responsible for committing the act, and if there are any other similar kinds of strikes planned

to happen soon. Press will immediately catch the alarm and the news is all over the internet very soon. Speculations follow about the reason and cause of contamination as some signs are showing that also other similar attempts may be done in the short run against the Nordic countries and other EU member states. This requires a general alert of the EU network of intelligence and counter-terrorism activities. A basic hypothesis in the case Aether is that the potential terrorists have also new unknown means of delivering dangerous material into the airplane, enough for a disastrous attack against such an important strategic target.

CBRN terrorism as a threat causing risks for societies has been studied widely. Previously it has also been studied from the point of view of total national defence. Today's counter-terrorism may anyhow be looked at also through blurring the line between the non-military and military crisis management. This is accentuated by the fact that counter-terrorism encompasses different parts of the EU system and cannot be reduced to any one pillar's responsibility. This collection of articles aims to address that issue from the intergovernmental relations perspective and it tries to give impetus for further study on decision-making processes within the EU.

The project Aether was launched in May 2009 and was led by the Aleksanteri Institute of the University of Helsinki. Other contributing research partners included the Centre for Asymmetric Threat Studies of the Swedish National Defence College, the Emergency Services College of Finland, Finnair Plc, the Institute for the Analysis of Global Security in the USA, the Institute for International Sociology of Gorizia in Italy, Jalasvirta Group, and the Radiation and Nuclear Safety Authority in Finland. The project advisory partners included Cassidian (former EADS Secure Networks Oyj), Elisa Corporation, Environics, the Finnish Air Rescue Society, the Finnish Meteorological Institute, the Finnish Ministry of Defence, the Finnish Ministry of the Interior, the Prime Minister´s Office of Finland, the National Defence Training Association of Finland, and SAAB Ab. The project was also supported by the Finnish Ministry for Foreign Affairs.

The project has benefited from being part of a larger network, the CIVPRO Civil Protection Network. This network, which made the project possible in the first place, has also contributed to the current study by facilitating cooperation with and learning process from a wide range of other related projects. Within the project we organised numerous working group meetings and three research workshops in Helsinki, Stockholm and Hong Kong. For networking and dissemination we organised two major conferences, *Air Passenger Transport Safety in Case of CBRN Terrorism*, on 19-20 May 2011 at the Central Plaza in Hong Kong, and *Transport Security, Case CBRN Terrorism*, on 9 February 2011 at the European Parliament in Brussels. Both conferences were attended by ca. 80 participants including several guests from governmental agencies, the European Parliament and the EU Member States. The conference receptions were sponsored by the European Parliament and the European Commission.

In a multinational and cross-continental project like this there are many people to acknowledge, who were generous with their time, professional advice and personal commitment. Here are just a few of them:
Ismo Aaltonen, Juan Luis Flores Arroyuelo, Ole Arrhenius, John Cameron, Myriam Van Campenhout, Maria Castillo Fernandez, Debbie Chang, Sidney F.C. Chau, Ivy Cheng, Tapani Ehrling, Johnny Engell-Hansen, Alberto Gasparini, Herve Guillou, Karin Hannukainen, Hans Holmberg, Anneli Jäätteenmäki, Kaarlo Karvonen, Markku Kivinen, Axel Leicht, Terence Leung, Kent Liu, Jukka Metso, Lars Nicander, Piia Nikula, Antti Nissinen, Risto Ojanperä, Marja Pellosniemi, Christer Pursiainen, Timo Rajakangas, Magnus Ranstorp, Pertti Salminen, Anna Salonsalmi, Vilja Savisaar-Toomast, Marja Rislakki, Glenn E Schweitzer, Tapio Tourula, Joseph Tung, Pekka Tuunanen, Ritva Viljanen, Jan Wiberg, Jolly Wong, Tony Wong Chi-hung, Kent Yau, the US Embassy in Helsinki and the EU Situation Centre in Brussels.

Our special thanks go to Dick Heimans, Head of Counterterrorism at the DG Home Affairs, for his personal support, commitment and professional guidance along the way of this project. I would also like to thank especially Timo Rajakangas, former Consul General of Finland to Hong Kong for his generous support and trust for our initiative and cause. Needless to say that without the support of two gentlemen at the Prime Minister´s Office of Finland, Timo Härkönen, Director of Government Security, and Risto Volanen, former State Secretary, this project and its profound exercises in October 2010 would not have been possible. Aapo Cederberg, Secretary General of the Security and Defence Committee of Finland, has always been there when needed and has faced all administrative challenges.

Thanks also go to Pekka Eskola, Tommi Niemi and Anne-Marie Turpeinen from the European Parliament for supporting the final conference at the Parliament with their multiple skills.

Any successful project, particularly one including several organisational layers and partners with different cultures need strong administrative and financial management. Without the professional project coordination by Maarit Elo-Valente and financial expertise of Marja Riikonen from the Aleksanteri Institute, this task would have been much more difficult to achieve, if not impossible. My friend and collegue Pekka Visuri has made this project possible and led the whole process of scenario building, not to mention the support with project leadership.

Finally, the editors want to make it clear that all possible mistakes and misunderstandings, as well as interpretations, arguments, conclusions and policy recommendations contained herein remain the sole responsibility of the authors of the respective individual chapters. The editors and the Commission are not responsible for any use of the information and analysis contained herein.

I wish that this publication would give an impetus to intra-organisational, cross-sectoral and transnational evolution in the field of CBRN terrorism-related threat assessment and capacity building in the participating countries and organisations.

The Project Aether has been a rewarding and challenging pathway, sometimes above our imagination. As an ancient Greek saying puts it: "Aether is the material that fills the region of the *Universe* above the *terrestrial sphere*".

Dr Timo Hellenberg
Helsinki, February 18th, 2011

Timo Hellenberg & Pekka Visuri: Overview of the European Union Crisis Coordination Arrangements - Securing Air Passenger Transports Against CBRN Terrorism

Prelude

On Christmas Day 2009 a passenger flight from Amsterdam to Detroit, carrying 278 passengers, turned out to be a wakeup call for aviation safety officials in the United States and elsewhere. The extreme act by a young Nigerian to serve as a firebomb 20 minutes before landing created a test case both to the plane cabin crew and the passengers on board. This Detroit case returned the US homeland security and safety authorities to the pre 9/11 thinking in their preparedness and planning. This case could be regarded as a cardinal mistake both by the Schiphol airport authority and by the multiply intelligence services. The situational awareness which was supposed to be created from various sources was not allocated and shared based on all the latest artistic and strategic plans. It is easy to agree with Sidney Chau, Executive Director of the Aviation Security Company (AVSECO) in Hong Kong that a number of questions have been raised subsequent to this case.[1] Why was the intelligence received by law enforcement agencies on Abdulmutallab not properly acted upon? Why was he not efficiently profiled at his originating and transit airports? Why were neither the PETN explosive nor the liquid chemicals not detected by security screening? And, as Mr Chau has asked, why did Abdulmutallab choose these specific routes and airports to enable him to carry out his plan?[2]

Risks and threats such as the one above affect modern societies both in terms of vertical and horizontal parallels, and they have become that way increasingly international and intertwined. At the same time our risk architecture, both in terms of technology, administration and policy has not much changed over the years. It wasn't until the terrorist bombings in the U.S., in London and in Madrid in 2004 that the vulnerability of infrastructures against terrorism became top priority in European context. It was realized that the risk of terrorist attacks can never be reduced to zero but can be minimized with a common action. This reinforced EU's exploration for concerted action in countering terrorism.

Security has been a matter of concern for civil aviation for several decades, but in particular since the bombing of a flight above Lockerbie in 1988. However, aviation security per se, has up until more recently, been addressed on essentially at a national level and often within the domestic security and safety operators, such as the Aviation Safety Administration, the Border Control and the Police/Rescue Services. At the international level, though for some time Standards and Recommended Practices have been laid down by the International Civil Aviation Organisation (ICAO) for States to implement, these are not regulated by a binding mechanism to guarantee their full and proper application.

1) Chau, Sidney; Speech at the Aether Conference in May 2010 in Hong Kong.

2) Chau, Sidney; A Personal View, AviationSecurity International, Feb 2010, pp 64.

There exists a lot of research on European Union policy-making, power struggles between various bodies and crisis management in its traditional sense related to military crisis[3]. Yet, there exists not so much analysis or investigation of EU crisis management performance related to new security threats, which may cause transnational emergencies affecting the whole Union[4].

Methodology and Aims

In a multinational research project such as this one, one of the basic challenges is how to harmonize and synchronize the concepts used and overall terminology among partners with different national, organisational and operational cultures, particularly in the field of studies which is not mature per se in terms of multidisciplinary methodologies. There exists an international mainstream understanding about the tools and vocabulary when it comes to studies on civil protection and emergency management as well as terrorism per se. The same stems with the aviation safety and various standards of aviation and airport security. Furthermore, the aviation specialists seem to make a distinction between aviation safety, which concerns standards and rules for the construction and use of aircraft, and aviation security, which is aimed at the prevention of acts of unlawful interference against civil aviation, such as seizure of an aircraft or placing on an aircraft a hazardous device.

When one conducts a study on CBRN terrorism in case of aviation and passenger transport, there is a thin line between success and conceptual minefield. In this study however, we look into both the safety and security issues. We follow the definition of the recently published Inventory of Crisis Management capacities in the European Commission and Community Agencies (July 2009). It describes the scope of *aviation security* as establishing common rules to protect civil aviation against acts of unlawful interference that jeopardise the security of civil aviation and the scope of *aviation safety* as establishing a uniformly high level of civil aviation safety in Europe by achieving harmony between air safety standards.[5]

The aviation security rules inside the EU are based on standards contained in International Civil Aviation Organisation (ICAO) rules and on the security measures laid down by the European Civil Aviation Conference (ECAC). In order to face possible terrorist strikes, EU security rules for instance establish a list of prohibited articles to be carried into the security restricted area and the cabin of an aircraft.[6]

The European Aviation Safety Agency which was established in 2002 is the central agency dealing with the EU´s strategy for aviation safety. It provides Commission opinions on suitable technical standards, ensures the implementation of safety legislation via inspections and provides certificates of airworthiness for new aircraft of component design.[7]

3) E.g. Richardson (ed.) 2006, Kervinen 2001, Ryter 2002.

4) Good examples of this perspective can be found e.g. in Boin, Ekengren, Rhinard 2006 and Larsson, Olsson, Ramberg 2005.

5) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 19.

6) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 20

7) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 20

The aim of this article is to look at the latest developments of the EU crisis coordination and decision-making arrangements in a terrorism related crisis. It also looks briefly at the development of the EU's counter-terrorism action plan into counter-terrorism strategy and its mechanisms and concentrates on the functioning of the EU emergency and crisis coordination arrangements and the problems they may contain. In addition to that, we are analyzing how the EU crisis coordination and the decision-making would be done in relation to a fictive aviation terrorism case. Consequently, the research questions are formed as the following:

- How do the EU emergency and crisis coordination arrangements (CCA) work in a terrorism related crisis? I.e. how do the EU institutions, affected Member States and presidency interact in a crisis mode?

- How would the CCA work in a fictive case of air passenger transport terrorism, i.e. in an Aether type scenario?

After the Project Aether scenario dissection and analysis we try to look at the advantages and problems that follow from the concerted action in a complex terrorism scenario, and conclude our thoughts of the complex issue to recommendations on EU counter-terrorism and emergency management when facing asymmetric threats.

Methodologically this article is based on studies of intergovernmental relations in the context of EU crisis coordination and decision-making on the EU emergency and crisis co-ordination arrangements (CCA). We have also used relevant EU websites and the EU-documentation and taken advantage of the expert meetings with the representatives of the Situation Centre of Prime Minister's Offices in Finland, the Security Bureau of the Hong Kong Government, the Hong Kong Police Situation and Monitoring Centre and the European Union Situation Centre (SitCen) in Brussels.

1. General Overview of European Crisis Management Systems

In its inventory of its crisis management capacities, the Commission has stated its purpose to be in terms of counterterrorism to enhance the EU capacity to prevent acts of terrorism and to make Europe safer, while respecting human rights and allowing its citizens to live in an area of freedom, security and justice. This is aimed to be reached by strengthening national capabilities through the exchange of best practices and financial support, by facilitating European cooperation in the field of counter-terrorism, and by developing collective capabilities.[8]

In terms of overall counter-terrorism, the Commission addresses the whole cycle of actions, i.e. social, technological and economic, that favours the spreading of terrorism. On the social side support is provided for the analysis of root causes leading to violent radicalization (incl. the ideology and narrative of violent extremism). On the technological aspect, the main focus seems to be on the use of the Internet. On the economic aspect the focus is on the financial system for terrorist purposes. In terms of explosives, the EU Action Plan on Enhancing the Security of Explosives has been launched comprising an EU-wide early warning system (EWS), a

8) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 29

European Explosive Ordnance Disposal units network (EEODN), a European Bomb Data System, a Network on Detection of Explosives (NED), and the Standing Committee on Precursors. For border security, the Community Risk Management System – Risk Information Form (CRMS – RIF) support the exchange of information which would be valuable in the Aether type of scenario.[9]

First loose intergovernmental cooperation framework in Europe against terrorism Trevi Group (Terrorisme, radicalisme et violence internationale) was set up already in 1975 and consisted of the meeting of Ministers of Home Affairs. In 1999 the mentality of looking at internal security matters from a common point of view increased with the *Treaty of Amsterdam* when the "area of freedom, security and justice" was created. However, it wasn't until the attacks of 9/11 in the U.S. in 2001 that formed a culmination point for the EU's take on terrorism. The need to develop a more substantial and stronger common response emerged and at the same time presented also an opportunity for the EU to gain more credibility in its counter-terrorism actions[10]. This however was not sufficient, since Europe had to encounter the Madrid attacks in March 2004 and London attacks in July 2005. If not before, it was clear now that terrorism is a constant threat also in the European soils which has further emphasized the necessity to go on with the work of enforcing the EU-CT.

EU-CT is a peculiar policy where the aim is to enhance common action with the core issues of security and safety but where the powers and capabilities are still kept within the authority of the nation states. Despite of this, the EU-CT is nowadays becoming more and more comprehensive and thorough, whereas in the 9/11 aftermath the EU addressed terrorism more broadly; as a general and global threat to open and democratic societies[11]. The emphasis was on the solidarity and working in a global coalition under United Nations aegis. The fight against terrorism was said to become more than ever, a priority objective of the European Union and as a proof, various issues such as enhancing police and judicial cooperation, developing international legal instruments, tracking and ending the funding of terrorism, strengthening air security and coordinating the EU's global action were raised in the plan of action which brought the CT to a more concrete and pragmatic level. The General Affairs Council has assumed the role of coordination and reporting of the fight against terrorism between all Union's policies whereas the integration of the fight against terrorism further to the Common Foreign and Security Policy (CFSP) was mentioned only briefly.

The *European Union Counter-Terrorism Strategy*[12] extends nowadays into four principal areas which are *prevention, protection, pursuit,* and *response*. Prevention aims at rooting up terrorism by conducting extremism, combating radicalization and recruitment into terrorism. The EU focuses on promoting good governance, human rights, democracy, education and economic prosperity in order to counter the conditions in society which may lead into radicalism.[13] *Protection* in the CT Strategy comes close to the policy of the CIP (critical infrastructure

9) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 30

10) Monar Jörg (2007): Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and its Problems. Government and Opposition, Vol. 42, No. 3, pp. 292-313.

11) Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001.

12) Council of the European Union: The European Union Counter-Terrorism Strategy. Justice and Home Affairs Council meeting, Brussels 1 December 2005.

13) This type of policy can be included in the Early Warning policies and action which are not dealt per se in this article.

protection)[14]. The aim is to strengthen the defences of key targets i.e. vital infrastructures such as border and transport security; airports, aircrafts and seaports by reducing their vulnerability to impacts of any attack. The CIP policy is based on the all-hazards approach which takes into account both natural and man-made disasters. *Pursuit* aims at impeding terrorists' planning, networking and funding as well as bringing them to justice. Within important tools is the *European Arrest Warrant* as well as creation of *Joint Investigation Teams* to enhance systematic police cooperation and cross-border investigations.[15] *Response* builds on the capacity to deal with any attacks at the moment they occur. The fact that the terrorist strikes may have cross-border effects is well recognized, and the existing structures of *Civil Protection Mechanism* as well as the *Crisis Coordination Arrangements* were precisely developed to respond to cross-border as well as to international crises.

The EU directives and regulations concerning air transport

LEGAL BASIS

- **Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.**
- **Regulation (EC) No 300/2008 of 11 March 2008 on common rules in the field of civil aviation security, repealing Regulation (EC) No 2320/2002.**
- **Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008.**
- **Regulation (EC) No 1217/2003 of 4 July 2003 laying down common specifications for national civil aviation security quality control programmes.**
- **Regulation (EC) No 1486/2003 of 22 August 2003 laying down procedures for conducting Commission inspections in the field of civil aviation security.**
- **Regulation (EC) No 1138/2004 of 21 June 2004 establishing a common definition of critical parts of security restricted areas at airports.**
- **Regulation (EC) No 820/2008 of 8 August 2008 laying down measures for the implementation of the common basic standards on aviation security, repealing Regulation (EC) 622/2003.**
- **Regulation (EC) No 1592/2002 of 15 July 2002 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency.**
- **Regulation (EC) No 2111/2005 of 14 December 2005 on the establishment of a list of air carriers subject to an operating ban within the Community and on informing air transport passengers of the identity of the operating air carrier, and repealing Article 9 of Directive 2004/36/EC.**

The list of directives and regulations for the legal basis of EU capacity in the field of Air Transport. Source: Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009.

Counterterrorism

The four principal areas covering terrorism and counter-terrorism reach under several domains and bodies in the *EU since there is a general understanding within the EU that countering terrorism requires a comprehensi*ve approach.[16] This is argued to enable to link different policy areas together and enhance interaction of measures at the member state, the EU and the international level. The reality, however, consists of several bodies with complex and sometimes

14) To read more on EPCIP, European Programme for critical infrastructure protection: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm

15) Pursuit can also be viewed as part of the early warning actions.

16) EU's approach is in agreement with the UN's global strategy to counter terrorism as well as with the OSCE's strategy in combating terrorism by linking the politico-military, human and economic dimensions.

overlapping linkages which make it a somewhat challenging task to describe the current EU measures and bodies dealing with the counter-terrorism. This is however our aim, and in the following we are looking closer at the EU legislation, bodies and mechanisms that have influenced considerably and still have a key role in the current EU counter-terrorism activities.

LEGAL BASIS

- **Framework Decision (2002/475/JHA) on combating terrorism.**
- **COM(2004)689 on Prevention, preparedness and response to terrorist attacks.**
- **December 2005: European Union Counter-Terrorism Strategy.**
- **EU Action Plan on Terrorism.**
- **COM(2004)700 on the Prevention of and Fight against Terrorist Financing.**
- **COM(2005)329 on measures to ensure greater security in explosives, detonators, bomb-making equipment and fire-arms.**
- **COM(2005)313 on Terrorist recruitment: addressing the factors contributing to violent radicalization.**
- **COM (2005)620 The prevention of and fight against terrorist financing though enhanced national level coordination and greater transparency of the non-profit sector Directive 2005/60/EC on the prevention of the use of the financial system (3rd AML/CTF Directive).**
- **EU Action Plan on Enhancing the Security of Explosives (adopted by the JHA Council in April 2008).**
- **Council Decision (2008/633/JHA) concerning access for consultation of the Visa Information System (VIS) by MEMBER STATES and by Europol for the purpose of the prevention, detection and investigation of terrorist offences.**
- **Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds.**
- **Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community.**
- **Directive 2007/64/EC on payment services in the internal market.**
- **Regulation (EC) 2580/2001 freezing funds of suspected terrorists, and Regulation (EC) 881/2002 implementing UN Al Qai'da and Taliban sanctions.**
- **Regulation 622/2003 on aviation security including restriRegulation (EC) No 648/2005 (Community Customs Code)**

Legal basis of EU capacity in the field of Counterterrorism. Source: Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009.

✓ *1.1 Analytical Framework*

The definition of crisis and other emergency situations could be generally expressed as follows: Crisis is an unexpected situation where important national values and assets are at stake either domestically or internationally, with time pressure and uncertainty prevailing.

An emergency situation can be managed with usual measures without special crisis management arrangements, but the same system of alarm and decision making should be used as a basis for preparedness.

It can be difficult to define exactly an emergency situation or the nature of a crisis in the first phase. Still it is essential to start measures without hesitation if there are signs which hint to a crisis potential or escalation in the threat situation. Therefore, the estimation of the risks on the basis of an adequate situational awareness is one of the most important duties in the crisis management.

Crisis management (CM) means actions

- Before: research, training and planning.
- During: decision making, planning, leadership, cooperation, information.
- After: evaluation, learning, encouraging.

National CM arrangements should be available for citizens, territory, property and interests. In a **comparative study of national CM systems in Europe** we have used following "ideal types" or "polar types" as analytical means for description of the structures and functions:[17]

- Centralized – decentralized
- Integrated – specialized
- Institutionalized – ad hoc
- Political (mandate) – professional
- Public – private
- Administrative – technological
- Comprehensive – civil/military
- Information open – segmented
- Progressive – reactive

The national CM systems can be placed on each axis, and they could there be assessed in relation to the opposite ends, for example between the poles "private – public". A national CM system can be named e.g.: "Very centralized, integrated, institutionalized, professional, balanced public and private, emphasizing technology, using comprehensive CM approach and having a very open information policy."

✓ *1.2 Trends*

Along this study we found following **general trends** in the development of national crisis management systems in Europe:

- After the Cold War a clear emphasis on the preparation for the prevention and response to peace-time disasters and terrorism.
- Trend towards all-hazards principle in CM.
- More centralization and integration of CM leadership and coordination for civil-military cooperation.
- More centralized surveillance and building of the situation picture, but borderlines between the sectors of administration still exist as hindrance.
- In many EU countries the CM systems have been fundamentally modernized during the last years.
- Emerging trend to standardize CM structures and practices, but the process is slow advancing.

It has been concluded also in some other comparative studies that crisis management systems (i.e. preparedness for disasters and other crisis situations which are threatening the state, society or citizens) have been developed on the basis of national historic experience and applied according to the national characters of each country's political system, changes in threat perceptions and as reaction to the latest experiences in dramatic crisis situations. They are not so much results of theoretical consideration and scientific studies or concluded from

17) A comparative study on crisis management systems in Europe by Timo Hellenberg and Pekka Visuri. Working paper in the Aleksanteri Institute, University of Helsinki, October 2009.

the experience of other countries.[18] That is why the CM systems also in European countries differ remarkably and it is difficult to shape standard structures, procedures and communication rules for crisis management duties. The decisions concerning the development of the crisis management are usually made as a compromise derived from practical experience and political processes. Therefore, the systems are often technologically and operationally outmoded, too. Many noticed malfunctions in the system can be ignored or are covered only by placebo measures in order to mind additional work or political and bureaucratic struggles.

After the Cold War the differences between internal and external threats have faded, as well as the strict dichotomy between peace-time and war-time threat scenarios has been smoothed. The preparedness systems in the EU countries which were aimed only to war situations have vanished, or they have been changed to be used for countering peace-time disasters or other kind of catastrophes. Though, the natural and man-made disasters, on the one hand, and the crisis situations followed from terrorism or other violence, on the other hand, are rather different by nature, the present preparedness systems are more suitable to handle different situations on the same basis, i.e. on the so called "all hazards" principle. This has some practical difficulties, but they can be minimized with good training of the leadership as well as by standardized communications and logistics. It needs, however, further academic studies and exercises.

2. EU System and Legislative Framework in Countering Terrorism

The legislative framework plays a decisive role in combating terrorism. It is the most efficient way to urge the member states to implement the legislative measures created by the Union. However, the legislation and other official documents such as declarations or action plans only set the premises for action, they don't implement and solve the problems as such. They also all too often only follow the drastic events. This is the same with the EU's take on terrorism.

Terrorism was raised in the EU agenda already in 1999[19] but the real culmination point for the EU's take on terrorism were the terrorist attacks in the United States on 11 September 2001 when commercial aircraft were used as weapons of mass destruction. Anti-terrorism Action Plan[20] took place immediately in September 2001 as an immediate reaction to the terrorist attacks, and has been extended several times since. It addressed the issues of enhancing police and judicial cooperation, ending the funding of terrorism, developing international legal instruments, strengthening air security as well coordinating the EU's global action.

After the 9/11, the EU has adopted its first common rules on aviation security in 2002, with detailed provisions on access to sensitive areas or airports, aircraft security, passenger screening and baggage handling, control of cargo and mail, staff screening and training, and

18) See also FEMA 2009: Comparative Emergency Management Book. In internet: http://training.fema.gov/emiweb/edu/CompEmMgmtBookProject.asp

19) See Tampere European Council 15-16 October 1999, Presidency Conclusions

20) Decided by the Extraordinary European Council Meeting on 21 September 2001. Updated and revised many times since. The latest Action Plan on Terrorism dates to 10/5/2005. Note also the Action Plan on Radicalisation and Recruitment (December 2005).

items prohibited on board planes or in airports. Before 2002, each Member State had its own rules for aviation security.

This initiative led to the adoption of framework Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security and thus provided the basis for allowing harmonisation of aviation security rules across the European Union with binding effect. This regulatory framework has since been overhauled by a new framework, in full effect from 29 April 2010, as laid down by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.[21]

Regulation 300/2008 on aviation security and its implementing measures put in place a series of measures to improve, streamline and simplify existing procedures. For example by:

- Eliminating duplication of security controls. For example, reducing costly duplication of checks in strictly controlled areas of EU airports, where ther has already been effective screening for access. This is of significant operational benefit for airlines and airports.
- Simplifying procedures. For example, by establishing a single set of standards for the documents you need to get access at airports. The new rules clarify which kinds of identification and authorisations are necessary for access to different restricted areas. This clarifies the situation for authorities making it easier for them to operate the system.
- Harmonising procedures. For example, introducing EU-wide procedures for the recognition of hauliers transporting air cargo consignments. These can be recognised and used by hauliers in all Member States – this reduces restrictions for hauliers and the need for costly re-screening of cargo.
- Introducing common minimum standards as regards security training for all staff that implement security controls.[22]

In 2002 the Council adopted the Framework Decision on Combating Terrorism (13 June 2002)[23] which represents the legislative basis of the counter-terrorism policy in the EU. The Framework Decision forms a common legal framework to all member states by aligning their

21) http://ec.europa.eu/transport/air/security/security_en.htm, 31.5.2010

22) The EU framework allows for the recognition of equivalence of security measures of third countries, which can open the door to the establishment of one-stop security arrangements between the EU and non-EU countries. One benefit of such a one-stop security system is that passengers arriving at EU airports and transferring to other destinations would no longer need to be re-screened, thus allowing for faster connection times, lower costs and greater convenience for travellers.
By 29 April 2013 at the latest, all liquids will be allowed in cabin baggage and will be screened. By that date, the current restrictions on the carriage of liquids in cabin baggage will end. The transition period until 2013 is necessary to allow for a roll-out of liquids screening equipment at all EU airports.
As a preliminary step in phasing out the restrictions on liquids, as from 29 April 2011 at the latest, duty-free liquids purchased at third country airports or on board third country airlines and carried in tamper evident bags will be allowed as cabin baggage and will be screened. Today, these liquids are only allowed in cabin baggage if they come from selected third countries (United States, Canada, Singapore and Croatia).

23) Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

legislation and setting out minimum rules on terrorist offences. It therefore provided the first common definition of a terrorist offence and offences relating to a terrorist group or linked to terrorist activities. Consequently the Framework Decision laid down the penalties member states must incorporate in their national legislation for terrorist offences, or for inciting, aiding or abetting and attempting to them, in the Union. By adopting the common definition of terrorism the aim was to help further deepen the cooperation in countering terrorism.

Terrorist offences are defined in the Council Framework Decision[24] in the following way:

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:

- *seriously intimidating a population, or*
- *unduly compelling a Government or international organisation to perform or abstain from performing any act, or*
- *seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation shall be deemed to be terrorist offences:*

(a) attacks upon a person's life which may cause death;
(b) attacks upon the physical integrity of a person;
(c) kidnapping or hostage taking;
(d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
(e) seizure of aircraft, ships or other means of public or goods transport;
(f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
(g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
(i) threatening to commit any of the acts listed in (a) to (h).

European Security Strategy (ESS) was adopted in December 2003 and was the first of its kind. It identified threats facing the EU, defined its strategic objectives and set out the political implications for Europe. The emphasis was on common and concerted action when dealing with the complex problems and interdependence of vital infrastructures. Terrorism was mentioned as the first of the key threats, and seen as a "growing strategic threat to the whole of Europe" as well as "phenomenon part or our own society". It therefore makes a clear statement of the necessity of dealing terrorism with its root causes and of connecting it to the security policy of the Union. To be able to counter terrorism a mixture of instruments, e.g. intelligence, police,

24) Article 1 - Terrorist offences and fundamental rights and principles.

judicial and military is required. The challenge, acknowledged also in the ESS is how to better co-ordinate the external action with the Justice and Home Affairs (JHA) policies. For a wider cooperation, the ESS underlines multilateral cooperation and partnerships.

In the wake of the Madrid bombings, in March 2004, *Declaration on Combating Terrorism*[25] was adopted which contained also the *Declaration on Solidarity against terrorism* i.e. the Solidarity Clause. This is one of the corner stones in the decision-making in the case of terrorism since it calls for mutual assistance in terror attacks and states that "Terrorism will only be defeated by solidarity and collective action." EU declared its solidarity to the United States already in the 9/11 aftermath and called for the broadest possible global coalition against terrorism under the United Nations aegis[26] but this time the solidarity was taken to a new level between member states as a real commitment to act in solidarity towards any affected state. It gave the EU an instrument to demonstrate general political support and speak with a common voice when facing terrorism.

The Solidarity Clause is also included in the prevailing basic treaty on the European Union i.e. the *Treaty of Lisbon*[27]. According to it the Union and its member and the acceding states shall act jointly in a spirit of solidarity if one of them is the victim of a terrorist attack or the victim of a natural or man-made disaster. The approach is now widened to the all-hazards approach when it initially only concerned terrorism. The Solidarity Clause in the Lisbon Treaty is the following:

1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilize all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) prevent the terrorist threat in the territory of the Member States; protect democratic institutions and the civilian population from any terrorist attack; assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

The establishment of the position of Counter-Terrorism Co-ordinator was agreed in the Declaration on Combating Terrorism, 25 March 2004. In addition of maintaining an overview of the EU-CT instruments, the task is to co-ordinate counter-terrorism work between the Council and Commission. Also the *Hague Programme*[28] underlined that member states should not confine their activities in preventing and combating terrorism solely to maintain their own security but focus also on the security of the Union as a whole.

25) 25 March 2004, 7906/04.

26) SN 140/01, Conclusions and Plan of Action of the Extraordinary European Council meeting on 21 September 2001.

27) The solidarity clause is included in the Lisbon Treaty. 2007/C 306/01 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 'TITLE VII SOLIDARITY CLAUSE Article 188 R.

28) The Hague Programme: strengthening freedom, security and justice in the European Union, 13 December 2004, 16054/04.

The London bombings in 2005 added urgency to the development of the EU counter-terrorism policy and the *European Union Counter-Terrorism Strategy*[29] was drafted later that year. The Strategy has been updated regularly and forms the principles for the overall European policy in the fight against terrorism. Counter-Terrorism Strategy is overseen politically by the European Council, Commission and European Parliament. Each EU Presidency holds a meeting on it in order to ensure the inter-institutional governance, and the process itself is monitored by the *COREPER* (Committee of Permanent Representatives) with regular follow-ups and updates by the Counter-Terrorism Co-ordinator and the Commission.[30] However EU-CT is also accused of lacking legitimacy since there are no real checks and balances in the EU-CT legislative consultative process. European Parliament needs only to be consulted but does not have any co-decision powers on the relevant legislation concerning police and judicial cooperation. Another body that could exercise control over the results of collective EU-level decision-making is the European Court of Justice but its jurisdiction remains limited due to restrictions made by several member states.[31]

In November 2007 the Commission gave a proposal for a *Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism*[32]. It updates the Framework Decision of the year 2002 by complementing it with the use of the Internet for terrorist purposes and aligns it with the *Council of Europe Convention on the prevention of terrorism* (Warsaw 16 May 2005) by including in its concept of terrorism also the public provocation to commit terrorist offences as well as recruitment and training for terrorism.[33] The package contains a series of proposals dealing with the criminalization of terrorist training, recruitment and public provocation to commit terrorist offences, the prevention of the use of explosives by terrorists and the use of airline passenger information in law enforcement investigations as well as the second report on the implementation of the Framework Decision on combating terrorism. The Framework Decisions are relevant in the sense that they bind the member states to achieve the results but leave the choice of form and methods of implementation to the national authorities.

In March 2008, the Commission in its Communication "Reinforcing the Union´s Disaster Response capacity" (COM2008 130), put forward practical proposals paving the way for a comprehensive and integrated EU response. The Communication highlighted the urgency for an integrated approach to disasters bringing together prevention, preparedness, response and recovery. It further addressed all kinds of disasters (inside or outside the EU), and it covered for the first time all EU Community instruments as well as inter-agency cooperation. Four key areas were addressed: Increased inter-institutional cooperation, reinforcement of European humani-

29) 30 November 2005, 14469/4/05 REV 4.

30) The present EU Counter-terrorism Coordinator (CTC) is Mr Gilles de Kerchove. He was appointed on 19 September 2007 by EU HR Javier Solana. Tasks of the CTC are to coordinate the work of the Council of the EU in the field of counter-terrorism, maintain an overview of all the instruments at the Union's disposal, monitor the implementation of the EU counter-terrorism strategy, and ensure that the Union plays an active role in the fight against terrorism. The first CTC appointed after the Madrid 2004 bombings was Gijs de Vries.

31)See e.g. Monar (2007) and Zimmermann (2006).

32) COM(2007) 650 final.

33) Other relevant documents in this regard are the UN Security Council Resolutions 1373 (28 September 2001) and 1624 (14 September 2005) and the UN Global Counter-Terrorism Strategy (8 September 2006).

tarian aid, gearing up of European civil protection, improved coordination of disaster response capacities across various Community policies. Since then the Commission has taken number of actions in these areas, such as defined multifaceted scenarios in various fields of disaster relief operations inside and outside of the EU, developed better crisis management tools to enhance the information exchange with and between EU Member States, has developed the Monitoring and Information Centre (MIC) into an operations centre of European civil protection intervention and presented a legislative package for Chemical, Biological, Radiological and Nuclear (CBRN) substances.[34]

During the 2010 there have been several steps to enhance the counter-terrorism cooperation both among the Member States and with the third countries. The Spanish EU Presidency planned to set up a special unit aimed at sharing counter-terrorism intelligence among member states, according to Spanish media[35] *El Pais* reports that the new body will facilitate the direct exchange of intelligence between two or several member states in close co-operation with the existing special counter-terrorism co-ordinator, Gilles de Kerchove, and the EU situation centre SITCEN – a Brussels-based crisis management unit which includes counter-terrorism activities. National counter-terrorism units in Spain, Great Britain, Germany, France, Denmark, the Netherlands, Italy, Belgium and Portugal support the plan.

The EU's new legal framework, the Lisbon Treaty, also enables more co-operation and intelligence sharing in this area. Europol, the bloc's police co-operation and criminal data exchange body, also gained enhanced powers from 1 January. Its activities touch on terrorism as it manages data on chemical, biological and nuclear weapons, cybercrime and Islamist extremism on the web. The EU's institutional changes come against the backdrop of increased fears of terrorist attacks in European countries, after a failed attempt on 25 December to blow up a plane destined for the US, which took off in Amsterdam.

In February 2010, the Council approved an Internal Security Strategy for the European Union (5842/2/10), one of the priorities of the Spanish Presidency in this area. The European Council is expected to endorse the document and the Commission is expected to adopt a communication on concrete actions in the area. The strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection. The strategy highlights the challenges the EU is facing, including terrorism and organized crime. The strategy put weight on prevention and information sharing among Member states. The European Council of 10/11 December 2009, echoing the Stockholm Programme adopted at the same time, asked to tackle in particular terrorism, organized crime and natural disasters.[36]

In April 2010, new measures to streamline and simplify the EU framework for aviation security, first put in place in 2002 after the September 11 attacks, came into force. The revision is about better regulation – simplifying and improving procedures to make it easier for industry on a daily basis to implement safety controls, without any reduction in security. For passengers, the package opens the door for the EU to negotiate "one-stop shop" security agreements with

34) Inventory of CM capacities in the European Commission and Community Agencies, 31 July 2009, 3.

35) EUObserver.com, 4.1.2010.

36) Council of the European Union: EU Internal Security Strategy, 6870/10 (Presse 44).

the third countries – allowing for the possibility to reduce re-screening for transfer passengers. Most importantly, it sets a clear deadline for the lifting of the current restrictions on the carriage of liquids in cabin baggage – new screening equipment for liquids must be used in all airports across Europe by April 2013. Overall, the package aims to improve the passenger experience, shorten transfer times at airports and reduce costs.[37]

In May 2010, Catherine Ashton, High Representative gave a speech at the UN Security Council by emphasizing the role of the European External Action Service. Following on 20 May 2010 the Commission made a decision on the conclusion of the Implementing Arrangement between the European Commission and the Government of the United States of America for Cooperative Activities in the field of homeland/civil security research[38]. Only time will tell what this means in practice and whether the essential obstacles to synchronize the seed funds from the homeland security funding and the EU funding for mutual benefit of research projects can finally take place.

3. EU Crisis-Mode Mechanisms and Institutions

In this chapter are presented the essential EU bodies and mechanisms which according to a thorough study as well as many expert interviews have been selected to be the most relevant during a terrorism related crisis. The list is not exhaustive and may be disputed, but here it serves the purpose of being illustrative of what have been seen as the most relevant bodies in the case of terrorism related crisis in general and especially in reflection of the fictive case of Air passenger transport in the case of CBRN terrorism. In order to reflect also the nature of these bodies they are separated under the headings of political-strategic and operational levels.

✓ *3.1 Political-Strategic Level*

The EU Internal Security Strategy

The EU Internal Security Strategy (since 2010)[39] lays out a European security model, which integrates actions on law enforcement and judicial cooperation, border management and civil protection. Its main objectives are; to present to the public the existing EU instruments that already guarantee the security and freedom of EU citizens and added value that the EU action provides in this area; to further develop common tools and policies using a more integrated approach which address the causes of insecurity and not just the effects, and; to strengthen law enforcement and judicial cooperation, border management, civil protection and disaster management.

37) Transport: EU Updates Aviation Security Rules to simplify and improve procedures, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/479&format=HTML&aged=0&language=EN&guiLanguage=en, 29.4.2010.

38) Commission Decision of 20 May 2010, on the conclusion of an Implementing Arrangement between the European Commission and the Government of the United States of America for cooperative activities in the field of homeland/civil security research (2010/293/EU).

39) http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf

EU Emergency and Crisis Coordination Arrangements, CCA

In the almost immediate aftermath and as a response to London terrorist bombings in 2005 the JHA Council called for the development of *EU Emergency and Crisis Coordination Arrangements "to share information, ensure coordination, and enable collective decision making in an emergency, particularly for terrorist attacks on more than one Member State"*.[40] Consequently, on 1 July 2006 the JHA Council approved interim *Crisis Coordination Arrangements* (CCA).[41] The decision also included the organization of regular exercises in order to test the efficiency and adequacy of the CCA internal procedures. It is up to the SitCen to coordinate and organize operationally the exercises as well as to implement the CCA.

The arrangements are cross-pillar and applicable to crises within or/and outside the EU, but not for the crisis affecting individual member states. The London bombings provided the momentum for the work towards the CCA however keeping the focus on the terrorist attacks targeted at more than one member state. Even if terrorism launched the development towards CCA, the aim is not to focus solely on the threat of terrorism but to provide a generic arrangement applicable to all types of crisis, e.g. natural disasters, industrial accidents or pandemic flu. This type of integrated and coordinated EU crisis-management arrangements (ICMA) for crises with cross-border effects within the EU were called for already in The Hague Programme[42]. They were understood as the practical, operational arrangements to implement EU-CCA and to facilitate co-operation between member states whereas the EU-CCA was aimed at providing a framework for the EU institutions and affected member states on how they should interact in Brussels in a crisis mode. Currently the ICMA is no longer existent but has been included into the CCA.

The backbone for the crisis coordination arrangements is the principle of subsidiarity. Member states carry the primary responsibility for managing emergencies in their territory and the national competences will be respected. This is particularly important in order to secure the comprehensive participation both by the national and sub-national agencies. No new permanent structures should be established but use already existing structures. The arrangements aim at enabling to develop a coherent, optimal and pragmatic response to cross-border emergencies by meeting the needs of fast-developing crises. Despite the generic applicability, also tailored solutions should be possible, however not yet much tested.

The tendency in the EU to develop for itself a generic crisis response mechanism emphasizes not the threat itself but the protection and resilience of vulnerable targets and the vital functions of these societies themselves. This can be compared with the all-hazards approach of the critical infrastructure protection (CIP). The comprehensive approach is emphasized also in the CCA which is aimed at emergencies affecting more than one member state directly, simultaneously or by their interests engaged with the responsibilities of EU institutions. In the event of

40) JHA Council Declaration of 13 July 2005.

41) Consequently the Council's Secretariat has written internal standard operating procedures (SOPs) for the arrangements. A second revised version is dated on 23 October 2006. None of the documents are public due to the sensitivity of the information contained.

42) The Hague Programme: strengthening freedom, security and justice in the European Union (13 December 2004, 16054/04, point 2.4.) called for the establishment of an integrated EU arrangement for crisis management with cross-border effects (ICMA) and was to be implemented at the latest by 1 July 2006.

such circumstances, CCA specifies six functions to be carried out:

a. Information Access & Sharing
b. Support
c. Enabling consistency in the actions taken by Member States, the Commission and EU agencies as far as possible.
d. Enabling debate on contentious policy decisions if necessary.
e. Enabling debate on collective external action if appropriate.
f. Media Co-ordination

CCA is built mainly to the action taken place in Brussels. According to the CCA there is a key role for the Presidency and affected member states in the case of cross-border emergency. In the EU this will be executed through member states' Permanent Representation in Brussels (COREPER). It is important to bring together the core group of decision-makers i.e. the COREPER which is the central body for coordinating decisions and connecting the EU bodies in order to share information, ensure coordination and enable collective action. So far the decision-making and crisis coordination mechanism is built so that in a crisis situation following components should be established: *Crisis Steering Group, Action Platform and Support Group*.

Crisis Steering Group's (CSG) task is to act as the central coordinating body and build a common understanding and assessment of the situation. The crisis steering group uses the information received from the EU structures to develop and report on alternatives for the decision and response as well as to follow-up on implementation of decisions to the COREPER and the Council. It is therefore up to the Steering Group to think and plan strategically in response to a crisis. In addition, it is the purpose of the Crisis Steering Group to act as a channel for information towards the member states, the media and other international partners. This may be e.g. advising member states on collective action or communicating the member states' needs if the existing arrangements are not sufficient.

It is under the responsibility of the Presidency, in agreement with the affected member states, to convene the Crisis Steering Group and decide on its composition. However, it is predefined that group will consist of high-level, cross-pillar actors or their representatives such as the Presidency as Chair, Secretary General/High Representative, Commission and the affected member states. Depending on the nature of crisis relevant staff of the Council Secretariat (e.g. Counter Terrorism Co-ordinator), Commission services (e.g. DG JLS crisis room), Agencies (e.g. Europol), Joint Situation Centre, Monitoring and Information Centre as well as from other member states concerned would also be included in the Crisis Steering Group.

Action Platform should be formed by a body that is empowered to take decisions or agree on coordinated action, i.e. the COREPER. The COREPER will consequently act as an overall coordinating body and convene as soon as the Crisis Steering Group has made a clear assessment on what has happened. The Steering Group lays down the groundwork for the COREPER whose task is to consider and decide on the different possible responses to the crisis at EU level. The COREPER is the responsible body for the political responses and to launch the operational responses. The decisions to be taken by the Council are identified by the COREPER, but at least so far, those decision-making powers are not delegated to the COREPER.

Support Machinery will support Crisis Steering Group by input, expertise and analysis provided by the affected member states' relevant services, Council Secretariat, Commission and Presidency. If necessary Crisis Steering Group will convene an ad hoc Support Group consisting of senior officials who have the expertise and analysis from the field of the ongoing crisis. In addition the systems of the EU SitCen, MIC, ARGUS, DG JLS crisis room as well as relevant experts would be included as support machinery.

If the member state cannot deal with the crisis situation without external help, an estimation of the need of help and of political EU-coordination is done as described above. If political EU-coordination is not needed, the Commission can coordinate EU-operation and member states act together by using the Crisis coordination handbook. Therefore, only if the political EU-coordination is needed, the CCA is activated. First time the CCA was activated or better applied, was during the Lebanon crisis during the Finnish EU-Presidency. Cyprus was the member state to request for the activation of the mechanism and Finland as holding the Presidency made the decision on the activation of the mechanism. CCA was applied inter alia to organize the evacuation. One can only underline the importance of full investigation and studies to be conducted how the CCA was able to cover the situation and what were both the major obstacles and benefits of its mobilization.

The EU Joint Situation Centre (SitCen)

The EU Joint Situation Centre (SitCen) was originally part of the Council Secretariat and it was established in 2002. Now the EU aims to merge into one new department the EU Council's Joint Situation Centre, its Watch-Keeping Capability and the European Commission's Crisis Room to help guide new established Europe´s External Action Service (EAS) decisions on security matters.

The Joint Situation Centre, known as The SitCen, today has 110 staff members and is located on Avenue de Cortenbergh, in the heart of the EU quarter. The Watch-Keeping Capability is in the same building. Its team, made up of 12 people from EU states' police and armed forces, pulls in news from the EU's 23 police and military missions, such as the EUMM in Georgia.

The Crisis Room, around the corner in the commission's Charlemagne building, is run by six officials. It operates a secure website with breaking news about the world's 118 active conflicts from open sources and from the commission's foreign embassies. It uses scientific tools, such as statistical analysis, and high-tech software: One program scans TV broadcasts round the world and automatically picks out quotes on search terms, such as people's names.[43]

The SitCen co-operates on analytical basis with the issues that touch the core of national sovereignty: national security and intelligence services. In the larger context it aims to manage political and other crises, but it can also be of great help in developing a common understanding of the terrorism threat itself with the contributions from national security and intelligence agencies, which is one of the fundamental issues in developing counter-terrorism policies.

The main task of the SitCen is to monitor and assess events and situations worldwide on

43) http://euobserver.com/9/29519

a 24-hour basis with a focus on potential crisis regions, terrorism and WMD-proliferation. According to The Hague multi-annual work programme[44], the intention is that SitCen furnishes the Council with strategic intelligence-based assessments on counter-terrorism matters and therefore supports the EU policy making. The aim is to jointly assess the terrorist threat already in the developing phase both inside and outside Europe. The cross-pillar work programme incorporates justice and home affairs priorities, as well as those issues highlighted by external policy working groups. As such, it includes for example, assessments on threats to modes of transport; threats to critical national infrastructure targets in EU member states; and an assessment of trends in terrorist financing.

In addition to the monitoring and risk assessment, the SitCen has an important role during the crisis. As we know, there is no online connection to the SitCen but once the EU Emergency and Crisis Coordination Arrangements (CCA) is activated, the connection is established. This of course might cause some organizational mistrust within Member states. However, the SitCen is manned with the analysts from the EU's external intelligence services and the internal security services which can overcome this situation through collegial networks and the code of conduct.

The SitCen has three units (cells): the Civilian intelligence Cell (CIC), which comprises of civilian intelligence analysts working on political and counter-terrorism (CT) assessment; the General Operations Unit (GOU), that provides 24-hour operational support, research and non-intelligence analysis; and the Communications Unit, that handles communications on security issues and runs the Council's communications centre (ComCen). The creation of a counter-terrorism analytical capacity within the Civilian Intelligence Cell became active in February 2005 and was a major aspect of the SitCen's development since the attacks of March 2004 in Madrid. The SitCen's priorities focused before largely on Common Foreign and Security Policy issues and did not necessarily serve to provide the necessary Justice and Home Affairs input. Now with the counter-terrorism Cell's work programme reflecting broader EU-CT priorities the support can be given to JHA policy areas. The principal area where SitCen counter-terrorism Cell can contribute to JHA work is strategic intelligence-based assessments on counter-terrorism matters in support of current policy discussions.

The SitCen also provides support to the EU High Representative, Special Representatives and other senior officials, as well as for EU crisis management operations. The Council Secretariat has worked through High Representative for the Common Foreign and Security Policy Javier Solana in implementing the Council strategies. The work remains confidential, but since the Council is accountable to the European Parliament, the EP can discuss the work of the SitCen with the Council of Ministers.

All in all, the SitCen is important in several ways. First, within the SitCen a merger is taken place between internal and external aspects of EU Counterterrorism policy. Second, the SitCen is an important channel through which horizontal structures of intelligence cooperation outside the formal scope of the EU merges with formalised vertical EU counterterrorist structures.[45]Thirdly, the SitCen can promote cross-sectoral cooperation and participate in national and

44) The Hague Programme – Ten priorities for the next five years, 10 May 2005.

45) Buuren Van, Jelle, 2009, Secret Truth, The EU Joint Situation Centre, Amsterdam, Eurowatch, 2-3

multinational table top and live exercises outside of its official agenda, as long as they support its mandate and overall interests of the Member states.

Council's Crisis Management Structures

The Council´s crisis management structures were established in the European Council of Nice in December 2000. The civil-military cell includes permanent political and military structures. The Political and Security Committee (PSC) keeps track of the international situation and helps to define policies within the Common Foreign and Security Policy (CFSP) including the Common Security and Defence Policy (CSDP), formerly known as the European Security and Defence Policy (ESDP). Formally, CSDP is the domain of the Council of the European Union, which is an intergovernmental body in which the member states are represented. Nonetheless, the Union High Representative Catherine Aston also plays a significant role. In her position as a Chairman of the external relations configuration of the Council, she prepares and examines decisions to be made before they are brought to the Council. Political and Security Committee is an ambassadorial level preparatory body for the Council. Its task is to prepare a coherent EU response to a crisis as well as exercise the EU's political control and strategic direction.

Crisis Management Planning Directorate (CMPD)

In December 2008, the European Council agreed to merge civilian and military aspects of the planning for European peace keeping missions into a single Crisis Management Planning Directorate (CMPD). It was a logical step that would help the EU to be more efficient in its response to conflicts. As this new structure is now taking shape, however, the military aspect has been given vastly disproportionate weight. One of the problems is to have enough well trained and experienced civilian officials for planning and conducting crisis management duties.[46] According to the *Lisbon Treaty* (2009) some new structures and arrangements are coming to be used for crisis management, counter-terrorism duties included. First and foremost, there is to be mentioned the *Crisis Management Planning Directorate* (CMPD) which is intended to be core of the External Action Service. The principle to integrate internal and external security duties is already accepted, but the implementation of organizational structures and strategic-operational functions is just beginning.

✓ *3.2 Operational-Tactical Level*

Community Mechanism for civil protection

Community Mechanism for civil protection was established by the European Commission in 2001[47]. A recast of the Council Decision was adopted in 2007[48]. The Mechanism is a tool to enhance and facilitate community co-operation in civil protection matters and assistance interventions in and outside of the EU. Even if the mechanism was established in the 9/11 aftermath, terrorism is not mentioned in the 2001 Council decision. In 2007 recast acts of terrorism are however included in all types of major emergencies.

46) See Alain Délétroz, *The spoils of EU reform*, Reuters 19. February 2010. In internet: mhtml:file://J:\EUcrisismanagement2010.mht

47) Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions (2001/792/EC, Euratom).

48) Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism (recast) (2007/779/EC, Euratom). Currently the annual budget is €7 million.

The Mechanism may be activated in the event of major natural or man-made emergencies which may require urgent response actions or in the situations where there may be an imminent threat of such major emergencies. The primary responsibility for dealing with the disaster lies with the country where the disaster occurs according to the principle of subsidiarity. When the scale of the disaster overwhelms national response capacities, the affected country can benefit from civil protection means or teams available in other member states. Support is therefore made available on request of the affected country for other member states' available resources.

Monitoring and Information Centre (MIC)

Monitoring and Information Centre (MIC) is operated 24/7 and is often described as the heart of the Community Mechanism. MIC is based in Brussels and run by the Civil Protection Unit of DG Environment at the Commission. It produces information letters called MIC Daily (Daily Monitoring and Alert Service) in collaboration with the EC Joint Research Centre. The MIC Dailies contain solely information on natural disasters and ongoing emergencies, e.g. forest fires, aviation accidents, pollution.

The MIC gives countries an access to a platform of civil protection means available amongst all participating states. Its task is to coordinate the alerts and offers, needs and/or requests of assistance directly at headquarters level and between participating states, the affected country, dispatched field experts and other organisations such as the UN or the Red Cross. Alerts and requests for assistance in the case of a major disaster can come from inside or outside the Union. The MIC also provides updated information on the actual status of any ongoing emergency.

So far the Mechanism has not been taken into use through the MIC in the terrorist strikes. Neither Spain nor the Great Britain made requests of help after the attacks of Madrid in 2004 or in London in 2005. Instead it has been used in several natural disaster cases in and outside of Europe (e.g. the Prestige oil accident 2002, forest fires in France and Portugal 2003, 2004, earthquakes in Algeria 2003, coordination of EU assistance to hurricane struck areas in the US). The Mechanism is therefore a good example of an instrument that was founded in the aftermath of 9/11 attacks but has clearly been directed to other types of emergencies than terrorism. However, following the EU's current approach on terrorism, the MIC is one of the bodies that have been stretched out to reach terrorism as well.

During emergencies the MIC plays three important roles:

- Communications hub: Being at the centre of an emergency relief operation, the MIC acts as a focal point for the exchange of requests and offers of assistance. This helps in cutting down on the 30 participating states' administrative burden in liaising with the affected country. It provides a central forum for participating states to access and share information about the available resources and the assistance offered at any given point in time.
- Information provision: The MIC disseminates information on civil protection preparedness and response to participating states as well as a wider audience of the interested. As part of this role, the MIC disseminates early warning alerts (MIC Daily) on natural disasters and circulates the latest updates on ongoing emergencies and Mechanism interventions.

- Supports co-ordination: The MIC facilitates the provision of European assistance through the Mechanism. This takes place at two levels: at headquarters level, by matching offers to needs, identifying gaps in aid and searching for solutions, and facilitating the pooling of common resources where possible; and on the site of the disaster through the appointment of EU field experts, when required.[49]

The General Rapid Alert System and Crisis Communications Network (ARGUS)

The ARGUS general rapid alert system and crisis communications network was introduced in December 2005 after both natural (tsunami Dec 2004) and man-made (Madrid 2004, London 2005) disasters had taken place.[50] The aim was to answer to the need to improve the co-ordinated management of multisectoral crises at the Community level. In the event of an emergency Commission may be called upon to support the member states by acting in its domains of competence and by providing comprehensive information to the public and the media.[51]

In the event of multisectoral crisis of natural or man-made origin, ARGUS aims to provide the following elements: information exchange via internal platform in real time, internal coordination, consolidation of the alert systems and having the appropriate processes for decision making ready.[52] ARGUS as other EU-systems is based on the principle of subsidiarity and complementarity taking into account the existing Rapid Alert Systems (RAS) and linking it to Directorate-General's and Commission's services. ARGUS also uses the already existing resources, technology and infrastructure.

In the event of a major emergency it is up to the Presidency to decide, after having been alerted or at the request of a Member of the Commission, to activate the ARGUS coordination process. The President may keep the responsibility for himself or delegate and assign it to a Member of the Commission. The responsibility consists of leading and coordinating the response to the crisis at hand. The Commission's Secretariat General will then activate the specific operational crisis management structure Crisis Coordination Committee (CCC) which will monitor and assess the ongoing situation as well as identify issues for action and decision which will be adopted through normal Commission decision-making procedures.

In addition to the selected crisis-mode instruments and bodies presented here there exist also EU bodies that operate mainly on the prevention, protection and pursuit areas of the counter-terrorism strategy. These are operational before the crisis occurs, since at the moment of a terrorist strike, they can be said to have failed. These bodies can also be listed under the so called early-warning mechanisms since they deal with the risk assessment, investigation and monitoring. In the following some of these relevant bodies are presented shortly.

49) http://www.geoportal.org/web/guest/geo_resources_details?p_p_id=vrdPortlet_WAR_geoportal&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_vrdPortlet_WAR_geoportal_rid=857

50) COM (2005) 662 final, Commission provisions on "ARGUS" general rapid alert system.

51) Creation of ARGUS was mentioned already in the Commission communication on preparedness and consequence management in the fight against terrorism (2004)COM(2004) 701 final.

52) CIWIN Critical Infrastructure warning information network aims to do the same in the field of critical infrastructure protection, COM (2006) 786 final.

The European Union's Judicial Cooperation Unit (Eurojust)

The Eurojust[53] was established in 2002 to enhance judicial cooperation, i.e. coordination and effectiveness of the competent authorities within member states when dealing with the investigation and prosecution of serious cross-border and organised crime. The aim has been in creating a network of experts to ensure the proper execution of mutual legal assistance requests, and member states are obliged to designate a national correspondent for terrorist matters.

European Police Office/European Law Enforcement Organisation (EUROPOL)

The Europol[54] was set in 1992. It is a body for the coordination of intelligence and investigative support. It aims at improving the effectiveness and co-operation of the competent authorities in the member states. Its priorities are preventing and combating terrorism among other serious forms of international organised crime. The role of Europol has been strengthened, and it is considered as a central and valuable tool in the fight against terrorism. Europol produces annual reports on terrorism activities. The personnel have no authority of their own to act in member states.

Joint Investigation Teams (JIT)

The Joint Investigation Teams were set up by the Framework Decision 2002 on combating terrorism to improve cooperation and exchange of information e.g. in the identification of presumed terrorists between the member states' intelligence services. Lists of terrorist organisations are drawn up according to these information investigations.

Rapid Reaction Mechanism (RRM)

The RRM has provided funds for the projects in the areas of terrorist financing and border management. It is part of the EU's external actions with the third countries in counter-terrorism. The future role of the RRM could be more essential in tackling the seed funding for pioneering research and development projects with the third countries and the various private sector partners.

European Union Military Committee (EUMC) and CIVCOM

The EU military body is called the European Union Military Committee (EUMC), composed of the Chiefs of Defence of the member states, who are regularly represented by their permanent military representatives. The European Union Military Committee provides the Political and Security Committee with advice and recommendations on all military matters within the EU. In parallel with the EUMC, the PSC is advised by a Committee for Civilian Aspects of Crisis Management (CIVCOM). This committee provides information, draft recommendations, and gives its opinion to the PSC on civilian aspects of crisis management. This type of crisis management however often refers to a more long-lasting crisis than to a crisis caused by terrorism.

Civilian Planning and Conduct Capability (CPCC)

The Civilian Planning and Conduct Capability (CPCC) has a mandate to plan and conduct civilian Common Security and Defence Policy (CSDP) operations under the political control and

53) Eurojust, http://eurojust.europa.eu/

54) Europol, http://www.europol.europa.eu/

strategic direction of the Political and Security Committee. CPCC works in close cooperation with the European Commission. The CPCC Director, as *EU Civilian Operations Commander*, exercises command and control at strategic level for the planning and conduct of all civilian crisis management operations, under the political control and strategic direction of the Political and Security Committee (PSC) and the overall authority of the Secretary-General/High Representative for the CFSP (SG/HR).[55]

There have been initiatives and plans to unite the efforts of military (DG8) and civilian (DG9) sectors towards common goals and working with an integrated planning and command structure like the Civilian Planning and Conduct Capability (CPCC). Actually, it is not so new an arrangement because many EU crisis management operations have already an integrated command structure.[56]

4. EU Crisis Co-ordination and Decision-Making in the Aether Type of Scenario

Terrorist offences defined in the Council Framework Decision (13 June 2002) on combating terrorism are realized in Project Aether scenario's situation almost completely. The Aether (like its predecessor Project Poseidon on Maritime Safety) scenario fulfils the criteria of an intentional act with the aim of *"seriously intimidating a population, unduly compelling a Government or international organisation to perform or abstain from performing any act, and seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation"*. In addition to this, the points *(a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; (c) kidnapping or hostage taking; (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; (e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; and (i) threatening to commit any of the acts listed in (a) to (h)* are fulfilled.

Essential aim of the EU counter-terrorism policy is the overall take on the crisis, i.e. prevention, protection, pursuit and response. This includes both the before-phase (risk-mapping, monitoring, early-warning) as well as the after-phase (reconstruction, regaining trust, and clearing the accountability) of the attacks. Here we focus on and emphasize the phase when the crisis is happening i.e. the during-phase.

We have divided the analysis according to chronological timeline of the fictional terrorist

55) http://www.consilium.europa.eu/showPage.aspx?id=1487 and http://www.consilium.europa.eu/uedocs/cmsUpload/100217%20Factsheet%20-%20CPCC%20-%20version%201_EN%20-%20DRAFT.pdf

56) See Stephanie Blair, "Towards Integration? Unifying Military and Civilian ESDP Operations", *European Security Review* 44, ISIS Europe, May 2009.

strike. The first segment would consist of **preparedness** (alerting, information sharing, analysis and assessment – information flow; from where and who to where and whom), the second of **response** (situation assessment, political and operational decisions, collective and consistent action, responsibilities, uncertainty, limited time) and the third of **consequence management** (organising operational arrangements, collective or supporting action). We are specifying here the information flow in the EU in these segments and at the end of the chapters; we are making the connection with the six functions to be carried out in a crisis situation stated in the CCA.

✓ *4.1 Preparedness: Alarm and Information*

To be able to start the crisis-mode mechanisms one needs to get the information on what has happened. When the terrorism situation emerges on the passenger plane, the flow of information becomes uncontrollable and spreads out where possible. Today in the era of having news updated many times per day in the Internet, it is without no doubt that the information of a terrorist strike will go as a lightning to different directions. In a crisis situation it is essential that the information received is correct and accurate. In addition to this and in relation to the decision-making the initial calls of alarm and contacts are essential since they form the basis for the framing of the problem and its solution[57].

The Council's SitCen monitors 24/7 the political situation in and outside the EU. It would get the information of the case Aether either through official and confidential channels or through public sources e.g. the Internet. When the SitCen receives the information of a crisis, it contacts the Commission, the EU Presidency/The On-Call EU Embassy and the Council Secretariat.

The EU-Presidency then negotiates the situation with the Commission, and with the member states (or with their permanent representatives i.e. the COREPER in the EU) involved in the crisis, and the Council Secretariat. In the Aether scenario the member state most involved would be Finland, since the terrorist offence is committed in a passenger plane flying under the flag of Finland. Therefore it would also be Finland's responsibility to act[58]. Other countries' legitimacy to act comes from the fact that they have their nationals on board[59]. This would therefore involve at least Sweden, Russia and perhaps the Hong Kong SAR and the People´s Republic of China as the plane is on a return flight from Hong Kong. It is up to the COREPER to keep other member states not directly involved updated on the situation.

The Commission's role would be supportive by using the ARGUS. In the event of an emergency Commission may be called upon to support the member states by acting in its domains of competence and by providing comprehensive information to the public and the media. The Aether case would most likely involve the Directorate-Generals of Justice and Home Affairs, Environment and possibly RELEX due to the third country Russia's involvement into the crisis as the plane is on a flight route in the Russian airspace.

57) Larsson, Olsson, Ramberg 2005, 88.

58) Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

59) Ibid, Article 9.

According to the Crisis Coordination Arrangements these functions are defined as tasks of *Information Access & Sharing* (Alerting and subsequent information-sharing, strategic analysis and assessment so that the member states and, where competent, the EU institutions can take the measures necessary to protect citizens) and Media Co-ordination (Co-ordinating information passed to the media on key points, to ensure consistency between what is said by representatives of member states and what is said by senior EU figures).

✓ *4.2 Response and Decision-Making*

According to the CCA it is up to the Presidency country and/or the President to decide on the start-up of the political coordination. If the decision is favourable, the Crisis Steering group convenes and takes the matter into the COREPER II[60].

Having a direct effect on more than one member state (Finland and Sweden) and engaging the entire Union as well with the specific ultimatum demanding for the EU action it became clear in the expert interviews that the Aether-scenario's situation would be so challenging, that CCA would be launched without any doubt.

The Permanent Representatives would communicate with each other and negotiate with the capitals before any key decisions are made. In the special circumstances the country that holds the EU Presidency and the Minister concerned can negotiate also directly with the member states faced with the crisis situation and EU-organs. The statements and directions are made on the basis of cooperation with the ministries when necessary. The COREPER is therefore the body to make the effective decisions.

It seems that the executive focus and overarching responsibility in the Aether case would be Finland's since the CBRN threat caused by terrorism or organized crime is taking place in the passenger plane under the Finnish flag as well as in the Finnish air space. However, as the first symptoms occur in the Russian airspace, there might be strong Russian involvement in proposing bilateral operation or Russian led rescue plan to solve the problem.

According to the CCA, it is the responsibility of the affected member state i.e. Finland to use all its equipment and resources available. However, in this type of multidimensional crisis the Finnish Ministry of the Interior would most likely send the request of assistance to the European Commission's MIC.

In a situation like Aether the EU has to take both political and operational stand on the situation. COPS/PSC would review the development of the crisis and consider possible EU actions. At the same time the EU Commission and member states would map the situation.

The Aether scenario involves also a non-EU country Russia as well as the country/countries of origin of terrorists (whatever that may be). Therefore the EU policies of justice and

60) COREPER II comprises of the Permanent Representatives and prepares for configurations regarding General Affairs and External Relations (including Common security and defence policy and development cooperation); Economic and Financial Affairs (including the budget); and Justice and Home Affairs (including civil protection).

home affairs and external relations should be connected and most likely this would be done via ARGUS.

Russian involvement and its geo-political position are of crucial importance for upholding the European security system and the action in the EU would be based on the analysis made by the COREPER and COPS/PSC. The premise for the political decision is the unanimity of the member states. Would there be any national interests that would make some member states not to content to the unanimous decision the decision-making could be hindered.

In CCA, these actions are named as the functions of Enabling Consistency in the actions taken by the member states, the Commission and EU agencies as well as Enabling debate on contentious policy decisions.

✓ *4.3 Implementation – Consequence Management*

In the Aether case, the Civil Protection Mechanism would most probably be activated, since it is a question of an *imminent threat of a major emergency which may require urgent response actions*.[61] Particularly in the light of large potential of several air planes carrying a similar threat simultaneously.

The scale of the disaster would most likely overwhelm Finnish national response capacities and the request of aid would be realized. It is the MIC's role to coordinate the aid of civil protection means or teams from other member states. Therefore, once the MIC has received a request of aid, it immediately informs the national civil protection authorities. Even if the aim of the Community Mechanism for Civil Protection is to cover all kinds of threats from floods to terrorist attacks, it is unclear what kind of mobilising would be done in the case of terrorism and more precisely in the Aether type scenario. It might be launched to aid in the rescue operation and/or consequence management at the European airports concerned. The Mechanism seems however to be more targeted at the victims of natural disasters since the assets aimed at saving lives and alleviating suffering in the first days of a disaster typically consist of search and rescue equipment, medical services, temporary shelters, sanitation equipment etc.

Otherwise the mobilizing of aid in the response for the terrorist strike in the Aether case would most likely be done according to the bilateral agreements e.g. with countries able to provide imminent emergency landing areas for the affected plane, Sweden and Estonia for example. Since Russia is involved due to its nationals onboard and airspace involved, one must take into account the debate on external action.

The implementation of operational decisions as the response action are defined in the CCA as the functions of *Support - Facilitating the provision of mutual operational support to Member States who do not have sufficient capabilities to deal with the crisis* as well as *Enabling debate on collective external action*.

The Aether type of terrorist strike contains the same generic attributes that can be as-

61) European civil protection, http://ec.europa.eu/environment/civil/prote/mechanism.htm

sociated more widely to the concept of crises. One of these is the lack of or the limited amount of time. The second is the importance of the values or the social order in stake, and the third the *uncertainty* that almost always prevails in a terrorism related crisis situation.[62] One could also add the element of *surprise*. These attributes and their influence however become real almost solely in an actual crisis situation, or in a well organised exercise. In a hypothetical situation and in the exercise such as the Poseidon table-top exercise these factors, which influence the end result of managing the crises considerably, may be identified and later become lessons learned.

5. EU's Common Action in Counter-Terrorism and Crisis Management

In the *European Union security strategy* (2003) terrorism is named as an essential threat, and measures of preventing and countering it have a high priority. In the *review report on the security strategy* (2008) terrorism and organised crime are still seen as a central threat for EU member states as follows:[63]

> "Within the EU, we have done much to protect our societies against terrorism. We should tighten co-ordination arrangements for handling a major terrorist incident, in particular using chemical, radiological, nuclear and bioterrorism materials, on the basis of such existing provisions as the Crisis Coordination Arrangements and the Civil Protection Mechanism. Further work on terrorist financing is required, along with an effective and comprehensive EU policy on information sharing, taking due account of protection of personal data."

In spite of the enhanced efforts mentioned above, the structures, organisational arrangements and practical functions concerning terrorism are too fragmented and complicated. It is, however, clear that the EU has much potential and capacity for working as a central actor in the international cooperation against terrorism.[64] Principles of decision making in a crisis, from the viewpoint of a member state, are described in the figure. It can be applied also to a terrorist case.

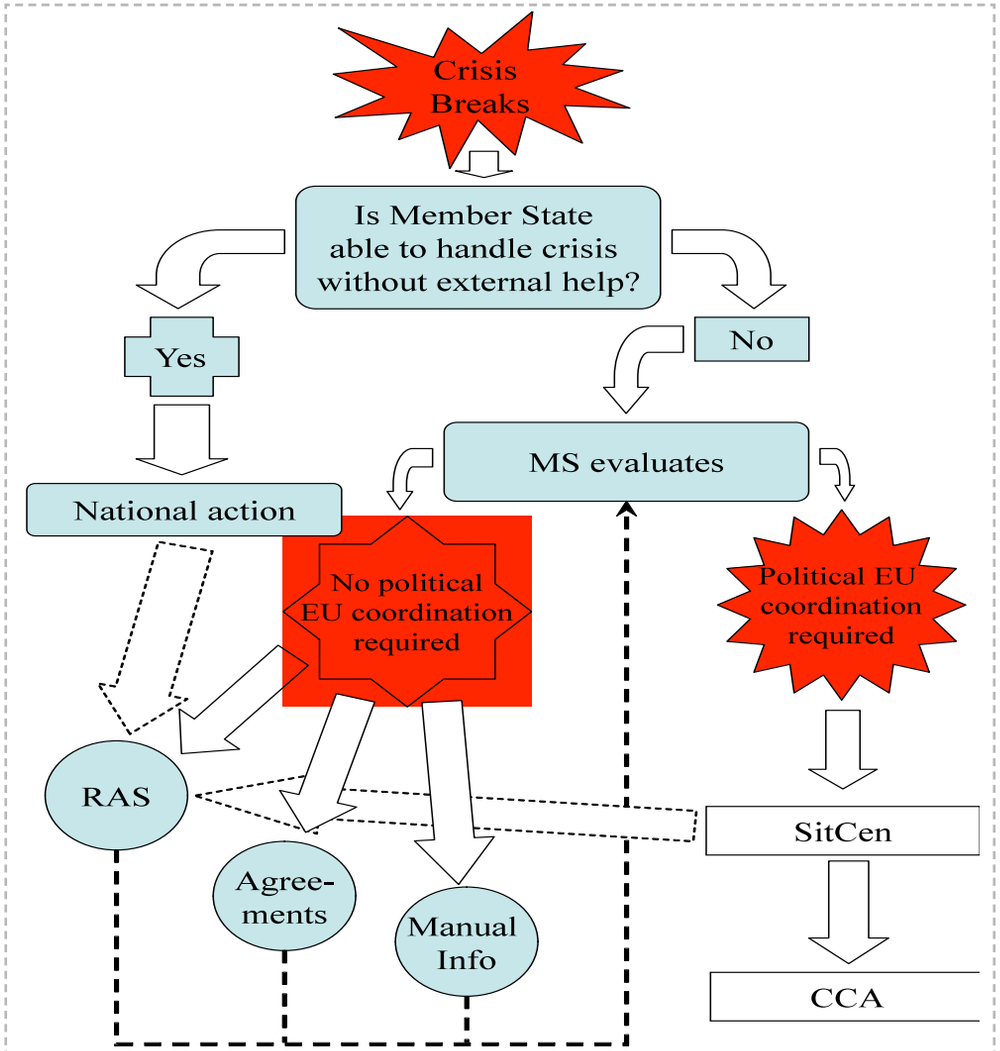
EU-counter-terrorism's added value is primarily the coordination and information sharing of the existing resources. Since counter-terrorism is still a policy the primary responsibility of which belongs to the member states, EU's role consists of strengthening national capabilities. This is done by sharing information, knowledge and experiences, and facilitating European cooperation between e.g. police and judicial authorities. However, it seems that EU-level coordination and resource back-up are currently still of minor importance in relation to bilateral and multilateral agreements on assistance and support. Collective capability and policy responses

62) These attributes can be found e.g. in the following works: Boin,'t Hart, Stern & Sundelius (2005): *The Politics of Crisis Management. Public Leadership under Pressure*. Cambridge University Press. New York; Boin, Ekengren & Rhinard (2006): *Functional Security and Crisis Management Capacity in the European Union*. Swedish National Defence College. Elanders, Vällingby; Brändström, Bynander & 't Hart (2004): Governing by Looking Back: Historical Analogies and Crisis Management, Public Administration Vol. 82 No. 1, 191-210.

63) *Report on the Implementation of the European Security strategy- Providing Security in a Changing World*, p. 4. In internet: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

64) See e.g. Piia Nikula - Timo Hellenberg, "EU crisis coordination arrangements and decision-making" in *Preventing Terrorism in Maritime Regions*, 2009.

CCA: CRISIS CO-ORDINATION ARRANGEMENT, 1st July 2006 →



Picture from the Prime Minister's Office, Finland.

instead lose their significance when national capabilities are strengthened and counter-terrorism still considered primary as an internal police matter.

EU-counter-terrorism promotes international partnerships beyond the EU with the third countries, other international organisations (e.g. NATO) and in particular with the United Nations (UN). These partnerships form a valuable asset for the EU in the global counter-terrorism. In threat perception the international and cross-border nature has been acknowledged, but in relation to responses the primary responsibility still remains under national jurisdiction.

Political support and solidarity capture the strongest added value the EU has currently to offer in counter-terrorism. Speaking with one voice and demonstrating a strong and unanimous position against terrorism is by far not a modest accomplishment by 27 member states. EU's joint policies are also defended by the European public. Citizens are increasingly favouring joint decisions within the EU in many policy areas, and the latest Eurobarometer shows that fighting terrorism became first when citizens were asked whether a decision should be made by the national governments, or jointly within the EU[65].

Many of the current mechanisms and actions to combat terrorism were not primarily designed to counter-terrorism. They were bodies that tackled against serious and organized crime. Afterwards these actions have been extended to include the natural disasters and moulded into the all-hazards approach. However the all-hazards approach becomes problematic during the crisis since terrorism and natural disasters as phenomena differ from each other so drastically by character and nature.

Terrorism has not respected nor operated according to the traditional order of borders or frontiers for a long time. However, the threat of terrorism is still almost solely treated as an "internal" problem within the EU (DG Justice and Home Affairs) as well as in many member states. Countering terrorism is often situated under the police matters[66] and most so-called European capabilities in CT are vested in the member states' domestic security and intelligence services, or justice, police or military organizations. Therefore, even if terrorism is considered as an international threat, the actual strikes and responses to them are still regarded national. Countries insist on having the primary responsibility and at the same time they reduce the EU's role into of little account. The question whether the current coordinative mechanisms should be developed from mere coordination to robust, integrated or autonomous EU-counter-terrorism capabilities comparable to those of the member states remains open.

Countering terrorism should also be raised more efficiently on the agenda of external relations. This would cohere well with the priority areas of the EU-CT strategy of prevention of extremism and violent radicalization. Overall, the EU-CT strategy should be linked directly to the Common Foreign and Security Policy and Common Security and Defence Policy.

Counter-terrorism reaches almost all branches of the EU. At least for the time being, this type of cross-sector and cross-pillar approach has not succeeded at its best. EU-CT remains as a jungle of concepts and bodies and opens up rarely to anyone outside the system. The EU-CCA and other

65) European Commission (2007): Eurobarometer 68 Public Opinion in the EU/ Autumn 2007, Publication December 2007. QA20. Fighting crime was also among the 8 top issues.

66) Zimmermann Doron (2006): Terrorist Threats, the European Union and Counter-Terrorism, PowerPoint presentation, Study Group on the Economics of Terrorism, 25 May 2006. Center for Security Studies. Swiss Federal Institute of Technology (ETH Zürich).

crisis-mode mechanisms are still seen as supportive mechanisms to "real" decision-making which is done either nationally or when necessary according to bilateral or multilateral agreements.

In the table below are listed the actions that strengthen and in contrast may undermine the EU's added value as a common actor in countering terrorism.

Strengthening EU's added value	**Undermining EU's added value**
Coordination, cooperation, teambuilding	Bilateral and multilateral agreements on assistance and support
Collective capability and policy synchrony	Strengthening national capabilities on domestic safety and security
International and private-public nerships	National responses to international threats and overlapping capacities e.g. training.
All-hazards approach	Counter-terrorism and natural disasters cannot be solved in one-size fits all Approach
Solidarity	Preserving sovereignity
Comprehensive and integrated situational awareness, crisis management system and sharing of information	Segmented intelligence and crisis management, e.g. a strict partition between internal and external affairs

During the last years the European Union has very much enhanced efforts against chemical, biological, radiological and nuclear (CBRN) threats. In February 2008 the Commission set up a *CBRN Task Force* to develop a special EU policy concerning that area. Its final report was issued in January 2009 and recommended an action plan for CBRN countermeasures.[67]

The Commission proposed a large package of 133 measures in June 2009. It has a broad approach to CBRN security, ranging from prevention and detection to enhancing preparedness and response capacities focusing on following areas:[68]

- Prevention: Ensuring that unauthorized access to CBRN materials of concern is as difficult as possible.
- Detection: Having the capability to detect CBRN materials.
- Preparedness and response: Being able to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible.

The measures included in the *CBRN action plan* (June 2009) will be predominantly implemented by existing national, EU and international structures, using a broad variety of tools. The directorate-general for Justice, Freedom and Security plans to allocate up to €100 million from existing financial programs to support the implementation process over the period 2010–2013. Other EC funding programs - such as the Security Research Programme under the Seventh Framework Programme - will also contribute to the CBRN action plan.

67) *EU action plan on chemical, biological, radiological and nuclear security* 24 June 2009: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0030_en.htm#

68) http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/992&format=HTML See also: http://aero-defense.ihs.com/news/2009/eu-en-cbrn-security-policy-062409.htm

6. Conclusions

European integration forms a unique ensemble of people, ideas, technology and goods moving freely within the European Union. A lot of borders are being run down to promote openness, democracy and solidarity. However, almost as much of control, supervision and joint monitoring is being increased due to the fear of some abusing these cherished freedoms. It is seen indispensable for the EU to enforce its counter-terrorism activities but at the same time guaranteeing the rights and freedoms of its citizens.

In this article the EU Crisis coordination arrangement (CCA) and decision-making capacity has been looked from the viewpoint of countering terrorism. We have used an imaginary and fictional case of CBRN terrorism in the air passenger transport flight from Hong Kong to Helsinki in order to find out how the information flow and decision-making would be enacted according to the CCA.

The EU CCA takes into account all the relevant phases of a crisis: alarm and information-sharing, decision-making as well as the implementation of the response activities but has no real operational role. Its main value is in starting up a mechanism for political support. This comes close to the main accomplishment of the EU-CT as well which forms of the common definition of terrorist offences and the common voice of solidarity. On the operational level, the added value still lies in the form of coordination and information sharing rather than true operational cooperation. The member states are still counting on the bilateral and multilateral agreements instead of EU-level action.[69]

The bombings in Madrid and London made the EU face its infrastructure's vulnerability against terrorism. Since crises are defined by uncertainty, the emphasis in risk mapping must be in new and unimaginable threats. The significance in the crisis management studies and exercises is not necessarily the absolute plausibility of the scenario *per* se but the fact to make relevant people to think about the process of an unimaginable threat situation.

Study on the fictive CBRN terrorist case concerning an air passenger flight has put the spotlight on the vulnerability of the transportation system and aviation industry as a whole that is in many connections considered high risk area for terrorism. Despite of the mechanisms and instruments developed to counter-terrorism, if they are never activated, one can only speculate on their functioning. It is a known fact that asymmetric threats will continue to be a challenge for the present and future EU decision-makers. EU has now established a framework of agreement to concretize its solidarity and political support and in addition has the operational bodies to implement the political decisions. Now, the member states must be convinced to start using this new model.

When it comes to the Aether project and the table-top exercise organized in its framework one can state the following: Crisis-like situations created in the minds of risk mapping experts and executed in the exercises can stimulate fast organizational learning if they are taken seriously enough. They will not give any precise and ready-made solutions since all crises differ

69) An example is the upcoming Barents Rescue 2011 exercise in Sweden, where the backbone of the intergovernmental cooperation is still on bilateral and multilateral agreements instead of EU level action.

but they will start a process of familiarizing one to think in a crisis-like situation where decisions are needed to be made under stressful conditions. Exercises should not be done only to get successful results but to challenge the already created and approved models and processes, and to learn by doing, sometimes even from mistakes.

The European Union counter-terrorism is first of all a *process*, which is evolving, even as we speak. Communications, proposals for action plans etc. are being drafted constantly and framework decisions are waiting to be adopted or have already been adopted[70]. The direction of the EU's counter-terrorism is going for a more concrete and pragmatic course with different mechanisms and arrangements.

Almost all of these instruments, legislative or operational, demonstrate and reflect the level of cooperation, integration and confidence that exists between member states in order to counter terrorism ever more efficiently. However, in order to *know* about the actual effectiveness, adequacy and possible gaps of these instruments something must happen. One only gets the answer post-factum of a crisis i.e. *after* something has happened. This of course is not sought-after. Instead the aim is to get the answers *before* something happens. The bodies, mechanisms and instruments should be *tested*.

Here the usefulness of the applied research, public-private exercises and hypothetical scenarios supported by "outsiders" objective evaluation comes into the picture. It is the most effective way to compel the process to stop for a while and think "out of the box". How the EU CCA, counter-terrorism instruments and mechanisms would act during a terrorist strike and whether the arrangements would allow a rapid and flexible response, will be examined in the following articles using the Project Aether scenario as a case study.

Bibliography

- ✓ Boin, Ekengren & Rhinard (2006): Functional Security and Crisis Management Capacity in the European Union. Swedish National Defence College. Elanders, Vällingby.
- ✓ Boin,'t Hart, Stern & Sundelius (2005): The Politics of Crisis Management. Public Leadership under Pressure. Cambridge University Press. New York.
- ✓ Brändström, Bynander & 't Hart (2004): Governing by Looking Back: Historical Analogies and Crisis Management, Public Administration. Vol. 82 No. 1, 191-210.

70) The list here serves to illustrate the process nature of the EU-CT and gives examples of various documents. Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism (COM (2007) 681 final), Annex to the report (SEC (2007) 1463), Communication from the Commission to the European Parliament and the Council - Stepping up the fight against terrorism (COM (2007) 649 final), Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism (COM (2007) 650 final), Communication from the Commission to the European Parliament and the Council on enhancing the security of explosives (COM (2007) 651 final) , Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes (COM (2007) 654 final).

✓ COM (2005) 313 final, Terrorist recruitment: addressing the factors contributing to violent Radicalisation, adopted on 21st September 2005, Action Plan on Radicalisation and Recruitment (December 2005).

✓ COM (2005) 662 final, Commission provisions on "ARGUS" general rapid alert system.

✓ COM (2006) 786 final, Communication from the Commission on a European Programme for Critical Infrastructure Protection.

✓ COM (2007) 649 final, Communication from the Commission to the European Parliament and the Council - Stepping up the fight against terrorism.

✓ COM (2007) 650 final, A proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism.

✓ COM (2007) 651 final, Communication from the Commission to the European Parliament and the Council on enhancing the security of explosives.

✓ COM (2007) 654 final, Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes.

✓ COM (2007) 681, Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism, Annex to the report (SEC (2007) 1463),

✓ Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, SN 140/01 www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/140.en.pdf

✓ Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions (2001/792/EC, Euratom).

✓ Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism (recast) (2007/779/EC, Euratom).

✓ Council Declaration on Combating Terrorism, contained also the Declaration on Solidarity against terrorism, 25 March 2004, 7906/04.

✓ Council Declaration condemning the terrorist attacks on London. JHA Council Declaration of 13 July 2005.

✓ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

✓ Council of the European Union: The European Union Counter-Terrorism Strategy. Justice and Home Affairs Council meeting, Brussels 1 December 2005.

✓ Crisis Coordination Arrangements, 1 July 2006, approved by the JHA Council.

✓ EU emergency and crisis co-ordination arrangements. consilium.europa.eu/uedocs/cmsUpload/WEB15106.pdf

✓ Eurojust: The European Union's Judicial Cooperation Unit, http://eurojust.europa.eu/

✓ European Commission (2007): Eurobarometer 68 Public Opinion in the EU/ Autumn 2007, Publication December 2007.

✓ Europol: European Police Office, European Law Enforcement Cooperation. http://www.europol.europa.eu/

✓ European civil protection, the Community Mechanism for Civil Protection, http://ec.europa.eu/environment/civil/prote/mechanism.htm

✓ European Union Counter-Terrorism Strategy, 30 November 2005, 14469/4/05 REV 4.

✓ European Council (2003): European Security Strategy – A Secure Europe in a Better World. Approved by the European Council held in Brussels on 12 December 2003 and drafted under the responsibilities of the EU High Representative Javier Solana.

✓ Galera-Lindblom, Patrick – Henriksson, Anu and Lange, Stefanie," The Early Warning System against Terrorism Attacks on the Ferry Traffic in Sweden" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Government Communications in Crisis Situations and Emergencies, Prime Minister's Office Publications 20/2008. Orig. Valtionhallinnon viestintä kriisitilanteissa ja poikkeusoloissa. Valtioneuvoston kanslia 10.9.2007. Valtioneuvoston kanslian julkaisusarja 15/2007.

✓ The Hague Programme: strengthening freedom, security and justice in the European Union (13 December 2004, 16054/04

✓ The Hague Programme – Ten priorities for the next five years, 10 May 2005. http://ec.europa.eu/justice_home/news/information_dossiers/the_hague_priorities/index_en.htm

✓ Hallituksen esitys Eduskunnalle valmiuslaiksi ja eräiksi siihen liittyviksi laeiksi. HE 3/2008 vp.

✓ Härkönen, Timo, Kriisijohtamismalli ja tilannekuva (Crisis management model and situation picture) PM, 14. 4.2008

✓ Härkönen, Timo, Tilannekuvatoiminta, valmiuspäälliköt, PM, Valtioneuvoston kanslia 7.3.2008.

✓ Kjellén, Sanna, Survey of EU warning systems (revised version). Krisberedskapsmyndigheten 2007-09-05.

✓ Kervinen Ossi (2001): Euroopan Unionin kriisinhallintatoimien päätöksenteko: Rakenteet ja toimintamahdollisuudet. Strategian Laitos. Julkaisusarja 2, No 12. Helsinki.

✓ Kokonaismaanpuolustuksen yhteensovittamisen strategia. Puolustusministeriö 2007.

✓ Kokonaismaanpuolustus (Total national defence). PM Turvallisuus- ja puolustusasiain komitea, Helsinki 15.4.2008.

✓ Kuusela, Anssi – Visuri, Pekka – Hellenberg, Timo, Pelastustoimen tietovirrat erityistilanteissa. Analyysi pelastustoimen ja valtion keskushallinnon välisistä tietovirroista YETT-strategian mukaisissa erityistilanteissa. Pelastusopiston julkaisu, B-sarja 2/2010.

✓ Larsson S, Olsson E-K. and Ramberg B. (Eds.) (2005): Crisis Decision-Making in the European Union, CRiSMART, Stockholm.

✓ Mikkonen, Anna, Valtioneuvoston tilannetietoisuuden muodostuminen lentoliikenteeseen kohdistuvassa CBRN-terrori-iskussa, Aether-projektin työpaperi (Working paper in Project Aether) November 2009.

✓ Monar Jörg (2007): Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and its Problems. Government and Opposition, Vol. 42, No. 3, pp. 292-313.

✓ Natural disaster in Asia on 26 December, 2004. Investigation report A2/2004 Y, Helsinki 2005.

✓ Nikula, Piia - Hellenberg, Timo, "EU crisis coordination arrangements and decision-making" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Parmes, Rauli (toim.), Varautumisen käsikirja. Tietosanoma, Helsinki 2007.

✓ Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Pursiainen, Christer – Hellenberg, Timo – Kivelä, Hanna-Mari, Puolustusvoimat ja sisäinen turvallisuus, Aleksanteri Papers 2:2004, Helsinki 2004.

✓ Rescue Services Strategy 2015. Ministry of the Interior publications 14/2008.

✓ Riskien hallinta Suomessa. Esiselvitys. Sitra, Helsinki 2002.

✓ Richardson Jeremy (ed.) (2006): European Union: power and policy-making. 3rd edition. Routledge research in European public policy. Abingdon.

✓ Ryter Marc-André (2002): Managing Contemporary Crises: A Challenge for the European Union. Department of Strategic and Defence Studies. Series 2, No 18. Helsinki.

✓ Safety first. Internal security Programme. Government plenary session 8 May 2008. Publications of the Ministry of the Interior 25/2008. (Orig. Turvallinen elämä jokaiselle. Sisäisen turvallisuuden ohjelma. Sisäasiainministeriön julkaisuja 16/2008).

✓ Sipilä Joona & Mikkola Erko (2004): Terrorism and counter-terrorism. Impact on Defence and other Security Systems. Department of Strategic and Defence Studies. Series 2, No 25. Helsinki.

✓ The Strategy for Securing the Functions Vital to Society. Government Resolution 23.11.2006.

✓ Tampere European Council 15-16 October, Presidency Conclusions. , http://europa.eu/european-council/index_en.htm

✓ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 2007/C 306/01.

✓ United Nations (2001): Security Council Resolution 1373, 28 September 2001.

✓ United Nations (2005): Security Council Resolution 1624, 14 September 2005.

✓ United Nations (2006): Global Counter-Terrorism Strategy, 8 September 2006.

✓ Valtioneuvoston asetus (Government decree) 7.6.2007 valtioiden rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehdyn sopimuksen (ns. Prümin sopimus) voimaansaattamisesta.

✓ Visuri, Pekka – Hellenberg, Timo, "Finnish crisis decision making system, cooperation of authorities and communications" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Zimmermann Doron (2006): Terrorist Threats, the European Union and Counter-Terrorism. Study Group on the Economics of Terrorism, ppt. 25 May 2006. Center for Security Studies. Swiss Federal Institute of Technology (ETH Zürich).

Magnus Normark: Understanding CBRN Terrorism Threat - An Overall Assessment

1. Introduction

✓ *1.1 The General Trend of Concern*

> *"The Commission believes that unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013".*

The threat from terrorism has evolved and changed shape through decades. One of the prevalent landmarks manifesting this evolution of the terrorism threat is the hijacking of the Israeli El Al Airways flight from Rome to Tel Aviv on 22 July 1968. This attack was performed by the Palestinian leftist movement Popular Front for the Liberation of Palestine (PFLP) and is referred to as one of the first terror attacks directed against targets in the international arena as an attempt to leverage the impact towards achieving their goals. The event marked the start of a wave of civil aviation hijackings for political purposes.

Other significant events that have impacted the evolving threat from terrorism are the demise of the Soviet Union and the end of the Cold War, resulting in the decrease of direct and indirect support and financing to organisations promoting acts of terrorism in conflict-laden areas where the superpowers were competing for influence. With the loss of financiers these groups had to adapt their organisation and activities in order to find alternative sources of support, which drove them in the direction of less hierarchical and more network-based structures and interactions. With this change of conditions these organisations using terrorism had to change their goals and ideology, becoming more long-term and broader in scope in order to attract and align with other groups and individuals. The emergence of long term strategies and goals became the driver for creating the diffuse and loose structures of actors leading to the dimensioning threat from the new form of terrorism that has shaped many countries' security policy during the last decade.

The fear that terrorists' objectives include an effort to escalate the impact of every attack, and their consequent striving for developing methods and acquiring means to do so, has further enlarged the scope of the terrorism threat. This was especially true during the period following the 11 September 2001 attacks in the United States and the subsequent anthrax laced letters sent to politicians and media representatives. These terrorist events had a tremendous impact on threat perceptions, especially in the West, due to the innovative methods and means used to attack Western urban societies with far reaching consequences in terms of number of

victims, negative socioeconomic effects and psychological impacts, leading to an increased sense of insecurity.

In the wake of these attacks many "experts on terrorism" as well as governmental institutions and authorities expressed their perceptions that if terrorists are capable of these attacks they would not hesitate to deploy weapons of mass destruction (WMD), should they be able to acquire such weapons. Another increasing fear was that al-Qaeda central were motivated and sought to escalate the level of violence and effects in terms of destruction and casualties in their continued planning of future attacks. Thus the fear of the event where the world's most dangerous actors will acquire and use the world's most destructive weapons became the most pressing scenario and the dimensional factor for many of the Western countries' evolving foreign and security policy.

✓ *1.2 Objectives*

This article seeks to assess the prospects of terrorist actors to pursue, acquire and use CBRN agents in terrorist attacks based on past incidents and other indications of intent and capabilities. The potential CBRN terrorism threat towards the civil passenger aviation sector will also be elaborated on in the light of the CBRN terrorism threat in general.

✓ *1.3 Methodology*

This study is primarily based on a literature review. Making an assessment of a potential threat based on open sources has its caveats as it is very likely that there are planned incidents that have been aborted as a result of effective intelligence and law enforcement interventions that never surfaced in the media or in other public documents. Furthermore, an assessment solely based on reports from media, government institutions, think tanks and academic institutions may include references to incidents of dubious character and information that cannot be confirmed or evaluated to any satisfactory degree. For these reasons, this assessment cannot be considered an all-encompassing and comprehensive evaluation of the current or future threat capturing all the relevant details, but should rather be seen as a contributing perspective.

✓ *1.4 Definitions and Limitations*

As the prioritized goal of this project is focused on the handling of a CBRN-incident against the international civil aviation sector, disregarding the scale of potential consequences, this study will apply a fairly broad definition of the term "CBRN-terrorism". We are using the term CBRN-terrorism in this study to take into account all uses of violence or the threat to use violence through means involving chemical, biological, radiological or nuclear agents or substances, conducted by non-state actors motivated by political objectives. We thus avoid using the term "weapons of mass destruction" (WMD) as this has to a large extent become a political one with a negative appellation, especially after the US justification for the attack on Iraq in 2003. In general, the term WMD often refers to classical chemical, biological and nuclear agents and materials, weaponized through some form of militarily significant carrier system which, for the most part, is in the hands of so-called "rogue states". As such, the term "WMD" does not distinguish enough between the vast spectrum of different technical aspects that exists within this category of violent means and methods.

Furthermore, the limited scope of this study and the related issues of threat perspectives included in other studies within this project have lead to a limited elaboration on radiological and nuclear-related strands of the problem.

✓ *1.5 Outline*

In the introductory chapter the scope of the study is described with stated objective, applied methodologies, definitions and limitations. In the second chapter this study will explore different expressions of CBRN terrorism threat perceptions of recent date and the foremost factors shaping these perceptions. Furthermore the very few known and confirmed incidents of CBRN-terrorism, both large-scale and small-scale eve entives that may influence and shape a terrorist's relation to these unconventional methods of violent means in the future are discussed.

2. Terrorism and Chemical, Biological, Radiological and Nuclear Material

The most destructive and high impact terrorist events have thus far been carried out using explosives, small arms or means other than dangerous substances such as toxins, chemicals, pathogens or radiological materials. To date there has been no act of CBRN-terrorism that has caused mass casualties or resulted in catastrophic consequences. However, this fact does not suggest that this category of actors has not tried to acquire necessary capabilities in order to perform such attacks, but simply that they have not been very successful in their attempts for various reasons.

✓ *2.1 CBRN Terrorism and Threat Perceptions*

Weapons of mass destruction have been a source of concern for the international community since the 1940s. On 24 January 1946 the very first resolution adopted by the United Nations General Assembly on the issue of WMD pushed for "the elimination from national armaments of atomic weapons and of all other major weapons adaptable to mass destruction". Since then there has been a wide range of resolutions from the Security Council on issues related to proliferation of WMD and also on the issue of fighting acts of terrorism. However, one of the first UN Security Council resolutions acknowledging the threat of convergence between WMD and terrorism was in resolution 1373 of 28 September 2001, as a response to the 9/11-attacks in the US. The increased fear of terrorists' potential intentions and capacities to use CBRN as weapons in violent attacks resulted in UNSCR 1540 from April 2004 which states that the Security Council is:

> *"…Gravely concerned by the threat of terrorism and the risk that non-State actors /…/ may acquire, develop, traffic in or use nuclear, chemical and biological weapons and their means of delivery."*

This expression of increased fear of CBRN-terrorism through the only institution in the world with a legal authority to harmonize and if necessary enforce measures to counter CBRN-terrorism as a threat to international peace and security is naturally an expression of the member states' growing fear. It also shows that CBRN-terrorism has never been high enough on the international agenda to merit a sentence in a UN resolution before the 9/11-terror events. This becomes even more underscored looking at the European Union's perceptions and actions based on the concern of the potential terrorist use of CBRN-agents and materials.

Before the 9/11-events the European Union did not have a specific strategy in countering the acquisition and use of CBRN by terrorists for malicious intent. As a matter of fact, the European Union's work against the spread of weapons of mass destruction had not been shaped by a coherent and long term strategy before December 2003 when the EU strategy against proliferation of weapons of mass destruction was adopted.[1] The first counter terrorism strategy that mentioned the threat of CBRN terrorism and terrorist use of non-conventional weapons was adopted by the EU council on 30 November 2005.[2] However, the 9/11 terrorism events in the United States initiated a debate regarding the concern for CBRN-terrorism, consequently during the Heads of States and Governments informal EU Council meeting in Ghent on 19 October 2001 a declaration was issued for the first time regarding the growing concern of CBRN-terrorism which stated that:

> *"The European Council has examined the threats of the use of biological and chemical means in terrorist operations. These call for adopted responses on the part of each Member State and of the European Union as a whole".*[3]

The Ghent meeting resulted in the adoption of a programme to improve cooperation in the EU for preventing and limiting the consequences of chemical, biological, radiological and nuclear terrorism threats.[4] This became the starting point for the increasing focus on the issues that have evolved in several updated and new strategies and action plans on countering terrorism and the spread of WMD within the European community. The EU actions and expression of concern regarding CBRN-terrorism is foremost linked to three different policy areas: external trade (export control on dual-use goods), foreign and security policy (terrorism) and public health (disease prevention and control). Despite the fact that CBRN-terrorism has yet to occur within Europe, the general concern surrounding such events is regularly raised in various documents produced within these policy areas.

Today, EU activities to detect and prevent CBRN-terrorism are foremost manifested through the CBRN action plan, adopted by the Commission in June 2009, which is based on the finding of a CBRN Task Force established by the Commission in February 2008. The action plan is designed to support the implementation of the counter-terrorism strategy and is focused on all the different strands of the CT-work (prevention, detection, preparedness and response).[5]

Of all the publicly available assessments of the terrorism threat from governments most concerned, none express any knowledge of existing terrorist groups with sufficient capabilities

1) European Council decision 15708/03 on the Fight against the proliferation of weapons of mass destruction.

2) European Council 14469/4/05, REV4 on the European Union Counter-Terrorism Strategy.

3) Declaration by the Heads of States or Government of the European Union and the President of the Commission SN 4296/01; Follow-up to the September 11 attacks and the fight against terrorism.

4) European Council, 14627/02, Adoption of the programme to improve cooperation in the EU for preventing and limiting the consequences of Chemical, biological, radiological and nuclear terrorism threats.

5) European Council, 11480/09 - COM(2009) 273, Accompanying document to the communication to the document from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and nuclear Security in the European Union – an EU CBRN Action Plan.

to perform a high impact CBRN-terrorism attack. Despite the absence of indications that contemporary terrorists have such capabilities the fear of such events has been considerably high, especially during the last eight years. What then lies behind these fears and perceptions of the CBRN-terrorism threat? There have been several publicly available assessments of this threat from governments, and international committees of which I will comment on a few in order to highlight some of the underlying causes for concern.

As the country most regularly mentioned as a prioritized target by international terrorists, the United States of America is one of the world's governments that has expressed most concern of the threat from terrorist acquisition and use of CBRN-weapons. This has been highlighted by a range of threat assessments from the US intelligence community and one of the latest is the Annual Threat Assessment by the Director of National Intelligence (DNI), Dennis C. Blair, released 3 February 2010. These annual threat assessments are shaped and tuned from one year to the other by recent experiences like, for instance, outbreaks of pandemics, financial crises, and cyber threats, but the threat from terrorists has remained one of the biggest challenges to US homeland security and safety. In this recent statement the DNI acknowledged that the traditional WMD use by most nation states has been constrained by various countermeasures, but at the same time the threat of proliferation is growing due to the difficulties in using these countermeasures to prevent the use of "mass-effect weapons" by terrorist groups. Despite the statement that there are no corroborated reports indicating that any terrorist group has advanced its CBRN-capabilities, the DNI expresses the continued concern over the potential for terrorists to gain access to WMD-related materials or technology. [6]

> *"We cannot rule out that al-Qa'ida's interest in damaging the US economy might lead the group to opt for more modest, even "low-tech," but still high-impact, attacks affecting key economic sectors."*[7]

Another American expression of the CBRN-terrorism threat is highlighted by the report World at Risk, released in December 2008 by the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism. This commission, which was created in accordance with the implementing recommendations from the 9/11 Commission Act of 2007, had a mandate to examine the threats posed to the United States by WMD proliferation and terrorism in a world that has been changed forever by the forces of globalization.[8] This report states that it is more likely than not that WMD will be used in a terror-attack somewhere in the world before the end of 2013 and that the threat from CBRN-terrorism is increasing at a faster pace than all efforts made in the US and internationally to counter it, leading to the net assessment that the margin of safety is shrinking, not growing.

This assessment of the threat is not a result of a traditional probability assessment based

6) Dennis C. Blair, Director of National Intelligence, 2010, *Annual Threat Assessment for the US Intelligence Community for the House Permanent Select Committee on Intelligence, February 2, 2010.*

7) Dennis C. Blair, Director of National Intelligence, 2010, *Annual Threat Assessment for the US Intelligence Community for the House Permanent Select Committee on Intelligence, February 2, 2010.*

8) *World at Risk; The Report of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism*, 2008, New York USA, Vintage Books.

on the product of intention and capabilities of actors of concern. In a world where these actors are vague, given that there are only a few examples of terrorist acquisition and attempted use of CBRN-weapons, the impact of globalization has become the dimensioning factor for the final assessment.

> *"In today's world, individuals anywhere on the planet connect instantly with one another and with information. Money is moved, transactions are made, information is shared, instructions are issued, and attacks are unleashed with a keystroke. Weapons of tremendous destructive capability can be developed or acquired by those without access to an industrial base or even an economic base of any kind, and those weapons can be used to kill thousands of people and disrupt vital financial, communications, and transportation systems, which are easy to attack and hard to defend. All these factors have made nation-states less powerful and more vulnerable relative to the terrorists, who have no national base to defend and who therefore cannot be deterred through traditional means."*

Throughout this chapter it has been obvious that the threat perceptions regarding the potential acquisition and use of CBRN-materials by terrorists are profoundly international. From the above we can conclude that the perceptions of this threat are foremost based on three aspects:

- the indications of terrorists growing interest in CBRN-materials for terrorist attacks;
- the decreasing thresholds for these actors to acquire or to access necessary knowledge, substances and equipment through the impact of globalization and;
- the potential consequences should CBRN-materials be utilized in an effective manner by terrorists in future attacks against modern civil societies.

✓ *2.2 Past CBRN Terrorism Efforts and Attacks*

What then is the current knowledge of terrorists' acquisition and use of CBRN-substances and materials in terrorist attacks? It is often stated that contemporary terrorists are agile actors exploiting global information technology and commercial infrastructure for their violent purposes, and are adaptive to the countermeasures put in place to prevent and disrupt their activities as early as possible. Much of this work is done by national intelligence and security agencies, and if their efforts are successful it is seldom disclosed to the public. This fact makes it somewhat difficult to identify what events and experiences have shaped national threat assessments in this area. However, there are a few incidents most often cited in the assessment of the CBRN-terrorism threat by governments, international organizations and academic scholars.

The history of bioterrorism events has by some researchers been dated back to the Middle ages and the 1346 sieges at Kaffa on the Crimean coast in what is today Ukraine, where the bodies of plague victims were hurled over the walls of the besieged city.[9] However contemporary terrorist efforts to use CBRN material as a weapon in an attack known publicly are very few indeed.

9) Kantona P. Intrilligator M.D. and Sullivan J.P., 2006, Countering Terrorism and WMD; Creating a global counter-terrorism network, Routledge, UK, p 18.

2.2.1 The Tamil Tigers and Chemical Warfare

The separatist terrorist group Liberation Tigers of Tamil Eelam (LTTE) was among the most innovative of contemporary terrorist organizations using new means and methods in their attacks against the Sri Lankan regime. In 1986 LTTE used potassium cyanide to contaminate tea crops in an attempt to harm Sri Lankan tea exports, which was a vital area of income for the state. Four years later the LTTE used a cylinder filled with chlorine gas as a chemical agent against a Sri Lankan army camp in Kiran. Sri Lankan forces stated that 20 soldiers had become seriously ill in the attack. This method was later copied by Al Qaida in Iraq in a series of 15 attacks in the Baghdad area between October 2006 and June 2007.

The allegations of the use by LTTE of dangerous materials in their struggle continued to flourish in media from the Sri Lankan regime up until the last year of fighting before LTTE was defeated in May 2009. These statements were often fuelled by rhetoric from LTTE regarding their capabilities in using chemical weapons.[10] There is however no confirmed information of LTTE chemical attacks that has resulted in fatalities or any significant negative consequences.

2.2.2 The Rajneeshee Sect – Bioterrorism in the United States

The religious Rajneeshee sect, having established an isolated community of their own in Dalles, Oregon, USA, aimed at leveraging their influence in Wasco County by nominating sect members in the upcoming election. This effort was initiated due to an increasing number of disputes and escalating tension between the sect and the citizens. As a measure to increase the sect's chances of getting enough votes, a plan for using Salmonella typhimurium as a biological weapon to incapacitate local voters was created. This event became the first known bio-terror attack in the US, resulting in 751 confirmed illnesses, including 45 who were hospitalized. The sect's biological weapon capabilities were created by a nurse and a trained laboratory technician who cultured the Salmonella used to contaminate salad bars in local restaurants.[11] The seed stock of Salmonella was legally purchased from a medical supply company by the Rajneeshee's state certified clinical laboratory. It is interesting to note that the sect's activity to produce biological agents for offensive use, which also included efforts to contaminate food with Shigella, became known only when defectors from the sect started to inform law enforcement agencies a year and a half after the attacks. In fact, an Oregon state official issued a report claiming that unsanitary practices by restaurant workers caused the outbreak and dismissed allegations that intentional contamination was a factor. Furthermore, bioterrorism never became a debated issue or a growing concern nationally as a consequence of Rajneeshee's use of pathogens against citizens in Wasco County.

2.2.3 Aum Shinrikyo's WMD Programs

The Japanese Aum Shinrikyo sect, known for the sarin gas attacks in Matsomoto in

10) "LTTE to acquire shortly chemical weapons", *Asian tribune,* 25 August 2007 and "Sri Lanka Govt. prepares for LTTe chemical attack", *LankaNewspapers.com*, 17 September 2008.

11) Carus S. "The Rajneeshees (1984)" In: J. B. Tucker ed. *Toxic Terror: Assessing Terrorists Use of Chemical and Biological Weapons*, USA, 2001.

1994 and in a Tokyo subway station in March 1995, was unique in their efforts to pursue a full scale WMD-program from the early 1990s. The sect, led by the notorious charismatic leader Shoko Asahara, is the only non-state actor that had the support and resources to acquire and produce military grade chemical agents and to pursue an ambitious attempt to produce biological warfare agents such as Bacillus anthracis (Ba) and Botulinum toxins. Within the course of eight years the sect had recruited approximately 10,000 members in Japan, 30,000 in Russia, and hundreds of millions of dollars in assets and offices in Germany, Taiwan, Sri Lanka, Australia, and the United States.[12] There are indications of efforts to disperse Ba in Tokyo and in other cities in Japan between 1990 and late 1993. These efforts failed due to the fact that the individual running the biological weapons program was a virologist, lacking the important knowledge to acquire the proper pathogens. The anthrax strain acquired by Aum was a vaccine strain and therefore not harmful to humans.

In July 1993, a liquid suspension of Bacillus anthracis vaccine strain was aerosolized from the roof of an eight-story building in Kameido, Tokyo, Japan, by the religious group Aum Shinrikyo. (Photographs taken July 1, 1993, by the Department of Environment, Koto-ward). [2/11/2009]

In parallel to Aum's efforts on the biological side, the sect also bought properties in Australia where a geologist had indicated a deposit of natural uranium oxide. Aum initiated research efforts on uranium extraction and enrichment technologies with the aim of producing nuclear weapons. However, the effort was abandoned when it became clear that this was beyond their capabilities, despite their excellent funding and broad support. With failed bioweapon and nuclear programs Aum started to focus on the chemical track of their WMD ambitions, which became the sect's most successful effort. A large scale production facility to produce the nerve gas sarin was built based on information from the Russian CW-program. Large quantities of high grade sarin was produced but later disposed of by the sect when information was leaked to the press of the sect's suspicious behaviour. Aum received information of a planned police raid against its headquarters on 22 March. This became the trigger for carrying out the Tokyo subway attack on 21 March 1995, launched with a very short lead time in an effort to target police officers on their way to the police headquarters located in the intersection between the targeted subway lines. The attack resulted in 12 dead and more than 5500 people in need of or seeking medical care for symptoms of nerve gas exposure.[13]

12) Furukawa K. and Parachini J.V. "Japan and Aum Shinrikyo" In: Art R.J. and Richardson L. ed. *Democracy and Counterterrorism: Lessons from the past*, Endowment of the United States Institute of Peace, USA 2007.

13) Furukawa K. and Parachini J.V. "Japan and Aum Shinrikyo" In: Art R.J. and Richardson L. ed. *Democracy and Counterterrorism: Lessons from the past*, Endowment of the United States Institute of Peace, USA 2007.

2.2.4 Al Qaida and CBRN Weapons

> *"Acquiring weapons for the defense of Muslims is a religious duty. If I have indeed acquired these weapons, then I thank God for enabling me to do so. And if I seek to acquire these weapons, I am carrying out a duty. It would be a sin for Muslims not to try to possess the weapons that would prevent the infidels from inflicting harm on Muslims."* [14]

Other efforts of acquiring and launching large-scale WMD-programs include activities initiated by Al Qaida central. Beside the various statements and rhetoric by leading figures in AQ central and affiliated organisations worldwide indicating their intentions and obligations to acquire such a capability, a specific effort was launched in Kandahar outside Kabul, Afghanistan in the late 1990s. The person often described as Usama bin Laden's "lieutenant" or "the real brains of Al Qaida", Dr Ayman al-Zawahiri, recruited two individuals with specific biological knowledge for the task of acquiring material and equipment in order to construct a bioweapons laboratory. The two individuals were the Pakistani microbiologist Abdur Rauf, a specialist in food production with the prestigious Pakistan Council of Scientific and Industrial Research in Lahore, and the Malaysian Yazid Sufaat, who held a degree in biochemistry from California State University and had links to the Indonesia-based terrorist organisation Jemaah Islamiya. After the Allied forces' invasion of Afghanistan in October 2001 various equipment, documents and literature on biological warfare agents such as anthrax were found at the site in Kandahar. The extent and sophistication of the equipment in the "laboratory" is unknown but it was apparently not in operative use. Furthermore correspondence between Zawahiri and Rauf discussing the latter's attempts to acquire biological agents in Great Britain for the biological weapons program was discovered. Through this correspondence it appears as if Rauf was unsuccessful in acquiring pathogenic strains of Ba or other potent pathogens. One possible explanation for the lack of success for this effort may be the poor funding for Rauf's activities, which he complained about in his correspondence with Dr Zawahiri.[15]

There are a large number of allegations and indications of al Qaida and their associated organisations' efforts and commitment to acquire a CBRN warfare capability. Many of these have been difficult to verify and a large number of them seem to be highly unlikely. However, Usama bin Laden's business agent during the Afghanistan war, Jamal Ahmad al-Fadl, who turned himself in to US Authorities in 1996, have made credible assertions that bin Laden on at least one occasion spent $1.5 million in an effort to purchase weapons grade uranium from a Sudanese military officer for a nuclear device. It turned out that al Qaida had been scammed in their quest to acquire a capability to develop a nuclear device. [16]

> *"We judge that, if al-Qa'ida develops chemical, biological, radiological, or nuclear (CBRN) capabilities and has operatives trained to use them, it will do so. Counter-*

14) Rahimullah Yusufzai, 1999. Conversation with Terror, *TIME* , January 11, 1999. A statement by Osama bin Laden in December 1998 as a response to the journalist stating that "The U.S. says you are trying to acquire chemical and nuclear weapons".

15) Leitenberg M., 2005. *Assessing the Biological Weapons and Bioterrorism Threat*, Strategic Studies Institute, U.S. Army War College, USA, pp. 28-42.

16) National Commission on Terrorist Attacks upon the United States, 2004. *The 9/11 Commission Report,* Official Government Edition, Washington DC USA.

> *terrorism actions have dealt a significant blow to al-Qa'ida's near-term efforts to develop a sophisticated CBRN attack capability, although we judge the group is still intent on its acquisition."* [17]

During a short period between the summer of 2006 and spring 2007 a group affiliated to al Qaida central performed a series of at least 14 attacks in urban areas where chlorine tanks where combined with improvised explosive devices. These chlorine attacks were generally seen as a trend in the terrorist group broadening its violent means and methods by including low technology attacks with dangerous materials against unprotected civilians in urban cities. However, the effect in using improvised explosive devices (IED) with chlorine tanks didn't in any significant way increase the effect in terms of more fatalities and through increased security of handling chlorine in Iraq this kind of attack soon disappeared.

2.2.5 Past Incidents – Illuminating the Thresholds and Bottlenecks

There are no solid indications of activities to acquire, produce or use CBRN-materials for large scale attacks from AQ central since the Kandahar efforts in late 2001. Fatwas have been issued legitimating the use of WMD in the Jihadi quest, so-called CBRN-manuals have been frequent on radical Islamic websites (none of any practical use for production of CBRN-weapons) and statements from terrorist groups have been issued declaring their intent or capabilities in using chemical and biological weapons. It is however obvious from these attempts and indications of intent that pursuing an advanced program to produce CBRN-weapons is extremely difficult, even for a doomsday sect, isolated from the rest of society with competent personnel, respectable facilities, equipment and good finances like Aum Shinrikyo.[18]

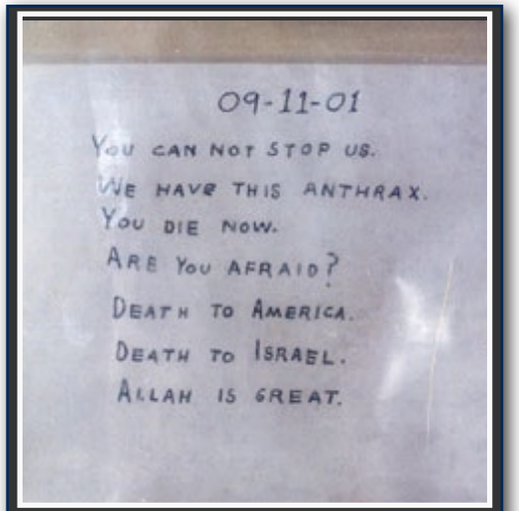
There are a number of thresholds and bottlenecks that have severely restricted these actors from successfully acquiring and using CBRN-materials in terror attacks with catastrophic consequences. These limitations include the difficulties in acquiring the dangerous substances, the knowledge required to successfully develop and produce the agent of choice and the vital challenge of distributing the agents to the target in an efficient manner.

The risk of terrorists acquiring the materials and technology to produce WMD constitutes a dilemma that from the 1990s has been a priority within western governments' security policy agendas. During the 1990s the key equipment and technology to pursue these kinds of weapons was foremost in the hands of western governments, which made the prospects of controlling the export of such items fairly possible. However, since the early 2000s it has become clear that controlling the trade with dual-use items has become increasingly difficult, especially in regards to non-state actors of concern. One of the most prevalent factors often mentioned as a driver for terrorists to complement traditional means of terrorist attacks with innovative new methods and modus operandi is globalisation and its consequences. Globalisation has become a buzz-word in various assessments of terrorists' near-future capabilities and opportunities, in some cases stating that advanced technology and knowledge is becoming available to any-

17) Dennis C. Blair, Director of National Intelligence, 2010, *Annual Threat Assessment for the US Intelligence Community for the House Permanent Select Committee on Intelligence, February 2, 2010*.

18) Ranstorp M. and Normark M ed. 2009. *Unconventional Weapons and International Terrorism; Challenges and New Approaches*, Routledge, London, UK, 2009, pp 195-204.

one, anywhere in the world. Despite these alarming assessments there are still no clear indications that contemporary terrorists are successful in taking advantage of this development by acquiring these materials for use in terrorist attacks.



Contents of letter tainted with anthrax sent to Sen. Tom Daschle.
Source: FBI Headline Archives, Amerithrax Case, 2008-06-08

The essential competence necessary for developing weapons with dangerous materials became evident in the context of the Amerithrax case in the United States in late 2001. Acquiring and developing Bacillus antracic (Ba) and other deadly pathogens as a weapon has been on the agenda for several terrorist groups including al Qaida and Aum Shinrikyo but have posed a too difficult challenge for them to master. The perceptions of the bioterrorism threat changed considerably when media persons and politicians in the US were targeted by at least five letters laced with very potent anthrax spores. The first set of letters was sent in September and a second wave again in October 2001 which resulted in five fatalities and 22 confirmed cases of anthrax. The Amerithrax investigation became one of the largest and most complex in the history of United States law enforcement and took 6 years before the Federal Bureau of Investigation (FBI) made public the name of the perpetrator behind the anthrax-letters. Speculation of probable terrorist actors behind these attacks was widespread and shifted in time, but it turned out that the perpetrator was not a known terrorist organisation but a researcher within the US bio-defence programme with long experience of handling these organisms and the equipment necessary to develop the agent in dry form and in sufficient quantities.[19] At the time of the incident the Ba strain used in the letters existed only in 15 laboratories in the US but only in liquid slurry form. Thus any perpetrator with the ambition to use dry Ba would have to know the right procedures and use the equipment necessary to dry the agent.

The revelation of the perpetrator behind the anthrax letters has contributed to a more nuanced threat perception of bioterrorism. The report "World at Risk" highlights their assessment of the bioterrorism threat by stating that …

> *"…given the high level of know-how needed to use disease as a weapon to cause mass casualties, the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists."*

There are differences between the various technology tracks regarding the required level of competence in relation to the prospects of being successful in using CBRN-materials in terrorist events. But it is all about varying levels of complexity and difficulties, and no technology track should be considered as easy if the goal is to achieve a high consequence terrorist attack. Not even the relatively simple method of using toxic chemicals in terrorist attacks has been fully mastered by any terrorist organisation, often limited to experience of using explosives and traditional terrorist methods. This became evident during al Qaida in Iraq's efforts in 2006/2007 to combine chlorine gas tanks with improvised explosives in the Baghdad area.

19) United States Department of Justice, 2010. *Amerithrax Investigative Summary*, USA.

Aum Shinrikyo's 1995 attack against the Tokyo Subway system is a very illuminating example of the importance of the method of distributing the chosen agent to the targets of the attack. Aum became very skilled in producing the nerve agent sarin in a very potent form but due to the choice of distribution, the Tokyo subway attack had a relatively low impact. The release of a potent nerve agent in closed facilities such as a subway train, filled with people during rush hour would be very effective if the goal is to kill many people. Aum performed five coordinated attacks of this kind on three different subway lines which had disastrous effects for the citizens of Tokyo that day, with 12 fatalities and 5500 seeking medical care.[20] However the primitive method of dispersion, using a sharp object to deflate a plastic bag filled with sarin placed on the floor of the train was a limiting factor for achieving a much higher number of fatalities.

The case of the Rajneeshee sect and the dissemination of Salmonella in restaurants is an illuminating example of simple means to create a substantial impact. The competence for this attack was based on a trained nurse and a laboratory technician who used the simple method of disseminating the pathogen into salad bars and salad dressing at restaurants. The consequences and the impact of that attack on the society as a whole would probably have been much higher if the outbreak of Salmonella would have been linked to a perpetrator with the capacity to continue to perform such attacks with the purpose of causing panic, fear and disorder.

✓ *2.3 Threats, Hoaxes and Low-level CBRN Incidents:*

Very few terrorists have an agenda where they have a priority on escalating the number of fatalities with each attack. There may often be other ways for these actors to maximize the impact of terror such as choice of target or simply sending a message through their activities, for example by using methods the public and the political leaders fear the most. This implies that ambitions of terrorists may not be of a large scale CBRN-weapon type but rather more simplistic and low-tech with the potential prospect of increasing the success rate of each attack and thereby escalating the impact on the target audience.

There are several organisations and institutes that register incidents of terrorism from open sources world wide. Two of the most renowned of these are the Global Terrorism Database 2 (GTD2), administrated by a DHS Center of Excellence (National Consortium for the Studies of Terrorism and Responses to Terrorism) based at the University of Maryland, USA and the World Incident Tracking System (WITS) administrated by the U.S. National Counter Terrorism Center (NCTC) in Washington.

GTD2 is currently the most comprehensive database of terrorism incidents with more than 80000 recorded cases covering the period of 1970-2008. The definition of terrorism has been changed from 1998 to the current wider definition which only includes incidents that are

20) Furukawa K. and Parachini J.V. "Japan and Aum Shinrikyo" In: Art R.J. and Richardson L. ed. *Democracy and Counterterrorism: Lessons from the past,* Endowment of the United States Institute of Peace, USA 2007.

"an intentional act of violence or threat of violence by a non-state actor". In addition two of the following three criteria have to be met for inclusion in the database:

1. The violent act was aimed at attaining a political, economic, religious, or social goal;
2. The violent act included evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) other than the immediate victims; and
3. The violent act was outside the precepts of International Humanitarian Law.

This definition is designed in order to be flexible to the shifting definitions of the term worldwide and thereby allow analysts and scholars flexibility in applying various definitions of terrorism to meet different operational needs.[21]

A search in the database of incidents where the threat or use of CBRN-materials has been included results in a total of 269 recorded incidents.[22] A large majority of these represent chemical related incidents with 220 hits. The range of incidents covers everything from Ku Klux Klan efforts to poison black Muslims with cyanide in the early 1970s to al Qaida in Iraq's efforts to combine chlorine gas with explosives in 2006/2007. Of all the recorded incidents where chemicals have been included a large majority resulted in no fatalities. In 29 incidents more than 10 casualties had been reported, a majority caused by a combination of other means and weapons where the toxic chemical most likely only had a minor effect or no effect at all. The category of targets for these attacks is to a large extent dominated by private citizens and properties, including a large number of anti-abortion related attacks where butyric acid had been used as an irritant. These anti-abortion related attacks escalated both in 1992 and again in 1998 in the US, causing no fatalities. Approximately 29% of the targets in these chemical-related attacks were government related such as diplomatic, military or police.

Of the 23 recorded incidents related to biological materials, 18 occurred in the US. Nine incidents were related to the Amerithrax case which resulted in 5 fatalities and 22 victims, of which 11 included inhalation anthrax and another 11 suffered cutaneous anthrax by absorbing it through the skin. In addition to the information in GTD2 it has been confirmed that another 31 people tested positive to exposure to anthrax spores and that ten thousand more people was deemed at risk from possible exposure.[23] Another four incidents are linked to the Rajneeshees dissemination of Salmonella in Wasco County in the mid 1980s. Three other recorded incidents in the United States, related to each other, include the use of ricin toxin as a weapon, distributed through letters to government representatives. Relatively substantial attention has been paid to the ricin toxin as a potential weapon for terrorists due to its high toxicity and that it is relatively easy to acquire and produce. Another reason for the attention paid to ricin has been the several cases where terrorists and non-state actors have been suspected of planning attacks with ricin toxin, but which turned out to be false or unconfirmed. These includes the London Wood Green ricin plot in 2002, former US vice president Cheney's allegations of ricin production for terrorism purposes at the Kermal Camp in Iraq and the alleged terrorist

21) National Consortium for the Study of Terrorism and Responses to Terrorism, 2009. *Data collection Methodology,* (online). Available at: http://www.start.umd.edu/gtd/using-gtd/, [accessed on 2009-11-02].

22) Search conducted in November 2009 using the following limitation: "Ambiguous cases excluded" and "only incidents where there is essentially no doubt of terrorism".

23) United States Department of Justice, 2010. *Amerithrax* Investigative Summary", USA.

ricin case at Gar de Lyon train station in Paris in March 2003. None of these three alleged "ricin cases" are registered in GTD2. All recorded incidents in GTD2 where biological agents were used as a weapon (from 1981 to 2005) have resulted in 9 fatalities and 800 injuries. Three of the Rajneeshee attacks in 1984 resulted in 778 of these 800 injuries. All but two fatalities occurred in the United States.

GTD2 also includes registered terrorist incidents in which radiological materials were used. A total of 15 incidents have been recorded of which 10 refer to a wave of letters with monazite sent to government offices in Tokyo, Japan in June 2000. The additional five incidents include materials found in Chechnya, in the United States, France and Austria. None of the incidents have resulted in any casualties.

The US NCTC's World Tracking Incident Database is a relatively new database currently covering incidents from January 2004 to December 2009, including 65,879 incidents. According to NCTC definition, terrorism occurs when groups or individuals acting on political motivation deliberately or recklessly attack civilians/non-combatants or their property (including military personnel and assets outside war zones and war-like settings) and the attack does not fall into another special category of political violence, such as crime, rioting, or tribal violence. Terrorists must have initiated and executed the attack for it to be included in the database; failed or foiled attacks, as well as hoaxes, are not included in the database. The information in WITS is based on open source reporting.[24] WITS thereby have a broader definition of incidents included in the database than GTD2. Twenty-eight incidents are recorded as CBRN-related (event type or weapon), 50% of these represent the attacks in Iraq where chlorine tanks where used in combination with explosives from 29 June 2006 to 13 June 2007. Three incidents included poisoning through toxic substances in food or drinks, including a Taliban attack against law enforcement and government employees in Nurestan, Afghanistan in September 2008. The attack resulted in 261 reported casualties. All fatalities and 75% of all wounded of WITS registered CBRN-related incidents are represented by the attacks in Iraq. Adding the casualties from the poisoning attack in Nurestan to the Iraqi casualties of CBRN-related attacks totals 98% of all casualties in the WITS database for these types of events.

These recorded incidents where some kind of CBRN-material has been included or CBRN-related facilities have been targeted in events relating to a broad definition of terrorism certainly indicate that there exists a broad segment of actors that view dangerous substances and materials as a useful tool in causing casualties, panic, fear and disorder. It is also clear that very few have had the means and competence to effectively plan and execute a CBRN-related attack with the potential of creating mass-casualties and catastrophic consequences. It should also be noted that these records from GTD2 and WITS of CBRN-related incidents should not be viewed as the full testimony of all events pursued or executed by terrorists. As stated previously in this report there are possibly a number of cases of CBRN-related attempts by terrorists that were in an early stage prevented by law enforcement and intelligence agencies that have been kept undisclosed to the public. Furthermore, incidents in these databases are based only on open source reports and thus reflect the ambiguous picture created by all the media reports of CBRN-materials and terrorists.

24) United States National Counterterrorism Center, *Worldwide Incident Tracking System*, Available at: http://wits-classic.nctc.gov/, [Accessed on 22 April 2010].

By these past events it's also possible to draw some conclusions regarding the terrorist actors inclined to use CBRN in causing fear and terror. Publications regarding CBRN-terrorism have to a very large extent been fixed on religious extremism and in particular on Al Qaida and its affiliated organisations worldwide. It is however clear by the few and often ineffective efforts of employing CBRN-materials in politically motivated attacks that there are a wide array of terrorist actors that have shown interest or tried to use these materials in the violent attacks, such as nationalist-separatist terrorists (Tamil Tigers), single issue groups (anti-abortion terrorists), right wing groups and radical religious fundamentalist groups. It is however possible to single out the religiously motivated terrorists from the others due to the potentially lesser constraints that this category of groups might experience in the undertaking of such attacks. While national separatist groups, right wing and single issue groups may be constrained to undertake an attack mode which causes mass-casualties, religious motivated cults and organisations like Aum Shinrikyo and Al Qaida seem to be less constrained. This conclusion is also supported by past studies on different terrorist organisations' propensities for large scale terrorist attacks.[25]

✓ *2.4 Some Technical Features of CBRN as a Weapon of Terror*

What then is relevant to focus on from a technical perspective in trying to frame the potential future use of CBRN materials by non-state actors? The evolution of technology within the medical, chemical engineering and biotechnology fields has long influenced the discussions and assessments of future threats. The concerns raised by the evolution of technology have strongly influenced the direction of many government CBRN-defense programmes. These research programmes develop in-depth knowledge for defence and protection against CBRN-weapons, but that knowledge could also be used for offensive purposes. Cutting edge defence research is conducted by highly competent scientists. To attribute the level of competence to non-state actors and thus the ability to carry out attacks that exploit such advanced technology is both excessive and unrealistic. It is more reasonable to assess the ability of these non-state actors based on the observed expression and indication of their competence level. In the case of bioterrorism, an individual could at "best", carry out a small-scale attack with an infectious agent that is possible to acquire, for example, contaminate muffins with Salmonella. A larger group with greater resources may be able to carry out an attack with higher consequences, but a major limiting factor today is the highly limited accessibility of the agents with the potential to cause the highest impact. The higher aspirations the actor has in terms of sophistication and impact of the biological attack the higher skills are required. Preparation time, cost and risk of failure also increases with complexity.

The same reasoning can be broadly applied in terms of non-state actors' use of toxic chemicals. Generally it is cheaper and easier to manufacture a toxic chemical than an infectious agent, and stability in different environments is usually higher. There are many commercially available chemicals on the "civilian market" today that can provide a fully adequate effect in terms of casualties. Some of these civilian chemicals are not regulated by import/export controls and are also relatively easily available through theft in connection with transport or storage. An example of attacks in which easily available chemicals were used in combination with very primitive explosive devices was the use of chlorine gas canisters intentionally exploded

25) Post J.M., 2005. The psychology of WMD terrorism, *International Studies Review vol 7 no 1, March 2005*, pp 148-151.

in Iraq in 2007. The technological developments in recent years are to a very high degree too advanced to benefit terrorists' ability to produce chemical agents.

> *"Add to all that now the risk of terrorist actors getting their hands on the makings of a nuclear weapon. We can no longer be under any illusions about the intent of certain messianic groups to cause destruction on a massive scale. And – although the probability is small, and probably lower than some alarmist accounts have suggested – their capacity should not be underestimated to put together and detonate a Hiroshima-sized nuclear device."*[26]

In the radiological field the amount of available radioactive materials throughout the world is increasing despite stronger regulatory frameworks in some countries. The industrialization in developing regions contributes strongly to the increasing use of radiation sources. In the Western world the strongest sources in hospitals are beginning to be replaced by accelerator-based equipment because it is safer and easier to handle, thus reducing the risk that radiological sources end up in the hands of actors of concern. The accelerator-based facilities are very expensive, which means that less wealthy countries are unable to acquire such equipment.

The wide availability of radioactive sources and the inadequate or nonexistent control of many of these sources in some geographical areas clearly demonstrate the potential for the use of radioactive materials in antagonistic purposes. In order to generate acute radiation injuries in larger groups of unprotected individuals by means of a dirty bomb, construction requires an extremely strong radiological source and an advanced detonation device which generates an appropriate particle distribution. Nevertheless, the consequences of a dirty bomb with a weaker radiological source and a perhaps not so advanced detonation technique would be anything but negligible. Radioactive materials could also be spread by other means such as through contaminated water or food products. In these cases it is not certain that there would be acute radiation injuries, but the effects on society and the individual would nevertheless be especially relevant. A large number of sources contain cesium chloride (CsCl), which makes the source relatively easy to convert to a liquid solution to be distributed through a spraying device. Placing a radioactive source in a place where people are staying is the simplest and least technology-intensive way to cause damage if you have access to a source. In addition, there are some radioactive materials that can not be fragmented easily, and with that knowledge positioning the source in a strategic location would be the obvious choice.

3. Terrorist Attacks against the International Civil Passenger Aviation Sector

Aviation has been a target of terrorism activities since the late 1960s when Arab hijackings of Israeli and Western airline flights were initiated, and was followed by a wave of hijackings as leverage for political purposes. The passenger aviation sector has become an attractive target for terrorists for a number of reasons. John Harrisson provides a lucid explanation of the potential motives behind terrorists' interest in targeting international civil aviation by classify-

26) International Commission on Nuclear Non-proliferation and Disarmament Report, 2009. *Eliminating Nuclear Threats: A Practical Agenda for Global Policymakers*, Canberra/Tokyo.

ing the multiple motives.[27] Harrisson portrays civil aviation as a powerful symbolic target with an international characteristic, making every effort to strike against it a top media story and a center stage worthwhile for any terrorist organization with a message to proclaim globally. All flights have a national symbolic value and significance. An El Al flight represents Israel, Aeroflot Russia, and so on. Beyond the company the destination of the plane represents an important factor influencing the nationalities of the passengers onboard. Furthermore civil aviation offers a relatively simple and vulnerable target which could result in significant economic losses for both the aviation carrier as well as the nations targeted. The aviation sector's first mission is to provide transport service that is easily accessed and implies a minimum of intrusion on privacy. The large flow of passengers makes it difficult to detect and detain an attacker and the fact that many passengers carries luggage makes it relatively easy to conceal a weapon.

Past incidents of terrorist attacks against airports and airplanes have included hijackings, small arms and explosives, which have shaped our current security systems and routines. The international and European regulations regarding security measures at international airports have become more extensive and have lead to more than tripled costs for many airports since the Lockerbie bombing in 1989, and have been further shaped by incidents such as the 9/11-attack in the US in 2001, the 2006 London plot and the Detroit incident in December 2009.[28]

The trend of criminal acts and terror attacks against civil aviation has varied over time. Since the deadliest decade in the 1980s, with 1207 dead, the number of incidents and casualties has declined, with the exception of the September 11 attacks.[29] There are 964 terrorist related incidents against airlines and airports registered through open sources covering the period 1970 – 2007. More than half of these incidents included explosives and 24% were registered as hijackings; 64% of the incidents where resolved without resulting in any casualties. [30] Hijacking was the dominant airline incident from 1968 to 1994. At this point in time terrorist attempts to strike at aviation targets started to indicate a change of tactics, from hostage taking and as way of transport to specific locations to the approach of using civil passenger aviation as an instrument of inflicting massive casualties and destruction. One likely reason for this change is the fact that security measures had increased considerately by amendments and developments within ICAO and IATA as a response to the wave of hijackings. This coincides with the new form of terrorism growing which to an increasing extent is founded on extreme religious ideologies and cults.

✓ *3.1 Assessing the Potential Threat of CBRN Terror against Civil Aviation*

There have been no terrorist attacks targeting civil passenger aircrafts by means of CBRN-materials according to available open source information. However, this does not provide sufficient grounds for concluding that terrorists haven't been planning for such events or have intent to pursue such attacks in the future. The past reported incidents surrounding passenger aircrafts and airports involving chemical, biological and radiological agents and materials in

27) Harrisson John, 2009. *International aviation and Terrorism; Evolving threats, evolving security, Routledge*, UK.

28) Interview with Anders Lennerman, Airport Security Director, Stockholm Arlanda Airport, October 209.

29) Maret Jean-Luc, 2010. From Lockerbie to Umar Farouk Abdul-Mutallab, *Transatlantic Security Paper No.1, April 2010*.

30) GTD2-search on target type "Airlines & Airports", including "only incidents where there is essentially no doubt of terrorism" and where Terrorism criteria I and II are fulfilled, 2010-04-27.

general have been few indeed. Most incidents have involved individual attempts to smuggle or otherwise illegally transport such dangerous materials, mostly radiological sources for economic gain. There are unconfirmed allegations of an attempt to spray botulinum toxin in the vicinity of Tokyo's international airport by Aum Shinrikyo in April 1990 and reports of a mysterious gas leak at Melbourne airport's south terminal on 21 February 2005, which resulted in 57 passengers in need of medical care and the evacuation of 14000 passengers. There have also been a few cases where passengers have been poisoned in connection with air travel.

As pointed out by many researchers, when studying the potential threat from innovative terrorists the past is often a poor guide to predict future events and we tend to place too much reliance on past observables. This is especially problematic on issues concerning terrorist behaviour and advances in CBRN technology which have shown themselves to be highly dynamic phenomena. As Gary Ackerman eloquently put it, "*If future developments in CBRN-terrorism look very different from those of today, we must be careful not to act like the proverbial generals fighting the last war by preparing responses applicable only to the terrorists and technology of yesterday, or for that matter, today*".[31]

With this perspective on the CBRN-terrorism dilemma we need to look into what may influence terrorists' ambitions and attitudes towards developing their toolbox in order to pursue terrorist attacks targeting civil passenger aircrafts by employing chemical, biological, radiological or nuclear materials as weapons. Having reviewed terrorist organizations' past efforts and stated interests regarding the use of CBRN-materials as a weapon, and reflecting upon that in the context of the character of the aviation sector, we can elaborate on a set of potential factors that may converge into a potential threat.

3.1.1 Circumventing Enhanced Security Systems

Terrorists in general have shown a fairly well developed ability to adapt their strategies and methods in light of the measures implemented by law enforcement, security and the intelligence community in the fight against terrorism. The aviation industry is a very typical example of this. There has been a dramatic development of security measures at airports as an effect of the numerous attempts by terrorists to target aircrafts with traditional means and methods. Although this development has generated much higher thresholds for terrorists to launch a successful attack, these actors have shown that targeting civil passenger aircrafts is still high on their agenda. A recent example of this is the young Nigerian Umar Farouk Abdulmutallab's unsuccessful efforts to detonate a PETN-based explosive device on the Northwest Airlines flight 253 from Amsterdam to Detroit, Michigan, on 25 December 2009. Abdulmutallab managed to conceal the explosives when passing through the security check by hiding the material in his underpants. Al Qaeda in the Arabian Peninsula claimed responsibility for the attack, describing it as revenge for the United States' role in a Yemeni military offensive against al Qaeda in that country.[32]

Another recent example of terrorists developing new methods as a reaction to increased security is the attempt by a well-known Saudi terrorist, Abdullah Hassan Talea' Asiri, affiliated to

31) Ackerman G., 2009.The status of CBRN Terrorism Research, In: Ranstorp M. and Normark M. ed. *Unconventional Weapons and International Terrorism,* Routledge, London UK, 2009.

32) Spiegel and Solomon, 2009. Al Qaida takes credit for the Plot, *The Wall Street Journal*, December 29, 2009.

the terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP), operating in Yemen, to assassinate the Assistant Interior Minister of Saudi Arabia, Prince Muhammad bin Nayef, through a suicide bombing attack on August 27, 2009. By claiming his intent to defect to the Saudi government, Asiri managed to be invited to a personal meeting with Prince Nayef at his office where he detonated an explosive device concealed inside his body. Before meeting with the prince, Asiri had spent over 30 hours with the Saudi security services, and passed through several security checks as part of his transport from Yemen to Saudi Arabia; and even at the checkpoints established to search all those approaching the prince.[33] Both these examples indicate that increased security forces these actors to adjust and develop their means and methods. At this point the introduction of body scanners seems to be the new development within some European airports, making security checks even more robust and intrusive for passengers.[34]

None of these attacks resulted in casualties or any extensive chaos, but represent worrying examples of terrorists accessing vulnerable targets with potent explosives. The failures of these attacks were rather a result of the perpetrators' lack of knowledge regarding igniting the explosive in one case and the limited effect of the explosive through the absorption of the body in the other. With the right training these perpetrators could have executed these attacks with a more destructive outcome.

Increased security checks of passengers could potentially force terrorists, planning attacks against aircrafts, to apply other methods in order to increase the prospects of a successful operation. As the scrutiny of all passengers and luggage is getting tighter, the prospect for a passenger to bring a weapon onboard is increasingly difficult. A civilian passenger aircraft today is however in the centre of a wide network of service and logistical arrangements which potentially could be utilized as an alternative route for executing a devastating attack. The catering service could be one way to effectively disseminate a pathogen, toxin, a toxic chemical or radioactive substance to all onboard the aircraft, including the pilots. By injecting a small amount of ricin toxin or a pesticide in the food, symptoms would be fairly quick leading to acute distress for all passengers eating the food or drink, while still airborne. This method of attack is relatively easy to perform as the potential material can be acquired without the need of difficult processing before launching the attack. Furthermore the dispersion method is very simple given that the perpetrator can infiltrate the catering service chain at some point before the food or drinks are loaded onboard the aircraft.

33) Europol SC5 – Counter Terrorism Unit, 2009. The concealment of Improvised Explosive Devices (IEDs) in rectal cavities, The Hague, Netherlands.

34) House of Commons, Home Affairs Committee, 2010. *Counter-terrorism Measures in British Airports*, Ninth Report of Session 2009-10, London, UK.

Ricin is relatively stable and would possibly even sustain heating to some extent, making it toxic if injected into food or beverages that are further processed trough heating before being served. The symptoms after ingesting ricin toxin appear within 4-12 hours as diarrhoea, nausea, vomiting and abdominal pains. More severe cases of ricin poisoning include fever, thirst and headache, which can result in collapse and shock. A lethal dose of ricin will result in death within 3-4 days.[35]

Poisoning through onboard catering could with a relatively low grade of competence be performed by adding a pesticide in the food. Rodenticide (sodium fluoroacetate) is a pesticide used worldwide to control rodent populations. It is colourless, tasteless and odourless with a lethal dose estimated to be 0.5-2.0 mg/kg body weight. First symptoms appear after 30 minutes to 2 hours or more after ingestion. Symptoms can include nausea, vomiting and mental apprehension followed by coma and epileptic convulsions. Death may result from either cardiac or respiratory failure.[36]

In line with these potential scenarios, other logistical services surrounding the aviation industry may provide opportunities for terrorists to deploy dangerous materials against a passenger aircraft in a way that current security systems would have difficulties to detect and prevent.

3.1.2 The Game Changer Effect

Any antagonistic attack by violent means against unprotected civilians is a horrible scenario to contemplate. But more appalling would be to suddenly become a victim with burning skin and lungs, grasping for air and convulsing, as an effect of something invisible, tasteless and odourless. Even if something is dispersed in the air fully visible to the victims realising that something in the air is poisoning them, they still have to breathe. Radiological, chemical and biological agents dispersed through air are impossible to dodge in contrast to bullets or fragments from explosives. Since this scenario of widespread fear was heightened in many Western countries in the wake of the 9/11-attacks, it has become obvious to terrorists and terrorist leaders worldwide that these weapons have an effect not only through their toxic or contagious properties, with the potential of enhancing the physical effect, but also in terms of creating an increased psychological and socio-economical impact on a much wider audience. This is further underscored by the attention these efforts and types of attacks receive in the media coverage of various incidents. Hence, fear, panic and chaos can be achieved simply by falsely stating the use of agents that are not really visible or possible to detect at the time of the event or by using fakes like in the anthrax-hoax letters distributed widely in the United States that followed the real anthrax laced letters in September and October 2001, causing tremendous costs to society on a variety of levels.

3.1.3 The Factor of Innovation

The propensity for a terrorist organisation to change tactics or means for their attacks is further a driving force which may impel terrorists to employ CBRN-materials in future efforts.

35) Lundberg S. et.al, 2004. Ricin; *Threat, Effects and Protection*, Swedish Defence Research Agency, Umeå Sweden.

36) Occupational Safety & Health Service, Department of Labour, 2002. *Guidelines for the safe use of Sodium Fluoroacetate (1080)*, Wellington, New Zealand.

Adam Dolnik's research on terrorists' innovative abilities highlights a number of factors driving terrorist innovation. Dolnik concludes that an organisation's domestic dynamics such as altering predominant ideology or strategy as well as a change in structure by the formation of splinter groups may motivate innovative developments to escalate the level of violence with each attack. Other factors may be the emergence of competition with other organisations operating in the same theatre, or as a response to governmental countermeasures such as hardening of potential targets. Furthermore, Dolnik emphasizes the prospects of innovation towards the use of CBRN-means as a result of intentional or unintended acquisition of a particular human or material resource that would lower the thresholds for successfully launching a CBRN-attack.[37]

In contemplating the contemporary terrorist organisations' dominant means and methods, actors employing CBRN-weapons in future mass-impact attacks would have to engage in radical technological innovation at a high level, making any sign of innovative measures extremely important for counter terrorism measures in the future. Small scale CBRN-attacks however could become a reality by pure opportunity, by gaining access to facilities storing or handling toxic or contagious agents, the recruitment of technically skilled operatives or the theft of redundant military chemical warfare munitions.

✓ *3.2 Concluding Remarks*

To conclude, there are no clear indications of contemporary terrorist actors with both intent and capabilities to perform a CBRN-terror attack. The few efforts made in recent years have been relatively unsuccessful in achieving large scale effects due to the complex and technologically difficult process of acquiring the right competence and materials, producing a potent agent in proper amounts, and the even more difficult challenge of distributing this agent in a way that will cause mass casualties and catastrophic effects in the targeted society. However, it is evident that there are organisations that have identified the potential in resorting to CBRN-materials to cause harm, fear and terror to a larger audience and at the same time have a fascination for the civil passenger aviation sector making CBRN-terrorism incidents a potential threat in the future.

37) Dolnik A, 2007. *Understanding Terrorist innovation; Technology, tactics and global trends*, Routledge, UK.

Juha Rautjärvi, Mikko Valkonen & Martti Annanmäki: Threat of Nuclear and Radiological Terrorism to Air Transport

1. Introduction

The civil aviation has been a target of terrorist acts since the end of the 60's. The terrorist acts have evolved through hijack, sabotage, assaults against the planes of certain nations and ultimately to the point where four planes were used as weapons against the civilian and military targets in Washington D.C. and New York in 2001. The USA and the international community as a whole reacted to this escalating violation promptly by launching a war against terror and mobilizing a war in Afghanistan against the suspects of the international terrorism. Within the international community various conferences were organized, conventions negotiated and security initiatives taken to combat terrorism. United Nations Security Council had several meetings and passed resolutions trusting the member states to take care of the security deficit.

Within the context of the European Union programmes, financial instruments were developed to launch projects aimed at addressing the concerns and implementing the required improvements in security. Among the various initiatives the Aether-project is the one aimed to improve the security by addressing various aspects of CBRN-threat against the civil aviation. This article deals with the radiological and nuclear threats[1]. The chemical and biological threats are subject for other studies.

The nuclear and radiological threats have been considered to be major concerns already for some time. There is evidence that the terrorist organizations have been contemplating to use nuclear and radiological materials in terrorist attacks. There is evidence that certain groups have been searching for the capability by investigating sources of materials, including nuclear weapon grade materials, as well as acquiring information about the experts that are knowledgeable of nuclear weapons. The same is valid for the possible use of other radioactive sources and substances.

In Finland the national threat assessments, response plans and communication systems are being produced. This study is aimed to provide a picture of the present situation and to identify items that may need to be improved to be adequately prepared for this kind of incidents.

This study is focused on the threat caused by the terrorists who may use nuclear and radiological substances for terrorist purposes. In this study the civil aviation, including the airports and the logistics serving the airport and the planes, is considered to be the target.

The terrorist threat emerges as an evolving phenomenon that does not necessarily follow

1) In this study the terms threat and risk are used. The term "risk" is understood as a function of the "threats probability" and "consequences involved" (Basil Steele, Sandia National Laboratories).

any common logic. Therefore the security is hereby also seen as an evolving process enabling to assess the situation timely, and, when needed, manage the threat situation efficiently and take appropriately care of the consequences.

This study on nuclear and radiological threats is based on several documents. References include international, Nordic and domestic (Finnish) evaluations of terrorism and threats involving the use of nuclear and radiological materials.

Also about 20 experts were interviewed. The experts included authorities and actors of the private companies responsible for security function. The findings of the interviews without any filtration are reported in this first study report. The findings will be subject for further review, and the final results are reported in the second study report.

Apart from the interviews this study is based on publicly available sources and references.

2. Aims of the Study

The first aim of the study was to understand the nature of the new challenge; how does it differ from the "normal" accidents involving nuclear and radioactive materials. A lot of work has been done to prevent such accidents and to limit the consequences in case the accident has taken place. The safety and related security systems are continuously tested in exercises to efficiently respond to incidents and accidents involving nuclear and radioactive materials.

The second aim of the study was to study what kind of role nuclear and other radioactive materials might play in terrorist attacks. What forms it would take, what kind of targets might be chosen and what kind of materials might be used during the next phase of this evolving threat?

The third aim of the study was to find out how the security arrangements and operations should be further developed and supplemented to meet the new threats and possible attacks. Particularly challenging questions related to the way how to cope with the evolving nature of the threat and the unpredictability of an attack.

3. Underlying Hypothesis

For the purposes of this study and based on the brief review of recent publications the validity of the following hypotheses were put for a test:

- The security systems of the civil aviation industry, including plane, airport and logistics providing the required services are not adequate at present.
- Hazardous nuclear and other radioactive materials are available to play a role in terrorist plans and to be used as an instrument of terror.

- Independent evaluations have not been made to obtain verification of the reliability of the protection and control arrangements.
- The existing procedures and the security functions have provided protection up to now.
- The use of NR-materials for terrorist purposes has not been really wanted by the terrorist groups up to now.

4. Work Process, Material and Methods

✓ *4.1 The Work Process*

The study was conducted in four parts: Firstly, a brief look into the available literature was carried out and some selected documents were reviewed. This was done to understand the nature of the problem and to determine the aims and the hypothesis for the work ahead.

Secondly, the security relevant operators at operative level were identified and selected for interview with the aim of conducting a 'reality check'. The interviews initiated a process that contribute to the development of improved security structures and in the end may deliver also some well justified recommendations.

The third phase involved a workshop to assess the findings of the interviews. The experts involved in this research also participated in the exercises of the Aether-project as observers.

The fourth phase included a workshop assessing the outcomes and identifying the conclusions and formulating the recommendations.

✓ *4.2 Material and Methods*

The basic literature study included some books, regulatory documents, conference presentations and scientific papers. The material was selected taking also into account the results of a brief web-review. The documents are post 2001 so that the impact of the 9/11 is already reflected in them. The literature sources include a book on the history of terror against civil aviation (Harrison 2009) , a book elaborating the use of unconventional weapons for terrorist purposes (Ferguson 2009), Finnish national strategy to secure vital functions of the society (National counter-terrorism strategy 2010) and the updated version of the national CBRN-threat assessment, Nordic and EU working group papers assessing the threat and materials that might be used for malicious purposes (Mustonen 2009, NKS 2008). Some publications have been used to study the factors influencing the management of the crisis situation and the conduct of security functions, with particular interest to understand the conditions enabling efficient communication and cooperation (Valtonen 2010, Sinkko 2004, Krogars 1995).

In addition, information from the IAEA Illicit Trafficking database (ITDB) has been used to provide more detailed information about the cases of interest. The relevant international Conventions, the UN Security Council Resolutions and respective EU Regulations have been also used as reference as well as the declarations of the Washington April 2010 Summit (http://fpc.

state.gov/documents/organization/140355.pdf).

The results of the literature review suggested that the nature of the subject matter is such that the approach initially selected for this study had to be changed. In order to avoid just repeating something that has already been done earlier, it was decided that the relevant security operatives of different organizations should be involved in this process.

In order to enable interactions and maintain the required discipline during the work process it was decided to apply the Delphi-method for carrying out this study. The Delphi-method was used with the aim to find out the most relevant issues that need to be addressed as the preventive measures against RN-threat.

The Delphi method can be described as follows: It is a systematic, interactive forecasting method which relies on a panel of experts. The experts answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgments. Thus, experts are encouraged to revise their earlier answers in light of the replies of other members of their panel. It is believed that during this process the range of the answers will decrease and the group will converge towards the "correct" answer. Finally, the process is stopped after a predefined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results (Valtonen 2010, Wikipedia).

The Delphi-method was applied in a flexible manner. Instead of using a panel of experts it was decided to interview experts one at a time. The outcomes and the findings from these interviews are presented in this report and they were analysed in more detail in a workshop later on, partly using the same experts.

This method may also be applicable when assessing the changes in the security environment or trying to understand the value of weak signals. The need of the new methodological proposition could be seen as one of the main outcomes of this study.

✓ *4.3 Search for the Approach*

In order to be in position to understand the problem, to be able to select efficient work process and to identify the relevant questions, some of the security operatives associated with the Aether-project met at Reinikkala manor in January 2010 so as to create the shared understanding of the direction for this study.

As a result a need for deeper understanding of the difference this threat is imposing on security operatives, who are trained to address the normal accident situations, was confirmed. It appeared necessary to interview the security operatives of different organizations and to develop a questionnaire for the interviews. The questionnaire was drafted and finalised after the meeting. The questionnaire is attached as appendix I.

It appeared necessary to extend this study to include the following four phases:

- Brief review of the literature and other publications
- Interviews of the security operatives of different organizations

- Monitoring of the exercises of the Aether-project and a workshop to elaborate the findings
- Elaboration of the findings by an expert group.

✓ *4.4 Interviews*

The security operatives from STUK and other relevant organizations were selected so that the operative environment and different roles and functions in operations were widely covered. The intention was to obtain factual and also perceptual information about the threat, security environment, systems and practices from different perspectives. The purpose was to reconcile this information with the concerns and expectations.

From STUK 10 experts were interviewed. The experts represented various organizational units and processes responsible for security, safety and safeguards as well as public information. The experts interviewed are currently engaged to prevent terrorism, to protect nuclear power stations, to protect nuclear and other radioactive materials in use and transport, to develop technology for security applications, to protect environment from the consequences and to develop and maintain adequate level of preparedness for the case of an accident or terrorist attack.

In addition, at STUK two experts on Probabilistic Risk Analysis were met to discuss the possible use of that method and existence of other complementary methods to assess the risks associated with such threat as terrorism (Ezell 2010).

From other relevant parties responsible for security functions 9 persons were interviewed. These represented Finnair, Finavia, National Security Police, Regional Rescue Services, Police and Ministry of Interior. Also experts from the University of Jyväskylä (Nuclear and accelerator based physics) and Central Hospital of Middle Finland were interviewed.

5. Results

As a general observation it may be stated that the hypothesis outlined above can be considered as valid. Fortunately, no terrorist attacks involving RN-materials have happened yet. One of the possible scenarios could have involved the use of stolen radioactive sources (for example in industrial or medical use) and other substances with conventional explosives against prominent places. Also the availability of highly enriched uranium and knowledge about weapons design could have lead to improvised explosives and then used for causing terror. We have been thus given an opportunity to continue taking care of the recognized security deficits.

It seems evident that the problem has been recognized, the relevant security concepts exist, at all levels, international, national and within the organizations providing security services. However, the threat perception associated with the use of RN-materials in terrorist attacks against civil aviation is not shared in a coherent manner yet.

Generally security related processes are well organized within organizations responsible

for security and secured communication channels exist. Responsibilities have been shared, and individual security operatives carry out their assigned functions as planned. However, the functions are not yet fully operational to be able to respond as an organization, coherently and efficiently when RN-materials are used against civil aviation.

✓ *5.1 Results of the Literature Review*

The use of nuclear and radiological materials for terrorist purposes is possible. Some terrorist groups have considered using these materials. In many countries, including those possessing nuclear weapons and associated materials and knowledge, there exist huge amounts of suitable nuclear and radiological materials in facilities and storages, which are not adequately protected.

Why not? The motivation may be of rational or irrational in nature, religious, ideological or economical. The reason is not known. In the future terrorists may want to demonstrate the power they have over the society and its security functions. For such purposes a smaller amount of nuclear and other radioactive material is sufficient to cause direct and indirect consequences that are considered undesirable. There is no need to create mass destruction using nuclear weapon. Explosive nuclear device, a dirty bomb or significant contamination of man and material may bring the desired impact. But the threat using nuclear weapon exists.

There is a need to improve the understanding of all the threats, consequences, and circumstances, to be able to recognize weak signals of terror acts and make it possible to neutralize the attack (Summary based on the references listed).

5.1.1 The Threat against Civil Aviation

The nuclear and radiological threat against civil aviation is perceived as real taking into account the evolution of terror against civil aviation since the end of the 60's. The use of nuclear and radioactive materials against the plane, travellers, airport facilities, people and the services is a possibility that shall not be ignored (Harrison 2009).

With reference to current Finnish national risk assessment the following can be stated:

The EU Terrorism Situation and Trend Report 2009 observed that there are a large number of various terrorist organisations active within the European Union. Their aim may be to strike at targets in a Member State or outside the EU while using the EU as a base. The Report classifies terrorist organisations according to their principal motive as follows: Islamist terrorism, ethno-nationalist and separatist terrorism, left-wing and anarchist terrorism, and right-wing terrorism.

In 2008, there were 515 attacks in the EU made by organisations classified into one of the above groups. Of these, 397 were made by separatist groups. Most of the attacks involved material damage only, without homicidal intent. The most common target countries for terrorist attacks were France, Spain and the UK. Half of all the arrests in connection with terrorist attacks were related to Islamist terrorism. International threat assessments indicate that Islamic extremist terrorism constitutes the most serious threat to the functioning of the international system.

In recent years, extreme Islamic groups and networks have become more active in Europe. Conflicts in Muslim areas contribute to radicalisation among Muslims living in Western countries. Conflicts may also lead to an increased flow of refugees to European countries, including Finland.

At the moment there is no direct terrorist threat against Finland. However, we must note that not only foreign and security policy decisions but also economic and social conditions within the country may contribute to violent radicalisation. Finland may also be used as a base for funding or otherwise supporting terrorist action (The Finnish Security Police 2008-2010).

There are present and future threats against the interests in Finland of those countries that have been named as targets by extremist Islamists. Major international events organised in Finland, such as summits, sports events and conferences, are also potential targets for terrorist action. However, to date the security arrangements at such events has been successful even by international standards. Globally active terrorists systematically compare the security arrangements in various countries Finland included, and aim to strike where they consider they have the greatest chance of success.

No international terrorist groups are operating in Finland, but the national extremist and alternative movements in Finland have become more international. This is particularly noticeable in the case of the animal rights movement, but other Finnish activists have adopted methods from abroad too. Environmental and climate issues and the problems involved in nuclear energy and the processing and storage of nuclear fuel remain the main themes among activists. Activists visiting Finland from abroad are almost without exception members of an international NGO disavowing violent action.

5.1.2 Availability of Materials

The terrorist threat is a complex phenomenon, which can not be just eliminated. However, we can make reasonable effort to neutralize the possible attempts by reducing the demand and by limiting the possibilities to exploit the supply side of NR-materials.

Availability of dangerous nuclear and other radioactive substances is one of the key attributes to be paid attention to. The terrorist interest in acquiring nuclear and other radioactive materials may be aimed to

- nuclear materials that can be used for nuclear weapons
- nuclear explosive devices in storages or transport, which are not adequately accounted for and secured
- research reactors that are using weapon grade enriched uranium
- secret programmes and supply channels
- high activity radiation sources that are not adequately accounted for and secured
- radioactive waste left from the past nuclear programmes
- enriched uranium and plutonium in storages and transportation for the purposes of the civil nuclear industry.

Nuclear material that is directly usable for weapons and explosive devices exists in about 40 states. The accountancy, control and protection measures have been improved since the early 90's in many countries and areas. However, the completeness of the inventories has not been assured yet; the accountancy and security measures are not yet adequate in many areas. Possibility of access to the weapons grade materials or nuclear weapons and relevant knowledge may well be increasing when the decommissioning of the old facilities and the conditioning of materials that are no more serving the weapons purposes, will proceed. At the same time the security culture is changing and the new generation of people guided by different values and motives is engaged in the processes and may well make the systems more vulnerable (Varjoranta 2010, Mustonen 2009).

Particularly vulnerable areas are understood to be in Pakistan, despite of the improvements that have been made with the support from the USA and in the DPRK, where the security situation is deteriorating. Both countries are by now instable and the possible changes unpredictable. The threat of disseminating material and knowledge to unknown purposes is possibly increasing. In Russia the security measures, including the physical protection of facilities and material has been improved during the past 15 years. The major collaborative effort of bilateral and multilateral partners as well as Russian's own efforts has improved the situation, but the work is not yet completed. The insider-threat and that caused by terrorists will be taken seriously and efforts to improve the security continue (Varjoranta 2010).

There are many other States where nuclear and radioactive material may become available for the terrorist purposes. Radioactive material is missing and orphan sources are found regularly. Estimates of the amounts of radioactive material lost and missing are inaccurate. Also the possibility that high amounts of enriched uranium are missing, can not be excluded. According to IAEA, samples of uranium originating possibly from bigger shipments are attempted to be sold. About 80 percent of the sources found have never been reported missing and about 65 percent of sources reported missing are never returned (Karhu 2009).

Worldwide there are hundreds of medical, industrial and academic applications using radioactive sources of significant strength. Seven reactor-produced radioisotopes are of particular concern due to their radio-toxicity, their widespread use and their sufficiently long half-life: Am-241 (432 years), Cf-252 (2,6 years), Cs-137 (30 years), Co-60 (5,3 years), Ir-192 (74 days), Pu-238 (88 years) and Sr-90 (29 years) (Mustonen 2009).

These radioisotopes are used in many applications with different activities as shown in Figure 1 (Mustonen 2009).

There are many factors decreasing the overall security of a radioactive source during its life cycle. There can be weaknesses in organisations, in regulations and procedures, in the proper working of regulatory bodies and in regulatory enforcement. Often a lack of knowledge and awareness are reasons for getting the source lost. E.g. security during transport can be lacking. Furthermore there can be obstacles to legally dispose of radioactive substances because of the high costs, or legal disposal can be non-existent (Mustonen 2009).

It is estimated that in the USA there are between 500,000 and 2,000,000 sources which are no longer needed and up to 375 sources are yearly reported to be orphaned. The figures for

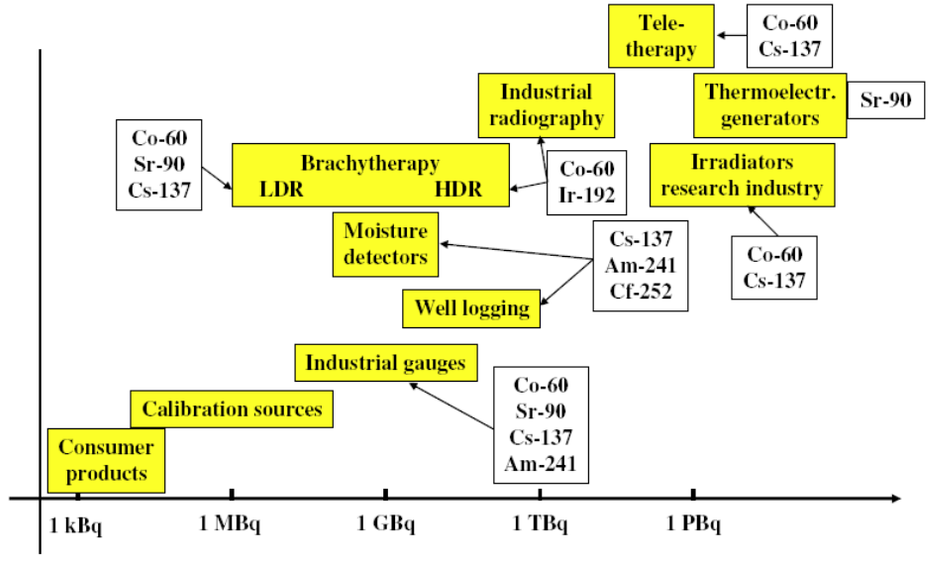


Figure 1: Commercially available radioisotopes and their activities in different applications in industry, medicine and research.

the European Union are 30,000 disused sources and up to 70 sources per year reported to be orphaned. In the former Soviet Union it is estimated that there are thousands of orphan sources of high threat category (Mustonen 2009).

The references above confirm that dangerous nuclear and other radioactive materials are available and one day may play a role in terrorist plans and may be used in terrorist attacks. The accounts of these materials are not complete enough. The prevention measures of thefts are not efficiently implemented. Also protective security measures, including the physical protection of the facilities and materials are not adequately implemented in all places. Vulnerabilities exist that need to be taken care of urgently. The amount of work a head should not be underestimated.

✓ *5.2 Nature of the Challenge and the Implications*

The information about the terrorism against the civil aviation gathered so far, confirmed the understanding that there are different kinds of challenges to the security systems depending on the threat. The discussions at the Reinikkala workshop were directed to process the complexity of the threat and the ability of the security systems to asses the situation, to prevent the threat and to manage the consequences.

The conditions and circumstances that make a terrorists action possible were identified and discussed. Table 1, which facilitated the discussions, identifies and characterizes the main attributes that need to be paid attention to in assessing the situation.

Primary modes of terrorist operations, logistics and possible consequences									
Incident	**Type of means**	**Expected target**	**Possible motives**	**Planning of the offence**	**Financial recourses**	**Logistics required**	**Security Sources**	**Consequences caused by the threat or the attack**	**Possible actor**
WMD-hit	Nuclear weapon	Airport (city)	Finnish policy	Easy to plan	30 - 50 MEUR	Car, airplane	PAL-code	Mass destruction Contamination	AQ***
	Self made bomb	Airport (city)	Finnish policy	Expertise needed	30 - 50 MEUR	Car, airplane		Mass destruction Contamination, High radiation dose	AQ
Dirty bomb	HAM*	Airport (city)	Finnish policy, ecological terror	Easy to plan, insider needed	10 - 100 kEUR	Car, aircraft		Contamination High radiation dose	AQ EF****
	HASS*	Airport	Ecological terror	Easy to plan	10 - 100 kEUR	Car, aircraft	Co-60: >0,1 PBq radiation therapy) Sr-90: >1 PBq (electric generator) Ir-192: >1 TBq (radiography) Co-60: >1 TBq (radiography)	Contamination Radiation dose	EF

*) HAM = High Activity Material
**) HASS= High Activity Sealed Source
***) AQ = big international terrorist organization e.g. al-Qaeda
****) EF = local activist group e.g. Earth Friends

Table 1: Primary modes of terrorist operations, logistics and possible consequences (The information presented in the table was collected from various sources including the interviews and references).

The attributes of different types of incidents include the following:

- Type of means, nuclear weapon or an improvised explosive device using nuclear material, explosive device containing radioactive material (dirty bomb), various means to damage or contaminate environment and people with radioactivity;
- Expected target and possible other options;
- Possible actor and motives;
- Planning of the offence;
- Financial recourses;
- Logistics required;
- Operative activities, including possible cooperation with organized crime (domestic and international)
- Consequences caused by the threat and that of an attack;
- Effectiveness of the preventive measures.

The discussions helped to understand the evolution of threat as an open and complex, dynamically changing process. It became evident that the contemporary definition of security and associated pragmatic measures and practices are not efficient in addressing this kind of evolving situations - and, may in some cases even prove to be counter productive.

On the basis of this conceptualization a dynamic framework was outlined. This is presented in the Figure 2.

The threat may be evolving over the period of many years. The different kind of information might be available but the weak signals may pass undetected.

A more detailed analysis of these attributes needs to be performed and issues to be paid attention to need to be identified.

The past experiences suggest that information exists within security operatives, and is also communicated, but not necessarily timely enough to be processed in a way that the embedded meanings would be understood. This means that the information is processed insufficiently and that paying attention to the additional information, that may be required, will fail.

The enhanced knowledge creation process may help to assess the relevance of the information at hand and to search for meanings of the weak signals. Such a process should possibly be operated separately from the line-management responsibilities of the situation. It is recognized that further study and exercises are needed in this area.

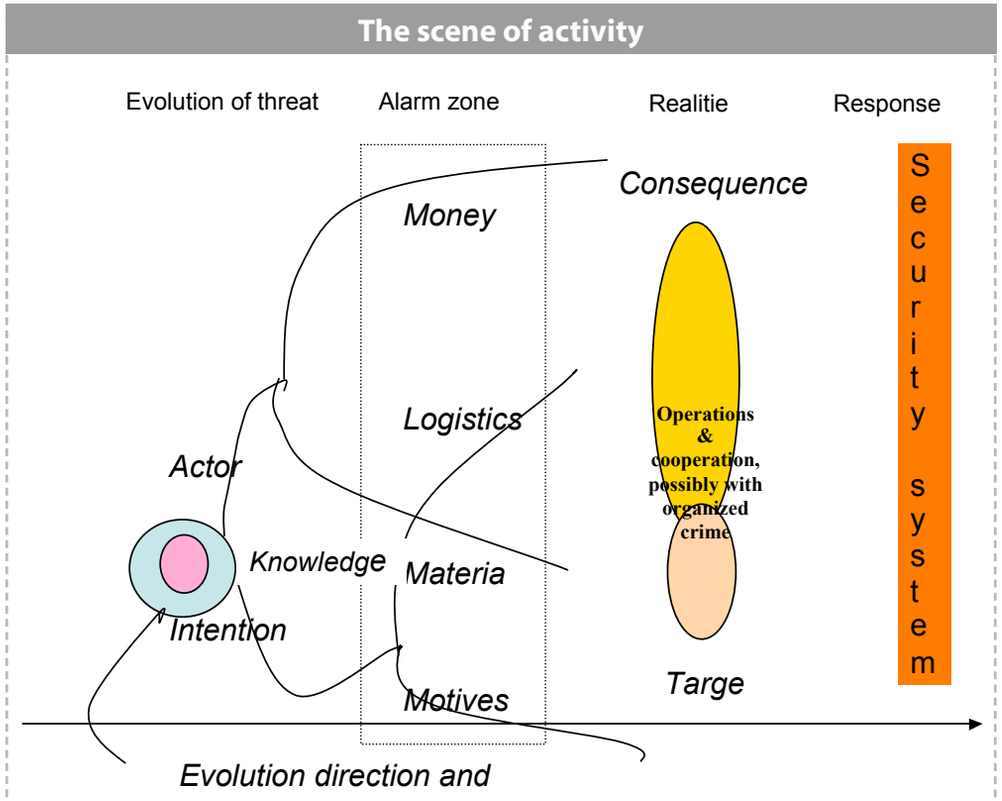


Figure 2. Evolving threat and the main attributes for its assessment

✓ *5.3. Issues Emerging from the Interviews*

5.3.1 Interviews of the Experts

Experts' interviews gave insights about the attitudes, present state of affairs and anticipated state of affairs. Experts interviewed came from STUK, Ministry of Interior, Regional Rescue Services, Finavia, Finnair, Police, the Finnish Security Police and the Finnish Defence Forces.

The preliminary findings (issues) obtained in this research are further processed in a workshop and revaluated later on against the findings obtained in the exercises of the Aether-project. The main aim of the workshop is to identify areas for improvement in current security systems, structures and procedures.

Below are the preliminary findings emerging from the interviews. The findings are organized in accordance with the set of the questions presented:

5.3.2 The Characterisation of the New Challenge

- Terrorism is a phenomenon which should be taken into account in all security related activities. Conventional emergency preparedness is not enough. The present emergency preparedness is a well established and proven, efficient praxis aimed at reacting to predictable accidents, not to respond on unpredictable events like terrorism. Therefore the potential value of the knowledge and experience of the experts that are operating outside the established structures should not be ignored.

- As a phenomenon it is very creative and ever developing. The different forms of terror seem to be developing along with the security measures. This interaction creates a continuously changing situation. The threat caused by the possible insider should not be ignored. We can learn from earlier experiences, but we must be ready and have the capacity to respond to unforeseeable acts.

- In the civil aviation the use of the NR-material in a terrorist act is considered to be a potential threat. Explosives might be replaced with other substances in the next phase of development. The challenge is totally new. It has not been part of the emergency preparedness exercises before. To be able to meet the new challenge and to be able to manage efficiently the threat situation, an operating network should be created as well as models and ways to address the problem.

- Nuclear material and other radioactive substances in Finland are known and under effective control. However, generally in the world there exists abundance of dangerous materials which are not under adequate control and can be used in a terror act. These materials should be taken over, entered in register, protected physically and secured and controlled more efficiently than presently. It can not be excluded that terrorist organizations can obtain nuclear materials, explosives and other dangerous radioactive substances and materials. Therefore, this should be taken into account when planning security systems and exercising respective measures.

- Generally the terrorist threat against Finland is considered to be minimal. This general assessment is understood to mean that the CBRN-threat is also considered minimal. However, for example Finland is now participating in the International Security Assistance Force (ISAF) activities in Afghanistan, which might change the picture. Realization of a small threat can have tremendous consequences. Adequate readiness to manage any possible situation must be developed.

- Security measures, activities and capacity of the actors should be developed to prevent terror acts and to complement the existing capacity of the normal emergency preparedness. Co-operation of the various security operatives should be organized and operations practiced.

- Changes in operating environments at the airport and in logistic serving the airport, including changes in personnel, should be managed so that deviations

from normal procedures and practices will be detected immediately. Information of anomalous incidents should be promptly forwarded to all relevant security operatives, evaluated and decisions made and actions taken as necessary. Threat caused by the insider should be taken into account in all communications and evaluations.

- Intelligence, analysis and evaluation of information and co-operation of various security operatives facing the threat of terror, are all relatively new challenges yet to be exercised. How to be prepared to face the threat emerging unexpectedly? Possibly new procedures and structures are needed to make it possible to exchange confidential information as the situation requires. Possibly also a new process and procedure is needed with respective authority and mandate to deal with the challenge which can be characterized as a "living threat".

- The intentional actor appearing in the present operational environment will change the security situation decisively. Threat by using NR-materials is regarded as a good blackmailing method due to the fear associated with them. We are prepared and we have had exercises to manage accidents involving radioactive materials. Now the challenge is to be well prepared to mitigate and to prevent an act of terror. In Finland CBRN-threat in civil aviation is a new and uncharted territory. So far we have been prepared to prevent illicit trafficking with dangerous goods, including radioactive substances.

- All security operatives are in need for special guidance as to how to behave and handle this new threat and how to manage a possible unpredictable accident involving an active player with bad intentions.

- Modes of co-operation with security operatives of other involved or influenced countries need to be established, including procedures enabling engagement in mitigation, in prevention measures and in consequence management.

5.3.3 Effects on the Role and Activities of STUK

- There is no need to change the role of STUK, but its activities and procedures should be further developed. Security matters are not dealt with as profoundly as other related areas as "safety" and "safeguards". More comprehensive, interactive, communicative approach should be taken to benefit from information and assessments made in different contexts. Compartmentalization of functions in organization, operation and in thinking, hampers the timely knowledge creation.

- Guidance on co-operation should be prepared in collaboration with all other security operatives and the co-operation be exercised. Necessary practical guidance for rescue services and for those who are responsible of security of civil aviation should be written. For example Helsinki-Vantaa airport includes about 1 000 private companies and 20 000 employees who need guidance. Operational environment has become very dynamic. The needs to train and practice are tremendous.

- In preventing acts of terror, the role and functional responsibilities of STUK are still under development. Person to person contacts are dominating presently but co-operation between different organizations should be further developed. Forwarding confidential information and tacit knowledge may be limited and thus assessment and decision making be hampered by not knowing all relevant facts. Knowledge creation and co-operation should become target oriented concerted action.

- Attention should be paid to conditions and circumstances, to elements or attributes that make a terrorist act possible, in order to be in a position to monitor and evaluate the evolving security situation effectively. The weak signals should be detected early and the operations should be performed efficiently through out, including the acute phase of the crises.

- This relatively new form of crises calls for well managed information and communication policies and practices. STUK should be well prepared and should have the appropriate guidance developed also for this kind of cases.

- Over exaggeration is not in place. This kind of challenge should be met with comprehensive independent, 'silent' operations and co-operation with focus on pre-prevention and close monitoring of the developments in the given security environment.

5.3.4 Stakeholder Groups and Co-operation

- STUK and its security operatives have several stakeholder groups: Police, Customs, The Frontier Guard, The Finnish Security Police, Defence Forces, users of radioactivity and their key-personnel, rescue services related public authorities, citizen groups and citizens.

- Main stakeholder groups for civil aviation are Police, The Finnish Security Police, Aviation Authorities, The Frontier Guard, other aviation companies, personnel and customers and also the public authorities of other countries.

- Main stakeholders for Aviation are Finavia and aviation companies, all the service providers, including those providing security services, shops, restaurants, post etc.

- The Finnish Security Police co-operates with e.g. respective international organizations.

- All the security operatives should be seen as a network which is present all the time and is ready to detect all the suspect raising incidents in early phase. All the operatives of the network should forward their findings to be properly processed. This process should be fast and effective.

- STUK needs the expertise of its stakeholder groups. STUK expects that its stakeholder groups contact STUK when needed and is prepared to assist when

required. Proactive approach from the side of STUK as the competent authority is appreciated.

5.3.5 Present Attitudes, Processes and Actions

- STUK is well prepared to respond to threats which are 'static' in nature: like nuclear accidents in Finland and abroad etc. The flexibility and preparedness needed in unforeseen incidents may be lacking. The terrorist related threat is considered to be minimal and the allocated resources and preparedness are also relatively small.

- STUK has an active group of security operatives. It processes the received and acquired information and forwards it on a need to know basis. It also evaluates processes and actions taken. However, a special action plan is needed and resources need to be allocated to this new area in order to ensure the required response capacity.

- Definitively a special action plan is needed to control incidents involving radioactive substances caused by the intentional actor. The aim is to get the whole organization committed to participate in the work. The relevant guidance is currently under preparation and it will be coordinated with the respective guidance of the Police.

- Emergency preparedness will be developed to cover also acts of terror using NR-materials. National database on the potential materials used in terrorist acts is under preparation. This database can be used to assess the threat and to plan the countermeasures.

- The guidance for first responders has been drafted and they are ready to be tested. Co-operation with the police and other security operatives is necessary for the efficient flow of information and for ensuring concerted action.

- STUK's preparedness to provide information about incidents involving possible terror acts should be improved. Also relevant guidance should be prepared and exercises should be organized.

- STUK has knowledge about NR-materials which might be used in intentional acts, but special studies have not been made. More detailed guidance and requirements are needed for adequate accountancy and control of radioactive waste and sources. This work is currently underway.

- Rescue services expect STUK to assist in providing the respective guidance. Regional rescue services are not sufficiently engaged in the network for dealing with the special situations. One of the regional rescue services is expected to co-operate closely with STUK, to conduct exercises and to prepare a model code of conduct to be used by the other regional rescue services. Special attention should be paid to the equipment, other materials and outfit of the first responders. The same observation applies to STUK as well. Liaison and regular contacts

are expected to assure proper preparedness and emergency planning.

- For Finnair normal operating procedures will be updated by adopting a new recording/handling system in summer 2010. This is expected also to further improve the handling of weak signals. Security and safety operations are partly overlapping. In controlling the dangerous substances the focus has been on protecting the airplanes and airports. Intentional acts of terror give a new dimension for the monitoring and control procedures. All the synergy benefits from the security and other related disciplines should be exploited to assure the cost-effective, target oriented operations.

- Finavia has a national security program, as required by the EU statutes, and also a program and relevant guidance for airports. So far these do not include RN-affairs. The directives require threat analyses which have not been made yet. STUK could contact the Central Organisation for Traffic safety in Finland to inquire what kind of support is needed to prepare the threat analysis. The list of prohibited substances is to be updated.

- A new law is expected to be issued in spring 2010. This is expected to improve the present regulations.

5.3.6 What More Should Be Done

- Aether-exercise in autumn 2010 should contain also unforeseen situations. The present exercise plan includes these elements. The exercise is meant to be a genuine test of our actual preparedness at the level of decision making and in the field actions.

- Information security, encrypting etc. should be taken into account when terrorism enters the scene. However, it should not prevent the efficient flow of information. Special guidance is needed and the procedures and practices should be exercised. A topical workshop on secure communication and knowledge creation should be arranged.

- The guidance should contain preventive actions by STUK and co-operation with other authorities and parties. Preparation of an action plan for security and safety operations should be started immediately. The guidance should cover special situations, at least in an exemplar (Po-210 contamination) way.

- To the EU it should be pointed out that all the security related regulations should be based on thorough risk-assessment and cost-effect analysis of the suggested measures. The means to achieve the goals should be evaluated by the security operatives. These means could be identified in the workshops where all the main security operatives participate.

- Chains of responsibilities should be clarified. E.g. which of the authorities is responsible for example, for the decontamination of the airplane and which au-

thorizes the further use of the decontaminated airplane.

- The special expertise needed should be part of the training of the security operatives. Also the availability and adequacy of the protective equipments should be assured, and when the need arises by purchasing the required equipment and materials.

- Finavia needs more RN-substances related training and other guidance. It is important to complete the renewal of all the detectors at the borders. In the related project STUK acts as a technical project leader.

- The cross border co-operation of all the security operatives should be improved by implementing new procedures which allow cross-border cooperation. Such situations could be practiced e.g. within the bilateral projects with Russia and Finland. Later on, such tasks could be added into action plans of the EU's security programs. The developed procedures and the experiences gained could be further tested by the security operatives of the EU.

- The results and experiences gained in the security projects of the IAEA should be exploited efficiently in the new projects. STUK's contacts with the IAEA should be coordinated. All the security aspects, procedures, techniques and practices should form a new area of focus in the Finnish support program.

- To secure different events and operating environments from acts of terror needs a comprehensive control of situation. It may be that the present way of thinking does not support effective preventive measures and control of the threat situation. The handling of this thematics might be realised in projects co-funded by the EU and the IAEA.

- To support the decision making about security measures a special group having high security clearing, authority and expertise should be established.

5.3.7 Possible Obstacles

- The administration should be honed for all the matters spending time, money and energy. Part of the resources should also be allocated to meet the new challenges discussed here.

- Common language in all organizations and domestic and international stakeholder groups is needed when facing the new threat. A special challenge is given by the use of several languages when making decisions in a very short time period.

- Hasty decisions based on non-existing risk analysis should be avoided to prevent adverse side effects, accidents and unexpected consequences and costs.

- No one can own security. Territorial way of thinking should be identified and

avoided. Security is to be perceived as a responsibility to recognize the deficit and to take care of it and not to do anything that may adversely influence the security environment and possibilities to respond efficiently.

- Threatening and exaggeration should be avoided. However, the threat of terror exists and it has its own terms. It may become a reality, now or in the future.

6. Summary Remarks

Possibility of the use of radioactive substances, including nuclear explosives, should not be ignored.
The threat of the use of nuclear weapons or explosive devises is largely recognized. However, it is left many times for the Nuclear Weapon States to worry about. We tend to believe that the nuclear weapons are adequately safeguarded. However, the threat and the security situation are both evolving.

It must be accepted that the security environment is vulnerable.
The security and safeguards experts share the view that the radioactive substances, including nuclear material and knowledge exist for terrorists to exploit. All potential materials are not yet adequately accounted for and protected.

One more opportunity to improve our security systems
We have been thus far protected by the safety, safeguards and security measures implemented. We still have one more opportunity to improve our security systems, implementation and cooperation practices at all levels. It is hoped that the practical improvements that are now underway, are timely and efficiently responding to the given threat.

Efficiency of the established security measures and operations must be proven.
Preconditions for the efficient co-operation of all the security operatives should be further studied and possible obstacles of co-operation should be identified. It may be necessary, in some cases, to revise regulations, attitudes, and/or processes. Also, methods to assess the effectiveness of the security systems and practices should be developed.

Knowledge creation support team to be established
To support the authorities responsible for security operations a so called Delphi-group should be established. Its main duties were to make sure that decision makers and other security operatives have not missed situation relevant information in assessing the threat and in considering possible consequences of the decisions.

Conventional risk assessment is to be complemented with new methods.
Conventional risk assessment and evaluations use probabilistic approaches, but in this case the information available is insufficient to support entirely such an approach. For example there is no basis to assign a probability measure to the frequency of an attack. A new approach and set of methodologies should be developed and tested for this new dynamically changing situation.

References

- ✓ Delphi method. Wikipedia, http://en.wikipedia.org/wiki/Delphi_method.
- ✓ Director of National Intelligence, USA, The Inaugural Report of the Global Maritime and Air Com-munities of Interest Intelligence Enterprises, November 2009.
- ✓ Eikelman, I. and Selnäs, Ö. Editors. Final report from the NKS NordThreat seminar in Asker, Norway 30 and 31 October 2008.NKS 206.
- ✓ Ezell, B.C., Bennett, S., von Winterfeldt, D., Sokolowski, J., and Collins, A.. Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis, Vol. 30, No. 4, 2010.
- ✓ Ferguson, C.D."Influence diagram analysis of nuclear and radiological terrorism." in Unconventional Weapons and International Terrorism - Challenges and new approaches. Edited by Magnus Ranstorp and Magnus Normark. Routledge, 2009.
- ✓ The Finnish Security Police 2008 - 2010. Helsinki University Print 2009.
- ✓ Harrison, John. International Aviation and Terrorism. Evolving threats, evolving security. Routledge 2009.
- ✓ Hoffman, B. 2005. "Does Our Counter-Terrorism Strategy Match the Threat?" Testimony presented before the House International Relations Committee, Subcommittee on International Terrorism and Nonproliferation on September 29. 2005.
- ✓ National counter-terrorism strategy. Ministry of the Interior Publication 24/2010. Ministry of the Interior 2010.
- ✓ Karhu, P.. Power Point Presentation Hyvinkää, June 2009.
- ✓ Krogars, M., Verkostoilla kriisinhallintaan. Väitöskirja. Ankkurikustannus Oy, Vaasa. 1995 (in Finnish).
- ✓ Mustonen R. "Radioactive contamination in residential areas" in Airborne Radioactive Contamination in Residential Areas. Radioactivity in the Environment, vol.15, Elsevier 2009.
- ✓ NTI. Radiological Terrorism Tutorial: Intro to Radiological Terrorism. http:/www.nti.org/h_learnmore/radtutorial/
- ✓ The Nuclear Threat Initiative- NTI, Radiological Terrorism Tutorial.
- ✓ Nordic Nuclear Safety Research - NKS. Final report from the NKS NordThreat seminar in Asker, Norway 30 and 31 October 2008.
- ✓ Okko, O. Implementing nuclear non-proliferation in Finland. Regulatory control, international cooperation and the Comprehensive Nuclear-Test-Ban Treaty. Radiation and Nuclear Safety Authority - STUK. Annual report 2008 STUK B-100, March 2009.
- ✓ Ranstorp, M., Normark, M. (editors). Unconventional Weapons and International Terrorism - Challenges and new approaches. Routledge, 2009.
- ✓ Sinkko K. Nuclear emergency response planning based on participatory decision analytic approaches. Radiation and Nuclear Safety Authority - STUK, STUK-A 207, 2004.
- ✓ Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack.
- ✓ TE-SAT 2009, EU Terrorism Situation and Trend Report, Europol.
- ✓ Valtonen, V., Turvallisuustoimijoiden yhteistyö operatiivis-taktisesta näkökulmasta. Väitöskirja. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1: N:o 3/2010 (in Finnish).
- ✓ Varjoranta, Tero. Oral communication. 2010.

Appendix I: List of Items Dealt With in the Interviews

The interviews were made keeping in mind the following themes:

- preventive measures against CBRN-threat
- reaction against threat
- control of the situation when the threat has realized
- dealing with the consequences.

1. The role of the interviewed person in the organisation. Which are his/her main duties.

2. What are the characteristics of the challenge (terror against civil aviation associated with NR-materials) we are facing?

3. What is the difference between the new challenge and ordinary threat?

4. The role of STUK/organization in the new challenge? What should be changed?

5. Which are the stakeholder groups?

6. What are our expectations from our stakeholders?

7. What are our stakeholders expecting from us?

8. What new actions should be launched?

9. What kind of obstacles are expected?

10. Any other issues which should be taken into account?

Appendix II: International Instruments

- ✓ NPT: The Treaty on the Non-proliferation of Nuclear Weapons INFCIRC/140 (FTS 11/70)
- ✓ Safeguards Agreement between the non-nuclear weapon states of the EU, the Euratom and the IAEA (INFCIRC/193), EIF 1995 & Additional Protocol (AP) to the INFCIRC/193, ratified 2000, EIF 2004
- ✓ CPPNM: The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1 (1980), and the Amendment to the Convention (2005)
- ✓ International Convention for the Suppression of Acts of Nuclear Terrorism (2005)
- ✓ ENAC: Convention on Early Notification of a Nuclear Accident, INFCIRC/335 (1986)
- ✓ ENAC: Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, INFCIRC/336 (1986)
- ✓ UNSC-1540 (2004), Counter Proliferation of CBN Weapons
- ✓ UNSC-1624 (2005), Prevention of Terrorist Acts
- ✓ UNSC-1373 (2001), Suppression of Financing of Terrorist Acts
- ✓ Code of Conduct for Safety and Security of Radioactive Sources, IAEA (2004)
- ✓ Guidance on the import and export of radioactive sources, IAEA (2005)
- ✓ The Comprehensive Nuclear-Test-Ban Treaty (FTS 15/2001), ratified by Finland in 1996
- ✓ 2001 EU legislation (Council Decisions, Directives) enforced by national legislation and implemented by competent authorities
- ✓ IAEA's, ICAO's and IATA's respective binding and guiding regulations.

Juha Rautjärvi, Mikko Valkonen and Martti Annanmäki: Prevention Measures and Consequence Management of Radiological Threats

1. Introduction

1.1 General

In our first Aether article (Rautjärvi 2010) the focus was on the threat caused by the terrorists that may use nuclear and radiological substances for terrorist purposes. The study aim was to understand better the threat of terror when NR-materials (nuclear and radioactive) are used, to disclose conditions and circumstances that may need further improvements, to provide ideas about the indicators and indications which could lead to an early detection of activities which may be foregoing a terrorist act. Ideas about the necessary abilities and capabilities to ensure the adequate preparedness were developed. Also questions were raised how to ensure adequate preparedness, efficient management of the situation and possibilities to effectively take care of the consequences. Civil aviation, including the airport and the logistics serving the airport and the planes was considered to be the target.

It was found out that there is plenty of NR-material available. It was also found out that the use of nuclear and radiological materials for terrorist purposes is possible and some terrorist groups have considered using these materials for their purposes. There are in many countries significant amounts of suitable nuclear and radiological materials in vulnerable conditions in facilities and storages. The threat of terrorists using such materials exists. Why have these potentials not been used by terrorists? The answer is not easy. It is not possible to provide any predictions of terrorist attacks and give associated probabilities. A conservative assumption may provide good guidance in this situation.

The nuclear and radiological threat against civil aviation is perceived as real one taking into account the evolution of terror against civil aviation since the end of the 60's, including the current events. The use of nuclear and radioactive materials against the plane, airport facilities, people and the services is a possibility that must not be ignored.

About 20 Finnish security and safety experts were interviewed and these interviews gave insights about the attitudes and about the present state of affairs. Experts included workers from STUK, Finavia, Rescue Services, Finnair, Police, Finnish Security Police, Finnish Defence Force, etc. These interactions contributed to the results reflected in the 1st report and provided direction for the work aimed at addressing the issues relevant for this 2nd report and follow-on activities.

We hope that the work undertaken by STUK within the Aether project contributes positively to the implementation of the national strategy and improvement of the efficiency of the implemented security systems and associated arrangements, including enhancement of co-operation.

In connection with this work further findings were made regarding the use of nuclear

and radioactive material in crimes/acts of terror. That information has not been elaborated in this report because it is not directly relevant to the subject matter. A short summary, however, is given in annex I.

2. Scope of the Study

This article seeks to identify means and ways to improve the possibilities to prevent, to manage the situation and to prevent the consequences of a terrorist attack against civil aviation. Further to that the aim is, in the areas where improvements are needed, to contribute to further development and implementation of security systems and arrangements. The work is performed with full awareness of the sensitivities associated and appropriate precautions are taken by the parties so that sensitive information is not disclosed nor disseminated.

The preliminary results obtained in the interviews were processed first through an enquiry in which experts (mostly the same group which were interviewed) rated the statements obtained from the interviews and then the results were processed in a workshop. The overall outcome was re-evaluated against the results obtained in the exercises of the Aether-project. The findings were communicated to the responsible security operatives for consideration of required follow-on actions. The work undertaken and status of these actions will be reported separately.

The findings of the above-mentioned study have been compared with documented national and European strategies against terrorism in order to assess the relevance of the findings in implementation of the strategies. The project work is seen as one of the ways the national and European strategies are put into practice.

In connection with this study some methods and measures were identified and briefly assessed regarding the possibility of using these in risk assessment as well as in assessing the vulnerabilities of civil aviation, including security systems and arrangements.

Particular attention was directed to the efficiency of the operation and co-operation of the security operatives on all levels. Also signals indicating attempts of terrorist acts were developed and discussed. New projects were identified to enhance efficiency in knowledge creation and operative decision-making and response to evolving terrorist threat.

3. Main Findings of the Interviews and Related Enquiries

Our first paper identified a list of issues which were considered by our expert group to be of great importance when fighting terrorism. The list covered about 30 issues. To further elaborate these issues an inquiry was arranged and a questionnaire was sent to a group of 21 experts mostly the same who were interviewed in the first phase.

The experts were asked to rate the issues presented in the form of statements on the scale from 1 to 5, 1 meaning that he/she fully disagrees, 2 meaning that he/she disagrees, 3 meaning neutral position, 4 meaning that he/she agrees and 5 meaning that h/she fully agrees with what was stated.

The results of the formal enquiry are presented in the annex II. In the results there might be a slight bias due to the fact that so many experts from STUK were involved. The issues identified in our first article were also monitored in the PAE (Project Aether Exercise). During the exercise issues emerging from the interviews and the formal enquiry were discussed.

In connection with the exercise a group of experts was invited to meet for one day to discuss the findings and their implications. Particular attention was paid to a possible need for further work to obtain concrete prove about the way how these findings need to be taken into account. The attention is in enhancing the efficiency and effectiveness of the security operations aimed at preventing and responding to the evolving threat characterized by unexpected outcomes.

In order to ensure the added value, the sustainability of development effort undertaken, the work of the STUK research team will continue still within the scope of this project.

Following conclusions are drawn from the interviews and enquiries:

1. STUK should finalize or prepare the following actions and documents: Database covering such radionuclides which can or might be used in criminal acts and guidance dealing with terrorist incidents. STUK should improve its knowledge about the needs and capacities of other security operatives to be in a better position to provide expected expert support to its stakeholder groups. Furthermore STUK should arrange enhanced training to its employees and, as required, to its stakeholders. It is evident that additional resources should be made available in order to meet the expressed needs. The guidance should also include public information taking particularly into account that the Police have primary responsibility to inform the public during the ongoing operation. However, it is emphasised that STUK is always the competent authority when radiation safety, safeguards and nuclear security are concerned.

2. Guidance on RN-incidents should be prepared for security operatives in the terrorist related incidents. Also guidance for first responders should be prepared (rules of thumb). In order to ensure efficient operation in prevention, detection and response, the guidelines should be prepared in good co-operation between the security operatives. Radiation protection related matters should be included into the respective rules of thumb.

3. To assure effective co-operation the guidance by the different security operatives should be made compatible. The guidance should be implemented and tested in common "workshops". Training and exercises should be arranged to achieve organizational readiness which does not depend on single individuals.

   National counter-terrorism strategy emphasizes the importance of revising the authorities' security and contingency planning processes for the fight against terrorism in order to ensure that necessary terrorism-related information is available for use in local security planning.

4. Measurement devices and protective equipment needed in the RN-incidents should be purchased. Respective training should be arranged. Taking into account the nature

of the threat and objective of ensuring the efficient management of the situation it is important that the competent authority STUK is able to carry out its monitoring and verification work together with other first responders.

5. Laws and regulations which relate to the security of civil aviation should be thoroughly reviewed.

   This statement is consistent with the one in the National counter-terrorism strategy which identifies the need to establish what possible amendments should be made to the legislation on terrorist financing and training and to the legislation on information exchange and executive assistance between the authorities, and to prepare amendments which are necessary.

6. To prevent the civil aviation related RN-terrorism effective procedures should be developed to detect and systematically process so called "indicating signals".

The National strategy requires that a counter-terrorism working group assesses the terrorism situation on a regular basis. Having done this, the working group may propose measures to be taken by the authorities to undertake the required work on combating terrorism.

In general, it may be concluded that the National counter-terrorism strategy is already well influencing the ways of thinking and is mobilizing the required activities of different security operatives. It is recognised that the presence of an active, knowledgeable and capable adversary calls for complementary approaches and strategies and new capabilities to be able efficiently to cope with the evolving threat and unexpected outcomes.

4. Tools to Analyze Threat and Improve Countermeasures

The national strategy manages attention to different ways terrorism can be addressed, e.g. trying to prevent violent radicalization, improving information exchange between different authorities, taking account of terrorism-related factors in security and providing a real-time picture of the security situation that clearly identifies terrorism-related issues. However, in this context the role of private partners is essential and information exchange and co-operation must be extended also to these partners.

Co-operation between authorities is considered essential to counter-terrorism in order to make the best possible use of the counter-terrorism resources available to the authorities and relevant organizations, including for example airports and technology holders providing measurement and monitoring services.

In the EU strategy the work to raise collectively standards in transport security is in focus. The protection of airports, seaports, and aircraft security arrangements need to be enhanced in order to deter terrorist attacks and address the vulnerabilities in domestic and overseas transport operations. However, the operational environment may be improved when new orders, procedures and instructions will come into force, tentatively in 2012. One of the key priorities is to develop risk assessment methods and tools to be in a better position to build the required

capabilities to prevent and to respond to an attack.

The findings and observations resulting from this work and reported below are aimed at providing incentives, ways and means to enhance and, as necessary, to improve the elements of the security system.

Some of the observations may well induce defensive reactions and even possibly cause bad feelings. It is understandable. We have good reasons to believe that our security system is well functioning. The question is does it work in case of terrorist engagement where CBRN materials are used. It is underlined here that the aim is not to criticize the system, the operations and the operatives, but to understand better the nature of the challenge and to learn to cope with the given situation efficiently.

Particular importance is placed on the following observations:

1. Identification and collection of any data and information deemed relevant to security and to the situation is an essential task for all security operatives, public and private alike.

2. Creation of actionable knowledge for the decision making in the situation where threat is evolving and where security needs to evolve too is not a trivial challenge. New approach is to be taken to respond efficiently to this need.

3. Generation and maintenance of a dynamic and credible picture about the evolving situation shall not be undertaken by the political or operative managers but be provided for their use by a separate expert team tasked to create a knowledge basis for the strategic and operative decision-making.

4. Risk assessment in case of terrorism appears to be a particularly complex matter. The methodologies which are used to assess risks, such as PRA, appear not to be alone applicable. New methods need to be developed to support expert judgment and decision making. In Finland the risk assessment is based on DBT (design basis threat) methodology. This may well bring some new ideas.

5. Normal functions and structures of the society, including those of the security relevant public and private institutions and organizations, must be tuned to contribute efficiently to prevention, detection, response and consequence management. These functions include also planning, development, testing and any kind of exercises aimed at building capacity that is providing required continuous services and available for action at any given time.

6. Security culture, the attitudes, the way of interactions, in short the praxis need to be enhanced not to continue running high risk of failing to address appropriately the new complex challenge embedding most undesirable consequences. The enhanced code of conduct needs to be developed to ensure efficient performance of given tasks. And this is to be incorporated as a standard operational procedure of every party.

7. Communication and presentation tools need to be further developed, tested and their performances demonstrated to provide efficient support for critical security functions identified in the above points. The real situation picture is the basis for tactical, operational and strategic management and decision-making processes.

8. The policies of the institutions and organizations guiding the normal resource allocation need to be modified to accommodate the resource needs arising from the new challenges.

With reference to the above points the following three different studies are briefly summarized:

- Probabilistic Risk Analysis and Terrorism Risk by Barry Charles Ezell, Steven P. Bennett, Detlof Von Winterfeldt, John Sokolowski1, Andrew J. Collins
- Nuclear Emergency Response Planning Based on Participatory Decision Analytic Approaches by Kari Sinkko
- Co-operation of Security Operatives by Vesa Valtonen.

✓ *4.1. Probabilistic Risk Analysis and Terrorism Risk*

Since the terrorist attacks of September 11, 2001, and the subsequent establishment of the U.S. Department of Homeland Security (DHS), considerable efforts have been made to estimate the risks of terrorism and the cost-effectiveness of security policies to reduce these risks (Ezell 2010).

For more than 30 years, probabilistic risk analysis (PRA) has been a major tool for assessing risks and informing risk management decisions by government and industry, in areas as diverse as environmental protection, industrial safety, and medical decision-making. Applications of PRA to terrorism risks are new, however, and not uncontroversial (Ezell 2010).

In the article a broad view of PRA is assumed, including any probabilistic approach involving tools like event trees, fault trees, and decision trees. Other tools such as game theoretic approaches and system dynamics, which may prove to be useful in dealing with intelligent enemies are also introduced. A major challenge in risk analysis of terrorism seems to be the fact that terrorists, unlike nature or engineered systems, are intelligent adversaries and may adapt to our defensive measures (Ezell 2010)).

The authors agree that multiple approaches, perhaps in combination are needed to address the complex issue of terrorism, including event trees, decision trees, fault trees, Bayesian belief networks, game theory, and agent-based models, among others. In this context, however, PRA and event trees have been shown to be useful approaches for assessing terrorism risks, especially for creating a baseline comparison of these risks (Ezell 2010).

Decision trees, like PRA and all approaches, have limitations and are not on their own a complete solution. In the case of applications for terrorism risk analysis, the NRC's decision tree approach has limitations that may be difficult to surmount upon implementation to include

the fact that adversaries' objective functions and level of ability to predict tree outcomes are unknown and difficult to estimate (Ezell 2010).

PRA (or PSA - Probabilistic Safety Analysis) is a well known tool and is routinely used when assessing e.g. nuclear power plant related risks. When PRA is made the respective activity e.g. nuclear power plant is modelled and such combinations of events will be identified which can lead to a severe reactor accident. The modelling is mostly based on the event trees or decision trees. Usually the modelling is a demanding project requiring several working years to be completed.

The airport, all the activities included, could be considered to be a single facility and its vulnerabilities could be assessed using PRA-approach. It must be kept in mind that the airports are of different size. There are small airports (e.g. Jyväskylä airport), medium size airports (e.g. Helsinki-Vantaa airport) and big airports (e.g. Frankfurt airport). The division here is arbitrary and it is made only to give a picture what we are proposing.

First PRA could be made for a small airport and later on in a separate project would be assessed the possibilities to scale up the method and model to a medium size airport and then to a big airport.

✓ *4.2 Knowledge Creation and Management Enabling Efficient Security Operations*

The National strategy puts particular emphasis on cooperation between authorities to be efficient in counter-terrorism operations and in order to make the best possible use of the counter-terrorism resources available to the authorities and relevant organizations that include also private partners engaged in these operations.

Sinkko in his theses (Sinkko 2004) developed methods and techniques for evaluating protective action strategies in the case of a nuclear or radiological emergency. This was done in a way that the concerns and issues of all key players related to decisions on protective actions could be aggregated into decision-making transparently and in an equal manner.

An approach called facilitated workshop was tailored and tested in the planning of actions to be taken in case of a major nuclear power plant accident. Workshops were organized in which all key players were represented, i.e. the authorities, expert organizations, and the industry. It was considered essential that the set-up strictly follows the decision-making process in which the key players are accustomed.

The realistic nature and the disciplined process of a facilitated commitment to decision-making yielded up insights in many radiation protection issues. Insight was also gained in what information should be collected or subject studied for emergency management.

The experience gained strongly supports the format of a facilitated workshop for tackling a decision problem that concerns many different key players. The participants considered the workshop and the decision analyses very useful in planning actions in advance. It was concluded that a facilitated workshop is a valuable instrument for emergency management and in exercises in order to revise emergency plans or identify issues that need to be resolved.

The general goal in all these kind of methods is that key players would be better prepared for an incident situation. All participatory methods, when practiced in advance, also create a network of key players.

A facilitated workshop (also called a decision conferencing) is an interactive approach to group decision making in order to generate a shared understanding of the problem and to produce a commitment to action. A facilitated workshop combines decision theory, group processes and information technology over an intensive, up to two- or three-day session attended by key players with different fields of expertise. The original arrangement is that a small group of key players is seated in a semicircle to discuss the problem through a facilitator who aids the group's discussion and sharing of knowledge. In the background an analyst, using decision-aiding technology, models the group's views.

Decision analysis had a major role in facilitated workshops. It guided focused discussions and offered a structured way to tackle the problem. An important feature was also that it allowed participants to try different judgments to see the consequences without a final commitment. This allowed them to re-evaluate their opinions. The applied facilitated workshop method was considered to fit in accustomed decision-making process, to offer a forum for constructive dialogue and to be open, equitable and auditable.

Observations made during the Aether exercise suggest the following:

- It is very important that there is a facilitated knowledge creation process in place long time before the situation escalates.
- The character qualities and relationships of the parties engaged in knowledge creation must be of the quality that enables addressing thoroughly any information and issues emerging.
- The knowledge creation process must be facilitated in order to be able to progress towards a coherent picture about what is actually happening. The process facilitator must maintain attention managed on one hand to the objective facts and the extent to which these are proven at any given time and, on the other hand, to the elements of subjective nature and to a need to enable development of a coherent judgment as to how close at true the propositions may be.
- The communicator of the knowledge creation process must keep the political and operative parties appropriately informed about the situation and about what is happening at any giving time and what is expected to happen and what can be ruled out.
- Information technology must be developed and implemented to support documentation, communication and presentation as well as evaluation, to ascertain what actually happened and to determine how it did work. The information technology and the knowledge management tools must also be able to facilitate continuous learning and simulation of various strategies of adversaries.
- The knowledge creation process must be separated from the political and operative (pragmatic) decision process in order to enable, on one hand, efficient creation of a coherent picture and knowledge based premises for action, on the other hand, pragmatic decision-making, including understanding of pos-

sible consequences of different perceived futures.

- Knowledge creation process must be perceived and conceptualized, instrumented and maintained operational as a standing element of national security services.
- Appropriate tools need be developed to facilitate cost-efficient operation and maintenance of such service. Public and private partners are to be identified and engaged to provide this service. The same is valid for the data and information services that will provide the input material for the knowledge creation process.

✓ *4.3. Co-Operation of Security Operatives*

National strategy identifies co-operation between authorities as one of the essential conditions to counter-terrorism in order to make best possible use of the counter-terrorism resources available to the authorities and relevant organizations. Naturally this includes also all those organizations and operatives that are engaged in and are responsible for certain security system functions.

Valtonen in his theses (Valtonen 2010) investigated co-operation of security operatives and how it is manifested. The study was based on co-operation exercises and projects and on query of experts in which the Delphi-method was applied.

Co-operation of security operatives is based on responsible conduct, management, confidentiality and appropriate allocation of resources. Foundations of successful co-operation of security operatives are effective co-operation of public authorities, and effective ways of co-operating on all levels. It is supported by the international co-operation.

Security is regarded more important than e.g. economical competition. Prerequisites for security operatives to co-operate successfully are competence and reliability. Personal contacts, commitment and a co-operative way of thinking are important factors on individual level. It is evident that improvement is needed in ability and skills to co-operate. These include co-operation processes such as sharing of information, development of situation awareness, measurement and feedback processes and common terminology.

Factors obstructing successful co-operation are those normally encountered in human relationships. These are power related factors, professional disagreement, emphasizing the importance of own activities etc. They can block setting common goals and prevent co-operation in practice.

Observations made during the Aether exercise are as follows:

- The conditions and relations experienced during the Aether project confirmed the findings of the research work referred to.
- As long as the exercise is planned and implemented strictly in accordance with the predetermined script that is known to all and adhered by all the participants feel comfortable and operate efficiently.
- When deviations are experienced the disturbances are there. The attention is diverting from the issue at stake to the exercise process, actors and non-

compliance with the expectations. Thus, making it not possible to maintain the attention managed on the subject matter and ensuring efficient and purposeful use of all resources and their capacity.

- It appeared also not very clear what is expected from the competent authority, like STUK, in supporting operation. What level of pro-activity is needed in an emergency situation when the time is running and no instructions are received from the operative management.
- If information about the threat refers to terrorism and C - B means but not explicitly to R or N, should STUK be mobilized and to what extent? It is suggested that the determining attribute is the terrorism and, as a matter of principle, any of C,B,R or N cases shall trigger relevant activities and response for all eventualities.
- It is suggested that within the time-constrained situations, like in this case the information on which the actions could be based is required within 2-3 hours, the competent authorities must be fully operational with the required capacity and bring it to the scene to be in a position to provide immediate support, when requested. This way the efficient communication will be also ensured.
- The exercise offered ample opportunities to experience the discomfort and destructions caused by an unintended condition. Besides, it caused additionally that some of the vital administration functions (police and rescue services) were not in a position to participate in the exercise.
- The Aether project exercises can be considered as valuable experiences offering opportunities to learn about the conditions and circumstances which are influencing the possibilities to build efficient practices for the situations that are characterized with constrained time, scant information and evolving threat.
- National strategy emphasizes incorporating to everyday functions and relations such security relevant elements, operations and procedures that will make it possible to efficiently take care also of such situations where a knowledgeable and active adversary is in action. This condition challenges the current attitudes, exercise plans and experiences. Are all these enabling the required capacity building and preparedness?

UN Security Council considered the security situation in 2004. Terrorism and possible use of CBRN materials for terrorist purposes and particularly the possibility that dangerous CBRN materials in various states may get into the hands of non-state actors would thereby endanger the safety and security of the world. Security Council came to the conclusion that the risk is there and passed the resolution 1540 under Chapter VII. That obliges all states, international organizations, like IAEA, legal and natural persons to take care of the security deficits and to avoid everything that may hinder or obstruct efficiency. Particularly the resolution calls authorities to be in contact with industry, private partners to enhance the possibilities to combat efficiently CBRN terrorism.

The resolution is a self-executing obligation binding all. Nobody can refuse to cooperate without running into a risk of being in non-compliance.

5. Role of Warning Signals, Indicators and Indications in Knowledge Creation

National strategy puts emphasis on the importance of intelligence work in detecting and pursuing terrorists. Also coordination and sound analysis of information is important. As part of basic preparedness, measures will be taken to ensure that security authorities have sufficient powers to prevent terrorist offences. In Finland, counter-terrorism should be based on the early identification of terrorism-related phenomena and the prevention of terrorist acts. Early identification of threats is the key-word in keeping preparedness on a sufficient level.

The early detection of indicating signals and indications and their analysis play a significant role not only in detecting and pursuing terrorists but also in understanding the CBRN terrorism-related phenomena, the motives, potential capacity, level of preparedness and target and timing of possible act.

The approach described in the Figure 1. below may well improve possibilities to timely interfere and influence the adversary actor, to enhance possibilities to prevent successful information and material acquisition, improve possibilities to identify the terrorists and to prevent their possibilities to carry out successful acts. The approach outlined here is aimed at enhancing also possibilities of the security operatives to understand the nature of the evolving threat and to take care of the necessary precautionary measures timely. The approach assists in determining the point of preparedness, the assets for attack are in position, it is just a question of will and timing. The aim is to obtain as reliable information as possible also about the target and possible consequences of an attack.

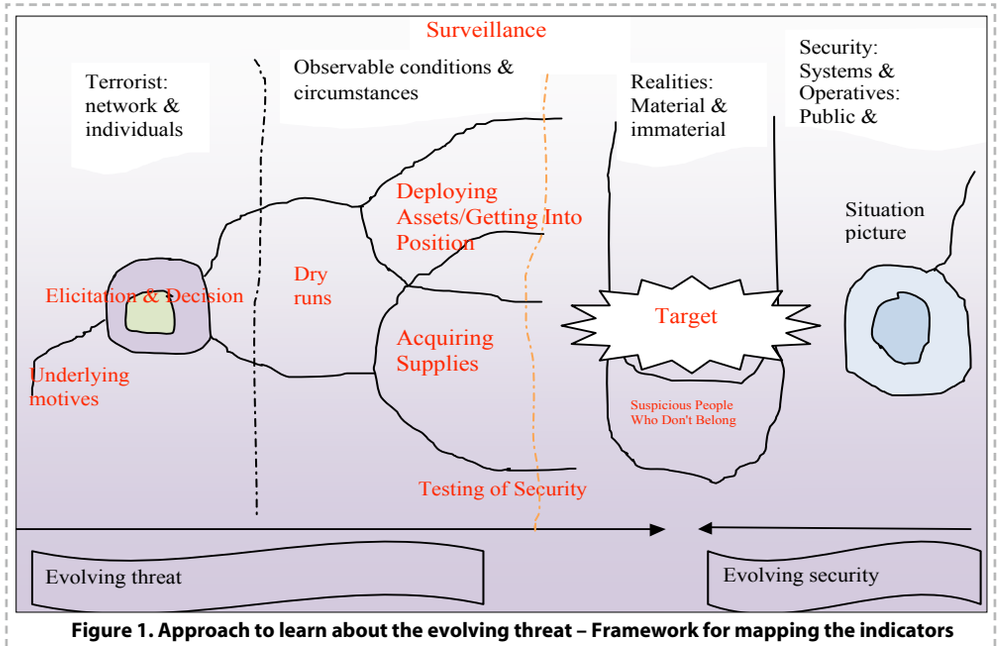


Figure 1. Approach to learn about the evolving threat – Framework for mapping the indicators

The terminology used in the above figure is developed by the Metropolitan Transportation Authority of New York and was made public by the ASIS public website. The seven signs of terrorist activity can be used to provide structure for the indicators and indications that were developed within this project. Three lists of detailed indicators and indications are one of the outcomes of this research and development work. These lists are however confidential and may not be published, and are therefore not attached to this report.

✓ *5.1. New Angle of View Is Needed*

ASIS (ASIS International) claims that earlier used randomly received weak signals have not been successful in preventing acts of terror. A new approach is needed - the terrorist's point of view. What is needed for the act of terror to be successful? In order to be able to become aware of what is happening the process of a terrorist act should be structured. A dynamic picture should represent the elements and conditions that need to be there and be taken care of so as to be in a position to launch a successful terrorist attack. The analysis and evaluation of indications and indicators would disclose the evolving nature and status of various terrorist activities. Information about the timing and targeting could also emerge. Managing attention to an evolving threat, to all indicators and indications would make it possible to mobilize timely the countermeasures.

✓ *5.2. Weak and Strong Indicating Signals*

The signals indicating that a terrorist activity may be underway can be categorized as weak or strong. Whether the signal is weak or strong depends on the quality of the information and on its origin. Each piece of information should be authenticated and assessed. In order to prove their relevance and value follow-on activities may be required. In principle any proven, verifiable condition and fact can be considered as a strong indicator. Expert analysis and evaluation is required to impute the value on the non-verifiable indications. As a consequence it would be possible to create and maintain a coherent picture about the evolving threat, to understand the degree of readiness and to have an idea about the targets.

In order to be able to address such complex situations systematically a new methodology, assessment process and procedure need to be developed, as discussed earlier.

✓ *5.3. Observing Indicating Signals*

The monitoring of possible terrorist motives and activities is an obligation to all. Responsibilities to monitor different signals should be allocated to different security operatives which would take these into account while carrying out their normal duties. The findings should be timely reported to the competent authorities and to the analytical and evaluation process.

✓ *5.4. Processing the Indicating Signals*

It appears evident that a special body should be established to compile and process the weak and strong signals. All the security and other operatives send information about observations to this body, which collects these and creates a situation awareness picture for decision making.

The knowledge creation process and the political and operative decision making should be separated. A continuing effort is required to monitor the signals and to create and maintain a coherent picture about the evolution of threat. Such work should not be constrained by any other motives. The principal relationships with the political and operative decision making and leadership are described in Figure 2.

A special group – Delphi-group – should be established to analyze and assess the indicating signals. The Delphi-group should consist of the experts of all the security operatives which have a central position in the security and safety of aviation. The duty of the Delphi-group is to use observed indicating signals to assess the situation as a whole and make recommendations of the actions to responsible security operatives.

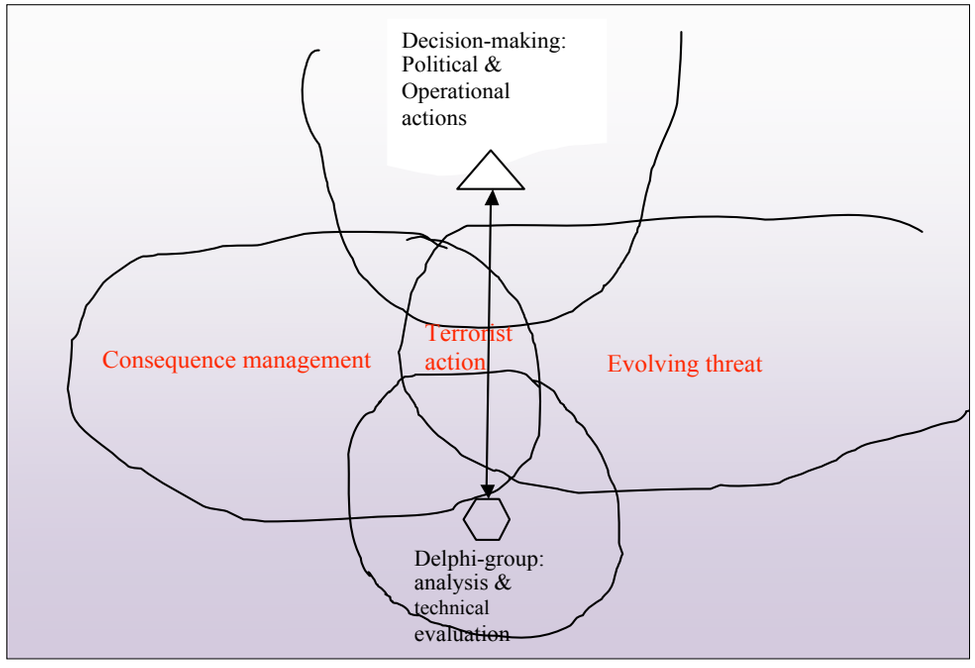


Figure 2. Delphi-group is creating actionable knowledge for the political and operative decision-making and action.

6. Main Conclusions

1. National counter-terrorism strategy and the elements of respective EU strategy are being operationalized.

2. Implications of the new challenge are not fully understood yet. The concepts are recognized, the perception about the implications is weak, structures and procedures are not yet changed. Resources, however, are being reoriented, some partly allocated. 3

3. Attitudes need to be reformed and resources redirected to accommodate new coping strategies and partners. A code of conduct is to be agreed to ensure efficient cooperation in planning, implementation and exercising security functions.

4. New methodologies for risk assessment need to be developed to cope adequately with the complexity inherent in the terrorist threat. The scenarios that need to be efficiently addressed should be identified, if not done yet. The society must be prepared to face the consequences of the risk by applying the existing emergency plans.

5. The security system functions aimed at addressing terrorism (intelligent, non-state adversaries in action) must be embedded to the daily work routines of the security operatives to be efficient. This is the only way the evolution of the threat can be understood and the situation managed efficiently - thus contributing to the establishment of the new security culture.

6. The knowledge-creation process should be restructured to be able to generate and maintain a credible and dynamic picture about the evolving situation. – This enables us to be in a position to maintain political actors and security operatives aware of the evolution and the situation at any given time. Knowledge creation and decision-making need to be kept separated (see Figure 2.). While developing and evaluating the situation, the picture should be anchored to realities, to prove indicators and indications as well as to the motives of the potential terrorists (see Fig. 1).

7. Information technology tools need to be further developed, and ultimately also used, to facilitate cost efficient data and information collection, analysis and evaluation, sharing of the created knowledge, decision-making and security operations. In short, a knowledge-management system needs to be developed and implemented taking particularly into account new leadership structures and the constraints which are associated with sensitive information.

9. The exercises improving and proving the functioning of the existing security systems must be complemented with other type of experiences. The uncertainty and unpredictability should characterize such learning exercises. Motto: It may well function today as intended, but here the question is different, does it work purposefully now!

10. The security operatives trust STUK to provide the required support to ensure efficient detection, response and management of consequences. In particular the following points, additional to the above, were identified in the interviews:

    a) STUK should finalize or prepare the following actions and documents: Database covering such radionuclides which can or might be used in criminal acts and guidance dealing with terrorist incidents. STUK should improve its knowledge about the needs and capacity of other security operatives to be

in a better position to provide expected expert support to its stakeholder groups. Furthermore STUK should arrange enhanced training to its employees and, as required, to its stakeholders. It is evident that additional resources should be made available in order to meet the expressed needs. The guidance should also include public information taking particularly into account that the Police have the primary responsibility to inform the public during the ongoing operation. However, it is emphasised that STUK is always the competent authority when radiation safety, safeguards and nuclear security are concerned.

b) Guidance on RN-incidences should be prepared for security operatives in the terrorist related incidences. Also guidance for first responders should be prepared (rules of thumb). In order to ensure efficient operation in prevention, detection and response, the guidelines should be prepared in good co-operation between the security operatives. Radiation protection related matters must be included into the respective rules of thumb.

c) To assure an effective co-operation the guidance by the different security operatives should be made compatible. The guidance should be implemented and tested in common "workshops". Training and exercises should be arranged to achieve organizational readiness, which does not depend on single individuals.

National counter-terrorism strategy emphasizes the importance of revising the authorities' security and contingency planning processes for the fight against terrorism in order to ensure that necessary terrorism-related information is available for use in local security planning.

d) Measurement devices and protective equipment needed in the RN -incidents should be purchased. Respective training should be arranged. For taking into account the nature of the threat and objective of ensuring the efficient management of the situation it is important that the competent authority STUK is able to carry out its monitoring and verification work together with other first responders.

e) Laws and regulations which relate to the security of civil aviation should be thoroughly reviewed.

This statement is consistent with the one in the National counter-terrorism strategy which identifies the need to establish what possible amendments need to be made to the legislation on terrorist financing and training and to the legislation on information exchange and executive assistance between the authorities, and to prepare such amendments as necessary.

f) To prevent the civil aviation related RN-terrorism adequate procedures should be developed to detect and systematically process so called "indicating signals".

The National strategy requires having a new counter-terrorism working group to assess the terrorism situation on a regular basis. Having done this, the working group may propose measures to be taken by the authorities to undertake the required work on combating terrorism.

In general, it may be concluded that the National counter-terrorism strategy is already well influencing the ways of thinking and is mobilizing the required activities of different security operatives. The awareness of the different implications to daily routine work is increasing. It is recognised that the presence of an active, knowledgeable and capable adversary calls for complementary approaches and strategies, new capabilities to be able efficiently to cope with the evolving threat and unexpected outcomes.

7. Recommendations for New Projects

1. Knowledge management system

Information technology tools are to be developed and demonstrated that enable to organize and operate, validate and authorize changes to the above services in a cost-efficient manner.

The environment in which security operatives are providing their services is continuously changing, the dangers and threats are evolving and so are the security systems and operative environments. Skilled and trained human resources are required, capacity building through training and education and transferring knowledge must be seen as an integral part of normal daily security operations.

The challenge is to maintain the human resources needed to sustain the secure functioning of the society under all circumstances.

The learning, education and training as well as working by use of network based knowledge management system would make the performance efficient and more attractive also for the new generation operatives, facilitate exchange of human resources and contribute to the development of educational quality benchmarks, thus enabling the exchange of learning experiences. Access to existing knowledge would be improved, and sharing of it would contribute to development and innovation, thereby enabling the evolution of the security system and its functions. – Thus, securing its efficiency.

The establishment of the knowledge-management system would enable to link the past information to the current assessment process and so benefit from existing decentralized sources of information. The system through its dynamic structure would enable to preserve the valuable knowledge for future use, and that without getting disconnected from the factual and judgmental premises of any given knowledge that is used for decision-making.

2. Risk assessment methodology for complex situations

In connection with terrorism the PRA has been used to estimate the risk of terrorism per se. However, keeping in mind potential acts of terror towards aviation and especially towards airports and planes, this tool - PRA - could be used to make a model of the airport and all the

activities there including passengers, personnel of the aviation company, personnel of the airport, airport facilities, services and associated operations. Identification of indicators, indications and verification of their absence, determination of detection systems and capabilities to detect timely significant events are of particular concern.

3. Multidisciplinary team process for knowledge creation

It is suggested to operate a multidisciplinary expert team that will be responsible for creating knowledge relevant to the given situation. The team would be accountable to the political and operative leadership. A code of conduct for the team (Delphi-group) needs to be developed to ensure that adequate conditions and relationships are maintained under all circumstances. The aim is to enable efficient communication, decision-making and security operations also under constrained conditions.

4. Code of conduct

In order to facilitate efficient performance in information collection, communication, the performance of the Delphi-group work and the communication of its results to a decision-making organ a code of conduct is to be developed and implemented in daily work praxis. This would ensure that the dedicated communication and knowledge management system would be efficiently utilized to support the performance.

5. Case study: Security operations at the Jyväskylä airport

In order to learn more about the implementation and operation of the developed concepts and outlined technology support in real conditions we suggest organizing a case study at the Jyväskylä airport, in central Finland.

References

- ✓ ASIS International, http://www.asisonline.org/newsroom/wmd.htm
- ✓ Delphi method. Wikipedia, http://en.wikipedia.org/wiki/Delphi_method.
- ✓ European Union Counter-Terrorism Strategy, November 2005, http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf
- ✓ Ezell B.C., Bennett S., von Winterfeldt D., Sokolowski J., and Collins A., Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis, Vol. 30, No. 4, 2010.
- ✓ Center for Nonproliferation Studies, Monterey WMD Terrorism Database, http://cnswmd.miis.edu/wmdt/
- ✓ Mustonen R. "Radioactive contamination in residential areas" in Airborne Radioactive Contamination in Residential Areas. Radioactivity in the Environment, vol.15, Elsevier 2009.
- ✓ National counter-terrorism strategy. Ministry of the Interior Publication 24/2010. Ministry of the Interior 2010.
- ✓ Rautjärvi J., Valkonen M. and Annanmäki M., Threat of the Nuclear and Radiological Terrorism to the Air Transport, June 2010.
- ✓ Sinkko K., Nuclear emergency response planning based on participatory decision analytic approaches. Radiation and Nuclear Safety Authority - STUK, STUK-A 207, 2004.
- ✓ Valtonen V., Turvallisuustoimijoiden yhteistyö operatiivis-taktisesta näkökulmasta. Väitöskirja. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1: N:o 3/2010 (in Finnish).

Setting up a decontamination line during the Live Exercise.

Annex I

USE OF NUCLEAR AND RADIOACTIVE MATERIAL IN CRIMES/ACTS OF TERROR

The Monterey WMD Terrorism Database is an open source list of worldwide incidents involving the acquisition, possession, threat and use of weapons of mass destruction (WMD) by non-state or sub-state actors.

Maintained by the Center for Nonproliferation Studies' WMD Terrorism Research Program, the database includes more than 1,100 incidents - from 1900 to the present - that relate to the use of chemical, biological, radiological and nuclear (CBRN) materials as possible weapons.

Database contains about 130 such cases where nuclear or radioactive material has been involved in the incident. When a group or individual is responsible for more than one incident over time, each separate attempt to release or use an agent is in this data base recorded as a separate incident. E.g. if an individual has sent letters containing radioactive material to several persons/institutes they all are recorded as separate incidences.

The database categorises the events as **Hoax/Prank** (a deceptive claim in order to frighten target, no direct harm), **Threat** (the motivation of the act is clearly to intimidate and coerce), **Plot** (plans to acquire and use NR-materials as a weapon, but those involved in the plot do not have the agent in their possession), **Attempted Acquisition** (there is evidence to suggest that there was intention to acquire NR-material for use as a weapon), **Possession** (perpetrator has NR-material in possession), **Threat with Possession** (perpetrator threatened to use a NR-substance and actually had the agent in his or her possession) and **Use of Agent** (perpetrator employed or disseminated a NR substance in the commission of a violent act).

Those incidents classified as a Use of Agent are not so many. They can be listed:

- in 1974 in Austria iodine-131 was placed aboard a train
- in 1985 in USA New York city drinking water was contaminated with plutonium-239
- in 1998 in the Russian Federation booby-trapped container with radioactive material was located near railway track
- in 2000 in Japan iodine-125 was dispersed inside the railway station
- in 2000 in Japan envelopes traced with monazite (contains thorium-232) were sent to various government offices
- in 2002 in China iridium-192 was hidden in the office of the business rival
- in 2005 in Belgium threatening letters containing slightly radioactive uranium-238 were sent to some public addresses
- in 2006 a former KGB officer was poisoned using polonium-210
- in 2009 in India in Kaiga nuclear power plant tritium was put inside a water dispenser.
- From another reference (Mustonen 2009):
- in 1995 Chechen rebels partially buried a container with a small quantity of caesium-137 in a park in Moscow.

There are only a few incidents involving nuclear agents or nuclear devices that have been classified as Attempted Acquisition and some incidents which have been classified as Possession Only. One of them was claimed to be SS-20 missile with a powerful nuclear charge and one nuclear bomb lacking some constituent.

It should be taken into account that these lists are not exhaustive because there might have been incidents which are not published for one reason or another.

The list above shows that mostly, when RN-materials are used in criminal acts until today there has been no real threat to the lives of people and only a small amount of possible victims are involved. Only the case where polonium-210 was used was successful from the criminal's point of view.

It might be that generally the threat of terror where NR-materials are used is in many times exaggerated. However, involvement of radioactive materials, including nuclear materials, causes fear that is expected to have significant consequences to the civil society, its functions and particularly to the credibility of its safety, security and safeguards systems and that of the security operatives.

Treatment of a contaminated patient.

Annex II

RESULTS OF THE QUESTIONNAIRE: THREAT OF THE NUCLEAR AND RADIOLOGICAL TERRORISM TO THE AIR TRANSPORT - MAIN ISSUES

Scale 1, 2, 3, 4, 5

Rating: 1 = Fully disagree, 2 = Disagree, 3 = Neutral position, 4 = Agree, 5 = Fully agree.

Characterization of the new challenge

Issue/Statement	Mean
Terrorism is a phenomenon which should be taken into account in all security operations and related activities including their planning	4,4
As a phenomenon terrorism is very creative and ever developing	3,7
Different forms of terror seem to be evolving along with the security measures	3,5
In the civil aviation the use of the NR-material (nuclear and radioactive) in a terrorist act is a potential threat	3,6
Terrorist threat against Finland or Finnish targets is small however, the situation may change rapidly	4,0
Security measures, activities and capacity of the organizations involved should be developed to detect timely and prevent terror acts	4,4
Work conditions of the relevant organizations at the airport should be arranged so that deviations from normal behaviour and procedures will be detected immediately	4,1
Security operatives are in need for special guidance on threat of the NR-terrorism to the aviation industry and air transport	3,7
Decision making structures, responsibilities and communication procedures should be reviewed and conditioned to be able to cope with the evolving threat situations	4,0

Effects of the threat on the role and activities of STUK

Issue/Statement	Mean
STUK's activities and procedures should be developed to take into account the threat of terrorist attacks where NR-materials are used	4,1
Guidance on co-operation should be prepared in collaboration with all other security operatives	4,2
Co-operation should be exercised all phases of the evolving threat included	4,2
Person to person contacts are dominating presently but co-operation between different organizations should be developed and further enhanced	4,1
Forwarding confidential and tacit information may be limited and thus decision making be hampered by all the relevant parties not knowing all the facts	3,8

Present attitudes, processes and actions

Issue/Statement	Mean
Special action plan is needed to monitor situations and control incidents involving radioactive substances caused by the intentional actor	3,0
Emergency preparedness should be developed to cover also acts of terror using NR-substances	4,0
Guidance for first responders should be prepared to cope with the threat	4,2
Finavia has a national security program, as required by the EU statutes, and also a program and relevant guidance for airports. These need to be updated to include also RN-affairs	3,6

What more should be done

Issue/Statement	Mean
Information security, encrypting etc. should be used when sharing information about the terrorism related findings and possible counter-measures	3,6
Information security should not prevent the efficient flow of information	4,4
Guidance should contain preventive measures and operations	4,0
EU should take into account that all the security related regulations should be based on thorough risk-assessments and cost-efficient analysis of the suggested measures	3,5
Chains of responsibilities should be clarified. E.g. which of the authorities is responsible for example, for the decontamination of the airplane and which authorizes the further use of the decontaminated airplane	3,6

Possible obstacles

Issue/Statement	Mean
Resources should be allocated to all the organizations involved to meet the new challenges	4,2
Communication praxis within and between organizations may hinder timely dissemination of information and sharing of knowledge	3,4
Common language (concepts and terms) in all organizations and domestic and international stakeholder groups is needed when facing the new threat	3,7
A special challenge is the use of several languages when making decisions in a very short time period	3,5
Hasty decisions based on non-existing risk analysis should be avoided to prevent adverse side effects, accidents and unexpected costs	4,1
Threatening and exaggeration should be avoided	4,4

Annex III

RADIOACTIVE NUCLIDES WHICH HAVE BEEN USED IN THE INCIDENTS PRESENTED IN THE MONTEREY WMD TERRORISM DATABASE

Radioactive materials used in incidents (use, threat, possession, attempted acquisition, plot)			
Nuclide	Type of activity	Half-time	Comment
Monazite (actually thorium-232, Th-232)	alpha	1,405 10^{10} years	Monazite mineral contains thorium Thorium series starting from Th-232 contains alpha, beta and gamma-active nuclides
Caesium-137 (Cs-137)	beta	30,1 years	Fission product
Tritium (H-3)	beta	12,32 years	Usually produced artificially in nuclear reactor
Uranium-238 (U-238)	alpha	4,468 10^{9} years	Uranium series starting from U-238 contains alpha, beta and gamma-active nuclides
Americium-241 (Am-241)	alpha	432,2 years	Produced artificially in nuclear reactor Used in smoke detectors based on ionization chambers
Polonium-210 (Po-210)	alpha	138 days	Exists naturally. Usually produced artificially in nuclear reactor
Iridium-192 (Ir-192)	beta	74 days	Occurs naturally. Produced artificially in nuclear reactor
Plutonium-239 (Pu-239)	alpha	24 100 years	Produced artificially in nuclear reactor
Strontium-90 (Sr-90)	beta	28,8 years	Extensively used in medicine and industry
Iodine-125 (I-125)	gamma	60,1 days	Used in biological assays, nuclear medicine imaging and in radiation therapy
Radium-226 (Ra-226)	alpha	1601 years	Naturally occurring nuclide in uranium-238 series

Hannu Rantanen: Weak Signals and Early Warning in Aviation Related Emergencies

1. Introduction

Emergencies are extreme events that put lives and properties at risk. They can strike suddenly or they will develop during a longer time. They require immediate response and coordinated application of resources. The effective management of the emergency response places extraordinary demands upon personnel for accurate, timely information in order to make optimum use of limited resources under urgent constraints of time and skills.

The emergencies and threats involving aviation today are multitude. Traditionally the main concerns have been ordinary crashes and occasional hijackings. In recent years there has been more and more attention to potential new types of actions feared to be planned by extreme organisations or individuals. These include also CBRN threats. Large numbers of people pass through airports. Such gatherings present a target for terrorism and other forms of crime due to the number of people located in a small area. Similarly, the high concentration of people on large airliners, the potential high lethality rate of attacks on aircraft, and the ability to use a hijacked airplane as a lethal weapon are supposed to be an alluring target for terrorism.

Responding to complex aviation emergencies in a timely and effective manner, can reduce deaths and injuries, contain or prevent secondary disasters, and reduce the resulting economic losses and social disruption. During these emergencies, responding organizations will confront grave uncertainties in making critical decisions. They need to gather situational information (e.g., state of the civil, transportation and information infrastructures), together with information about available resources (e.g., medical facilities, rescue and police units). There is a strong correlation between the accuracy, timeliness, and reliability of the information available to the decision-makers, and the quality of their decisions. (Mehrotra & al. 2004)

This was clearly demonstrated on Monday 21 February 2005, when Australian State and Commonwealth emergency services were involved in a multi-agency response to a mysterious incident at Melbourne Airport resulting in the evacuation and closure of the southern terminal housing Virgin Blue Airlines. The incident began at around 7.10 am as a medical response to a collapsed female by the Aviation Rescue and Fire Fighting (ARFF) service and concluded shortly after 6.00 pm with the reopening of the southern terminal. By the end of the day 57 people had been seen by ambulance officers, 47 of whom were transported to hospital. All, but one person with an underlying medical condition were released the same day. It has been reported that symptoms persisted in some people for a number of days (Esplin 2005).

At approximately 7.12 am, the Airport Coordination Centre was notified that a female news agency employee had collapsed at the bottom of the escalators on the mezzanine level of the southern domestic terminal. In accordance with airport procedures, a medical response team was dispatched. The female was subsequently transported to the Northern Hospital.

At approximately 8.48 am, the Airport Coordination Centre was notified about a second female newsagent employee who had collapsed and further at about 9.02 am, an American Express stand employee had collapsed. Airport management cordoned off the immediate area on the mezzanine level and commenced air testing for breathability, receiving normal readings. The air conditioning for this area was in full fresh air mode. Test results were unremarkable, although the test was later considered incapable of detecting any chemical or biological contaminants.

After testing, the southern terminal's air-conditioning system was switched to outside spill mode (air is expelled from the building to the outside), possibly removing any harmful agents that may have been in the facility.

The number of the patients was, however, growing and The ARFF Senior Fire Commander responded to the incident and while en-route advised Air Traffic Control of the situation and that the closure of the terminal may be required. He arrived at the scene at approximately 9.34 am and was briefed by his staff. At about 9.45 am, the ARFF Commander and the Ambulance Services Commander conferred about the exact numbers of casualties. The Ambulance Commander recommended evacuating the terminal. The recommendation was made on the basis of multiple casualties over a short period of time, that it occurred in an enclosed area and that there were common symptoms. After a while The ARFF Commander decided to close and evacuate the terminal. This effectively stopped all aircraft traffic from docking at the southern terminal aircraft stands.

The Melbourne Airport Emergency Plan was put into effect. Safety and security activities around the terminal were implemented, including handling arrangements for passengers in aircraft that had already landed.

The Incident Controller and Department of Human Services (DHS) staff met to consider the situation. It was determined that the event was more likely a hazardous materials incident than a biological issue and control should remain with ARFF. DHS requested advice concerning the type and level of detection equipment being used. Following confirmation that testing was for air quality and flammability, not for toxic chemicals, DHS suggested to undertake analysis using more sophisticated and comprehensive testing equipment.

From 1.00 pm through to 6.00 pm, hourly briefings with agencies were held by the Incident Controller. At each of the earlier briefings, the participants, including Melbourne Airport and Virgin Blue were advised that the testing would take some time, but no minimum or maximum time was given.

As no substances in the atmosphere of the southern terminal were discovered, the
Incident Controller decided to return the air handling system to its normal cycle. The final test produced normal results. A briefing was held with all agencies and a reoccupation strategy for the terminal was prepared. At approximately 6.20 pm the scene was formally handed back to Melbourne Airport management and the incident was officially closed. DHS believes that the cause is unlikely to be determined.

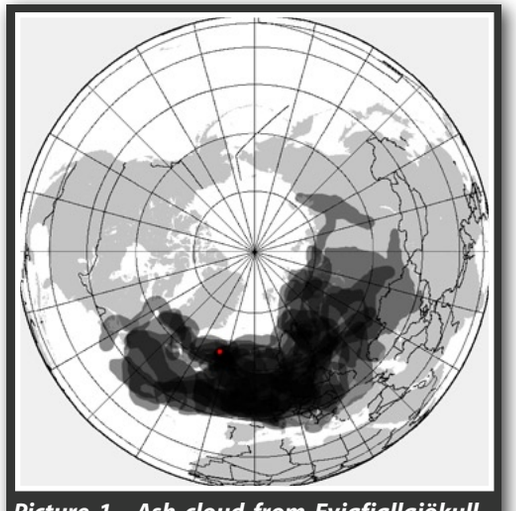
The incident disrupted a third of the domestic passenger flights over 2 days and cost a commercial airline company an estimated three million dollars. Emergency Services Commissioner was tasked to "investigate and analyse any matters pertinent to a comprehensive understanding of the incident".

The review identified coordination shortcomings involving a range of agency processes during the incident. While these did not materially affect the outcome in terms of public safety they highlighted the importance of early detection of the nature of the emergency as well as the need for multi-agency notification at the earliest possible time. This is to ensure delivery of a comprehensive emergency response to an incident with the correct mix of specialist resources.

Formal and informal notification processes during the early stages of the incident did not work as expected, delaying the attendance of personnel whose collective expertise would have contributed to crucial early decision making.
Coordination of the media and communication of information to the general and travelling public was poorly managed.
While the emergency management procedures where appropriate the shortcomings that were identified arose in many instances from a lack of knowledge concerning the arrangements or the capability of the other agencies involved.

The recommendations stressed common plans to ensure the capabilities of agencies are adequately documented and understood by all stakeholders, formal and informal notification processes to ensure early access to specialist advice and support and the need to develop risk based tactical plans that, where safe and appropriate, allow the staged or progressive closure or re-opening of terminal space to support continuity of airport operations during emergencies.

Another interesting incident concerning early warning and notification within the aviation was the eruption the Eyjafjallajökull volcano in Iceland, which began by increased seismic activity that started at the end of 2009 and gradually increased in intensity until on 20 March 2010, a small eruption started that was rated as a 1 on the Volcanic Explosivity Index. Beginning on 14 April 2010, the eruption entered a second phase and created an ash cloud and brought chaos to international air travel by spreading the volcanic ash over northern Europe.



Picture 1. Ash cloud from Eyjafjallajökull volcano spreading over Europe

Most of Europe has little experience in dealing with ash clouds, but the warning and response procedures have been part of international protocols that evolved following the encounter in 1982 between a British Airways Boeing 747 and an ash cloud from Mount Galunggung in Indonesia. After that ICAO, along with the World Metrological Organisation (WMO), established the International Airways Volcano Watch (IAVW), which is responsible for dealing with volcano ash warnings from scientists. They have divided

the world's airspace into nine Volcanic Ash Advisory Centres (VAAC). (ICAO 2004)

The VAAC is part of the host country's meteorological authority. In the Iceland case, London is the VAAC in charge, and the VAAC is part of the UK Met Office. These centres are responsible for coordinating and disseminating information on volcanic ash to the aviation sector.

The monitoring and warning system of the volcanic ash is very effective and worked well during the second phase of the eruption. It is, however, worth noting that after the initial eruption the indications of possible bigger problems were not detected or at least not disseminated to all stakeholders. Also the overall understanding of the situation at hand during the early hours of the second phase was vague. For instance the aviation authority of Finland (Finavia) gave the first public notification on 15th April 2010 at 9.30 by stating that the volcanic ash has had no effect on flights in Finland. The next bulletin at 11.00 stated that due to diminished visibility in northern Finland some traffic regulations will be imposed. Finavia gave several bulletins during the day gradually closing the airspace of Finland and finally at 22.15 stated that the full Finnish airspace will be closed due to volcanic ash cloud (Finavia 2010).

It is interesting to see how the situation came as a surprise to most of the stakeholders responsible for the air travel and thus stranded unnecessarily a large number of passengers far away from home.

Although some incidents and emergencies may seem to happen suddenly there are always some signals or indicators about coming events. The indicators may be vague or the lead time before the impact may be very short. In this study we look more closely to early detection, early warning and early notification of threats and emergencies within aviation. The core questions here are:

How can we detect the signals that contain significant and relevant information of impending threat or emergency?

How can information be analysed and shared in as early a stage as possible, so that there will be as much time as possible for responses necessitated by the threat?

2. Scope of Study

The scope of this study is to look at the early indications of an impending emergency or threat within the aviation environment. These threats may be caused by natural phenomena such as storms or volcanic eruptions or by man-made unintentional or intentional actions. The main emphasis is on intentional criminal or terror related intention to carry out a CBRN attack.

The study uses a main scenario of an international passenger flight with a CBRN threat. The time line of the flight is divided in separate phases; 1. Before the flight, 2. Airport activities, 3. During the flight, 4. Landing and disembarkation, 5. After the flight.

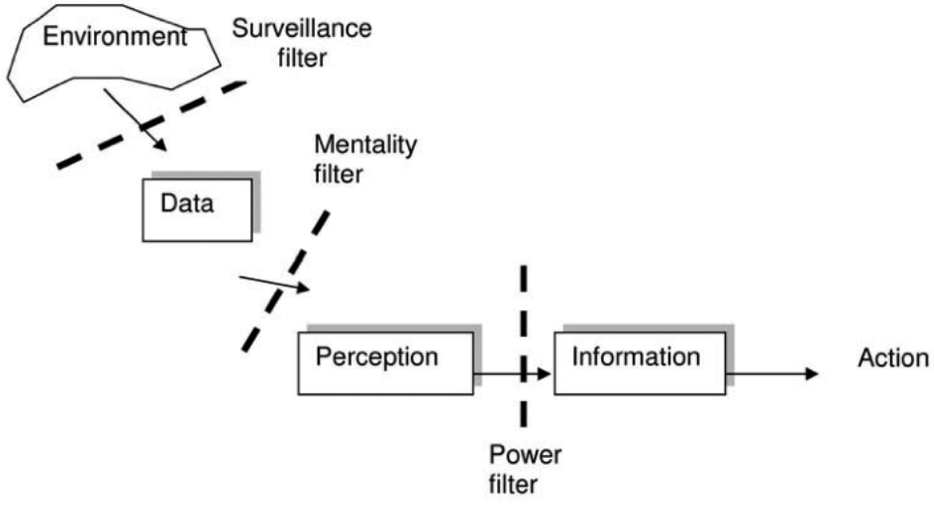
The different aspects of containing the threat by detection of weak signals and using early warning methods is studied.

In these phases we study different sources of information, different stakeholders and the

challenges and possibilities to detect the early indications and what is needed in sharing the information between the key stakeholders in order to launch a timely and effective response for various types of emergencies.

The following picture was first introduced by Igor Ansoff, who presented his theory of weak signals in business economics in the 1970s (Ansoff 1984). It can be used as a feasible frame of reference also for emergency response information management. In complex multi-agency emergencies e.g. the surveillance is done in every organisation and hence there should be added information sharing function in order to use full potential of the expertise that exists within all the organisations. Also the link from Information to Action is too straightforward giving the impression that with information the action is automatic. In a complex emergency the information (including early warning/early notification) may vary depending on the type of the emergency, the lead time before impact or action as well as the actors and their resources and response capacity.

Information has to pass three different filters to have an impact on threat analysis. These filters can either hamper or facilitate the reception and processing of the information. First a surveillance filter defines the area we are observing. However, the challenge here is that we usually build the surveillance filter based on our past experience and the anomalies often come from outside our own discipline. That is why the information sharing is needed. Then a mentality filter is used for evaluating novel issues that have passed the surveillance filter. At this point the receiver of information evaluates the arrived information and decides what to accept and what to discard because it is unrealistic, unnecessary, of little use, or otherwise irrelevant. Finally, a power filter is applied when the cognitive filter is triggered by threat analysis rules. This filter is used especially by the decision makers.



Picture 2. Information filtering (Ansoff 1984)

3. Weak Signals

The term weak signal was introduced by Igor Ansoff, in the 1970s (Ansoff 1975). His idea was to seek an improvement to the strategic planning method, as this method didn't work satisfactorily when sudden changes or unanticipated discontinuities in development occurred in the business environment; the environment showed turbulence. Ansoff also used the term "strategic surprise" to describe these discontinuities.

According to Ansoff strategic surprises give advance information of themselves. There are signals or symptoms of surprises to come. This information is initially inexact: the signals are vague, fuzzy, and difficult to interpret, but gradually they become more distinct and easier to decipher. Even on the basis of the initially inexact information some action can be taken. Ansoff claims that weak signals may mature over time and become strong signals. He also defines five different stages of signals: 1) the sense of a threat is felt; 2) the source of the threat is known; 3) the shape of the threat becomes concrete; 4) the response strategies are understood; and 5) the outcome of the response is predictable.

Today, there is a growing amount of literature analysing weak signals. Although the initial work done by Ansoff and other early researchers focused in business economics, many other disciplines have also become interested in weak signals; these include future research, communications research, research on international security, international politics and military science.

Traditionally the weak signals are associated with gradual development over time. Ansoff claims that weak signals may mature over time and become strong signals, which are "sufficiently visible" and "concrete".

Another term that is used in describing sudden events is *Wild Card*, which is sometimes used as a synonym of weak signals (Hiltunen 2006). Wild card is a surprising, startling event that has important consequences. In future studies wild cards are defined as developments which are possible, and which, if they occur, will change everything.

In aviation context the World Trade Center 911 attack was a clear example of above defined wild card. There were, however, a number of weak (some claim even strong) signals preceding the actual deed.

In this article we define a weak signal as any early indicators or a soft form of information about coming events. A weak signal might be visible well in advance or just before the impact. So the time frame may vary from months or even years to a few minutes or seconds. The significant feature is that it exists but cannot be detected or comprehended without special attention. The selection of indicators is very important, because monitoring will center on them. The wrong indicators can lead to wasted time, effort, and resources.

One relevant issue in the threat scenery of today's aviation is also that the extremists will feed signals in purpose to have desired effects and harm the business. A number of flights have been cancelled during the past few years due to intercepted messages interpreted as indicating a potential threat to flight security. Are all these threats real or done on purpose for

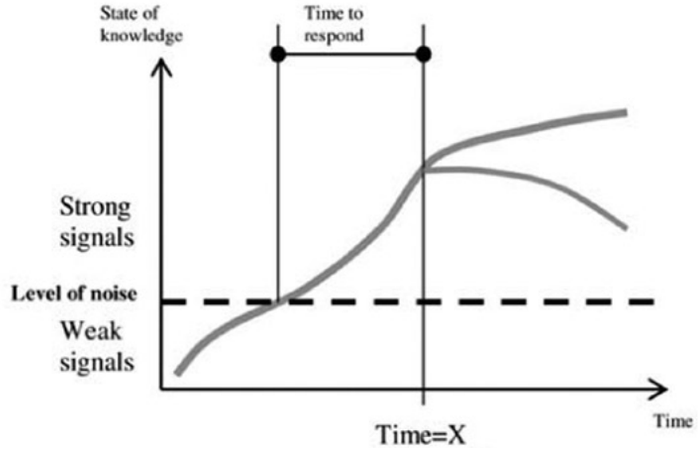
disturbance, remains unknown. It has been claimed that scaremongering is rife where CBRN materials are concerned, and can cause more damage than effects of the substances themselves. Terrorists, of course, are fully aware of this phenomenon (Marcus 2005).

Weak signals are not problematic because their influence is unpredictable, but rather because they are difficult to distinguish from the mass of other related and unrelated information. The main problem with weak signals is that they are easily missed because they are uncertain and irrational (Harris&Zeisler 2002). We have to decide whether the picked up signals represent a message, a change in the prevailing situation, or whether they represent merely arbitrary changes or scattered information.

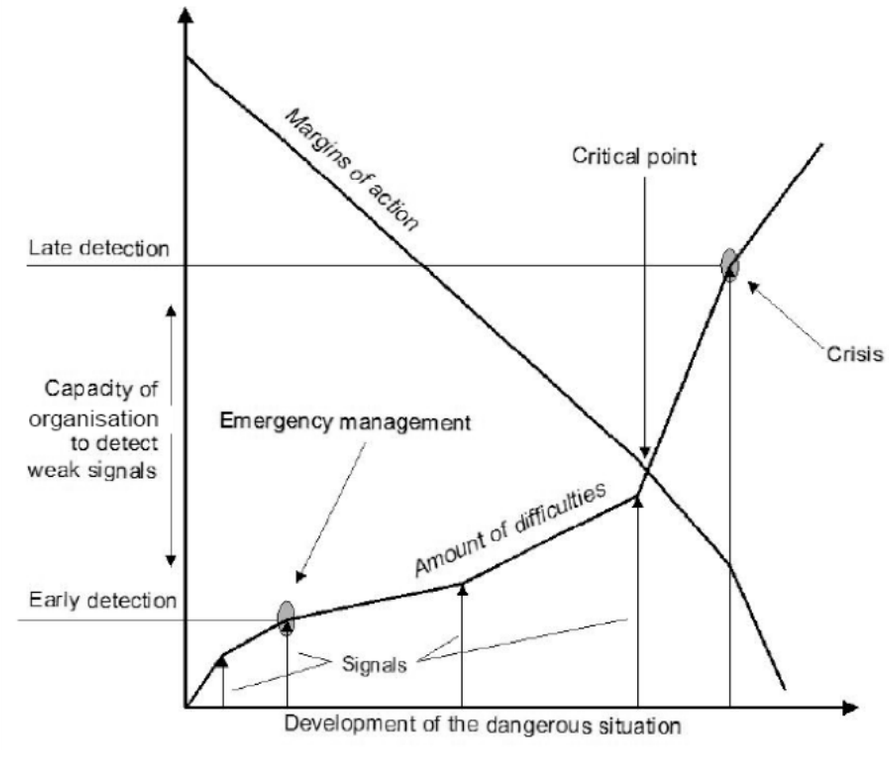
In the following picture the level of noise refers to the level, above which the event is visible to the sizeable group of actors. Above the level, one can notice strong signals. Below the level of noise, only weak signals of the threat exist. If nobody notices the weak signals the time to react is the time from when anybody can understand that an event is indeed happening (i.e. the level of noise exceeded) to the time when it actually takes place. And apparently if we are able to drop the level of noise we are able to detect the signal earlier and will have more time to respond.

The weak signals are important not only before the impact. In some cases e.g. during the one at Melbourne Airport it might be clear that an impact has occurred and we are in an emergency. The nature of the emergency might be, however, obscured and then the situational picture will be gradually formed by adding together weak signals from various sources. After the decision makers have comprehension of the emergency at hand they are able to decide on appropriate response measures.

Also during the actual response work the concept of weak signals is meaningful. During



Picture 3. Response time is dependent on the detection (Adapted from Hiltunen 2006)



Picture 4. Weak signals during an emergency

emergency situations, some signals and events announce changes in the situation that may create unexpected difficulties if they are not detected, analysed and processed in due time. By generating surprise, uncertainty and confusion among actors, the late detection of such weak signals is a key factor to turn emergency situations into crises (Wybo & Latiers 2006). The following picture describes this situation.

4. Early Warning

There is not a clear definition for Early Warning. In some circumstances it is used more or less as a synonym for weak signals especially in the field of emergency management for slow onset disasters.

In 1997, the UN's Guiding Principles for Effective Early Warning stated that the objective of early warning "is to empower individuals and communities, threatened by natural or similar hazards, to act in sufficient time and in an appropriate manner so as to reduce the possibility of personal injury, loss of life, and damage to property or nearby and fragile environments" (UN 1997).

In this study Early Warning means the actions carried out after there is comprehension that an emergency is impending or has happened. This comprehension may come through analysing strong or weak signals.

How early is early? This relates to the timing of the warning. Christer Pursiainen has studied weak signals in the Civil protection and notes that there is no factual difference between the concepts of early warning or mere warning in the sense that an early warning signal can precede, or sometimes immediately follow, the actual event, thus helping to prevent it or mitigate the emergency (Pursiainen 2008). In this study an Early Warning is a message delivered so that it will give some extra time to prevent the emergency or plan and launch the response efforts.

Philip Hall states that the international community has lost sight of the fact that early warning is the integration and extension of existing emergency management capabilities, and therefore, efforts to establish any local, national, regional and international early warning capability must be led by emergency managers, not by scientists and technologists. He further notes that we would be better able to envision and discuss early warning strategically if it were considered as a capability rather than as a system. (Hall 2007)

Although differing views exist on how extensive an early warning process should be, in this study we look at a process that does not simply disseminate the warning information. In order to be useful the process will have the responsibility to issue the warning to all stakeholders, and assure that the warning is well communicated to the target organisations and understood by them and that there are appropriate responses to various levels of warning. If we look only at disseminating the message the approach will easily be technology driven with elaborate modern devices and fast connections and the message is promptly delivered but what it means and what actions it calls for is not necessarily understood by the recipient. Also the sender will not always know when and what type of response will be initiated.

A good example of the extent of efforts and time available caused by a new type of threat are the activities during the incident when authorities got information that gave reason to believe that terrorists had planned to detonate gel-based explosives on U.S.-bound flights from London in August 2006. Airports in the United States and the United Kingdom were put on red alert — meaning a potential attack could be imminent — and liquids were banned from carry-on luggage. In order to make this happen there was a need to change literally thousands of people's behaviour in the course of about 12 hours. They had to be trained. Everybody had to understand what the new rules were going to be. And the authorities had to communicate to the public in a very short period of time (ABC 2007).

There are a number of considerations and challenges within the Early Warning in Aviation emergencies. Especially dealing with CBRN threats brings together organisations that have not much common experience. Therefore it is not always clear, who has the authority and responsibility to issue warnings. When and who should be warned, since false alarms mean loss of credibility? Also different stakeholders may rely on different early warning methods and systems.

5. Passenger Flight's Time Line

The following deliberation is not meant to be an exhaustive report of all the possible aspects during a CBRN threat against a passenger flight but rather tries to demonstrate the multitude of issues which may have an effect on the security environment as well as some of the challenges and possibilities in dealing with them.

The globalized aviation system, which includes countries with different capabilities and approach to security, is vulnerable and plagued with substandard security, corruption, bribery, and weak governance. Additionally, the Internet provides worldwide access to all types of information that could be useful to extremists, including flight schedules, specific details and diagrams of both aircraft and airports and reports of successful terrorist tactics and countermeasures developed by governments (Forest 2007).

1. Before the Flight

The monitoring of the security environment is an ongoing process and will usually notice general threat often with no direct link to any specific flight or airline. The intelligence community and law enforcement officials will have the lead role in this and employ methods such as data mining with Bayesian networks, internet monitoring as well as more classified intelligence methods.

An example is the case when officials discovered an Arabic-language video clip on the Internet in October 2007 illustrating how to convert a remote-control toy car into a detonator for a bomb, the US transportation Security Administration officers stepped up their scrutiny of passengers carrying remote-control toys aboard airplanes (Forest 2007).

According to Raphael Ron, who served as director of security at Ben Gurion for five years, aviation security has to develop comprehensive layered security programs that protect airports in their entirety, from perimeter access roads to passenger checkpoints. Second, airport security have to come to terms with what Ron calls the human factor — the inescapable fact that terrorist attacks are carried out by people who can be found and stopped by an effective security methodology including behaviour pattern recognition (Fickes 2003).

A clear case of neglected weak signals and/or early warning was demonstrated in the case of Northwest Airlines flight 253 from Schipol Airport Amsterdam to Detroit Metropolitan Wayne County Airport on 25th December 2009. On board the flight one individual tried to detonate an improvised plastic explosive concealed in his underwear. The attack failed and later it was revealed that some U.S. intelligence agencies had advance information about the individual but failed to share this information with other actors involved (MacAskill &Stratton 2010).

2. Airport Activities

Airports are busy places with various occupational groups and traveller categories.

To prepare a commercial aircraft for flight requires attendance from separate organisations. These actions include checking in the passenger and the luggage, catering services, cargo services, refuelling services, other activities including cleaning. Although all the personnel in-

volved in these activities are every time screened for security purposes there are not effective methods to screen the items delivered to plane for a possible CBRN threat. There is much more research needed for good universal detectors. Detection is difficult and whereas the military does have a lot of good equipment, this is not yet available in the civilian sector and also the CBRN training is still scarce (Marcus 2005).

3. During the Flight

The flight is a confined space so after the lift off no outside intervention (except communication) is possible for emergencies. It is important that the crew is able to record their observation during an incident in a consistent manner and that there is a link to outside experts in case of a CBRN emergency or threat. Most of the major commercial airlines have well established systems for assistance in case of medical emergencies during flights (Boureel&Turner 2010) but no similar systems for CBRN threats exist.

The CBRN threat during a flight may come through food, and beverages, cabin air or contamination through skin or external radiation. The symptoms for all different contagions are similar to food poisoning including nausea, vomiting, muscle pain and weakness, headache, dizziness, and rapid heartbeat etc. This makes it difficult to determine what is the cause and careful going through of the weak signals and other information is important.

The ventilation system plays a key role in reducing the airborne spread of pathogens within an aircraft. The cabin air supply system pulls air in from the compressor stages in the aircraft's jet engines. This pressurized air is cooled and may be mixed with an almost equal amount of highly filtered air from the passenger cabin. The mixture is then blown into the cabin through overhead supply outlets. In the cabin, air typically flows in a circular pattern and exits through floor grilles. About half of the air exiting the cabin is immediately exhausted from the airplane and half filtered and remixed. The filtered air, called re-circulated air, normally passes through a High-Efficiency Particulate Air (HEPA) filter, before it is mixed with the air from the compressors. This filter is a place to install the possible detectors if we want to have early detection of pathogens. Also after a possible incident it is important to inspect and analyse the filters without delay.

4. Landing and Disembarkation

Usually there are no security checks for incoming passengers. Some airports are, especially during pandemic threats, using automatic infrared body-temperature measurement systems that can rapidly detect body-temperature at crowed public places.

Here again the main stakeholders will be law enforcement and intelligence officials detecting possible threats.

5. After the Flight

Incubation period is the time elapsed between exposure to a pathogenic organism, a chemical or radiation, and when symptoms and signs are first apparent. This period may be as short as minutes to as long as years. So a possible contamination of the passengers may not be

noticed at least for days after the flight has landed and the passengers dispersed to their final destinations. The poisoning of Alexander Litvinenko with Polonium 210, and his subsequent travel on British Airways aircraft, demonstrated how infected passengers, be they intentionally contaminated or just naturally ill, could impact on the health of those taking to the skies with them.

Here again the weak signals will be formed as a combination. Some passenger may have an illness with peculiar symptoms. If the history of the patient is checked carefully there might be found another similar case and determined that the case is not mere illness but something more severe. So the overall awareness of the possibility of a CBRN threat among all the stakeholders will contribute to the rapid detection of an incident.

6. Conclusions

Using weak signals to detect threats in aviation business, demands action and skills from various stakeholders. Signals detected within one actor may not have any significance but with diligent combining with information from other sources may reveal an imminent threat.

Every effort must be made to increase coordination and improve surveillance and detection techniques in addition to developing improved response mechanisms. In many instances the lack of knowledge concerning arrangements or the capability of the other actors involved will have a detrimental effect in the timeliness or efficiency of the joint response in an emergency. Today no agency works in a void and has to understand its own as well as other actors' roles and responsibilities in an emergency in order to rapidly identify and contain CBRN emergencies all while retaining order rather than causing panic.

Today many of the threats in aviation will affect the global aviation as a whole. The preventive measures taken to block the attacks, mean more restrictions in travelling. One objective in dealing with weak signals and early warning is to develop systems and methods by which we would be able to better detect the threats and their time frame and the specific targets in order to support the business continuity without compromising the security.

One of the challenges is the diversity of information users: Information may need to be shared across diverse, loosely coupled, emergent multi-organizational networks in which different entities play different roles in response activities, have different needs and urgencies, have different cultures, and may have vastly different capabilities with respect to technology utilization. These organizations may or may not have policies in place regarding data sharing and collaboration. Furthermore, these organizational networks must rapidly reconfigure to adapt to the changing communication and control demands present during emergencies. Finally, different people/organizations have different needs and urgency levels regarding the same information (Mehrotra & al. 2004).

References

- ✓ ABC 2007. "Plot Would Have Killed Thousands: Homeland Security Secretary Michael Chertoff Offers Chilling Details about 2006 Airplane Plot and Current Terror Threats," ABC News, 6 August 2007.
- ✓ Ansoff, I. 1975. Managing Strategic Surprise by Response to Weak Signals. *California Management Review*, Vol. XVII, No 2, 1975
- ✓ Ansoff, I.1984. Implanting Strategic Management, Prentice Hall International, New Jersey 1984
- ✓ Bourell, L., Turner, M. 2010. Management of in-flight medical emergencies. Oral Maxillofac Surg. 2010 Jun;68(6):1377-83. Epub 2010 Mar 29.
- ✓ Esplin B. 2005 A report of the response to an emergency at Melbourne Airport on 21 February 2005. Melbourne, Vic: Emergency Services Commissioner, 2005
- ✓ Finavia 2010. Finavia rajoittaa vulkaanisen tuhkan vuoksi lentoliikennettä kaikilla lentoasemillaan. http://www.finavia.fi/medialle/tiedotearkisto/finavia_tiedotteet/finavia_tiedote?id=2544106
- ✓ Forest J. 2007. The Modern Terrorist Threat to Aviation Security.
- ✓ Hall, P. Early Warning Systems: reframing the discussion. The Australian Journal of Emergency Management, Vol. 22 No. 2, May 2007
- ✓ Harris, S., Zeisler, S 2002. Weak Signals: Detecting the Next Big Thing. *Futurist 36(6)*, 21-28. 2002
- ✓ Hiltunen, E. 2006. Was It a Wild Card or Just Our Blindness to Gradual Change? *Journal of Futures Studies*, November 2006, 11(2): 61 – 74
- ✓ ICAO 2004. Handbook on the International Airways Volcano Watch (IAVW), Doc_9766-AN/968, Second edition, 2004
- ✓ Ilmola, L., Kotsalo-Mustonen, A. 2003. Filters in the Strategy Formulation Process in *Journal of Universal Computer Science, vol. 9, no.6 2003*..
- ✓ MacAskill, E., Stratton, A. 2010 UsS Intelligence on plane bomb suspect was 'vague but available' Security review blames human and systemic errors for failure. *The Guardian* 1. January 2010.
- ✓ Marcus, R. 2005. CBRN: technologies to detect chemical, biological, radiological and nuclear weapons. Aviation Security International, April 2005.
- ✓ Mehrotra, S., Butts, C.,Kalashnikov, D., Venkatasubramanian, N. Rao, R. Chockalingam, G.,

Eguchi, R. , Adams, B., C. Huyck, C. 2004. "Project RESCUE: Challenges in Responding to the Unexpected.", IS&T/SPIE 16th Annual Symposium on Electronic Imaging, Displays, & Medical Imaging, volume 5304, 2004.

✓ Pursiainen, C. 2008. Early Warning and Civil Protection: a Framework for Analysis and Action in *Early Warning and Civil Protection, When does it work and why does it fail?* NORDREGIO REPORT 2008:1 Stockholm

✓ UN, 1997. Guiding Principles of Effective Early Warning, IDNDR Early Warning Programme, August 1997, Geneva, Switzerland

✓ Wybo, J-L., Latiers, M. 2006. Exploring complex emergency situations' dynamic: theoretical, epistemological and methodological proposals. *Int. J. Emergency Management*, Vol. 3, No. 1, 2006

✓ Glantz, M. (ed.) 2003. Early Warning Systems: Do's and Don'ts, Report of Workshop 20–23 October 2003 Shanghai, China

The Government Situation Centre during the Tabletop Exercise arranged in the framework of Project Aether.

Pekka Visuri & Timo Hellenberg: Finnish Crisis Management - A Case Securing Of Air Passenger Transports against CBRN Terrorism

Introduction

The Finnish crisis management system has been developed after the Cold War from the preparedness to overcome extreme situations, a total war included, towards a more peace-time oriented crisis management which is based on the comprehensive security concept.

In this article the emphasis is laid, firstly, on the description of the decision-making system according to the government resolution 2006 *The Strategy for Securing the Functions Vital to Society* and the improved system in the new resolution 16 December 2010 on the *Strategy for Securing the Society*[1]. The main principle is to have all authorities prepared to manage crises with their everyday organisations and flexibly enhanced administrative powers up to the situation.[2]

The present crisis management system is generally appreciated as adequate and has functioned rather well in exercises. The emergency legislation is under scrutiny but there has been no urgent need to make major corrections because of the unfinished review of the constitution concerning the political competence sharing in the crisis management leadership. Finland is still prepared to cope with extreme crisis situations, too, with the national defence system which is organized according to the "comprehensive approach" and frequently exercised.

An overall *definition* covering various crises and other emergency situations can be expressed as follows: *Crisis* is an unexpected situation where important national or societal values and assets are at stake either domestically or internationally, with time pressure and uncertainty prevailing. The national crisis management system must be prepared to handle a large variety of emergency situations from natural and man-made disasters to terrorist attacks and armed conflicts.

An *emergency situation* can be managed with usual measures without special crisis management arrangements, but the same system of alarm and decision making should be used as a basis for preparedness concerning all kinds of crisis and other emergency situations following the "all hazards" principle.

1) Government resolution 16.12.2010 *Yhteiskunnan turvallisuusstrategia* (Engl. Security Strategy for Society), an updated version of the strategy in resolution 2006, has been published during the redaction work of this report and not yet implemented for practical use. Therefore, this article refers to both resolutions 2006 and 2010 which have rather common basis for crisis management systems but differences in detailed administrative stipulations.

2) This article is partly a continuation and specification of the article "Finnish crisis decision making, cooperation of authorities and crisis communications – especially in terrorism related crises", in *Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon*, Aleksanteri Papers 1:2009.

It can be difficult to define exactly an emergency situation or the nature of a crisis at the first stage after an alarm. Still, it is essential to start response and counter measures without hesitation if there are signs which hint to further escalation or crisis potential. Therefore, the estimation of the risks on the basis of an adequate *situational awareness* is one of the most important duties in the *crisis management* (CM). That includes actions

- Before: research, training and planning.
- During: decision making, planning, leadership, cooperation, information.
- After: evaluation, learning, encouraging.

National CM arrangements should be available and promote the interests of citizens, territory, and property. In this definition, the latest trend has been to add the national and economic interests abroad to the CM portfolio to be protected. It is difficult to define a mass or time scale in which an emergency situation becomes a crisis because the threat perceptions are very much context related.

There have been problems in managing surprising emergencies or minor crisis situations, especially so called normal-time disturbances which can emerge rapidly, have many surprise elements and need inter-sector measures. This kind of situation was also the Tsunami disaster in December 2004. It occurred in a very distant country but affected many Finnish citizens and required urgent rescue and evacuation measures.

The lessons-learned from the Tsunami catastrophe 2004 have been taken in account in the preparedness arrangements of the Government, Foreign Ministry and rescue services. However, some administrative and operational culture problems still exist in that kind of crisis situations. For example, it is not so easy to get good information from large and severe disasters, especially if they occur in foreign countries. Also the responsible authority may be difficult to be defined in such circumstances. Moreover, responsibilities and cost sharing between public and private sector in conducting rescue missions is still too unclear.

The great variety of crisis types and the need to make decisions swiftly also in "civil crises" have made it necessary to construct an effective system for maintaining situational awareness. A situation centre has been built for the permanent use of the government, and it is located at the Prime Minister´s Office at the Government Council. There are still the usual military, police and border guard command and control systems as well as air and maritime surveillance arrangements for operational tasks.

The principle of independency of administration sectors concerning crisis management in Finland is well functioning in the contingency planning and in responding to such emergency situations which can be clearly defined and managed by one sector of the state administration. Difficulties may emerge especially with crises which have inter-sector effects and must be handled without delay. The most problematic case would be a terrorist attack against some vital functions of society or critical infrastructures in Finland or in vicinity. The risk is rather low because of a small probability, but the consequences would be very fatal. Therefore, this kind of case must be taken into account seriously and the counter-measures shall be prepared according to the threats.

This article aims, firstly, to find out needs and possibilities to develop situation awareness and decision making arrangements in Finland. Also the cooperation in the EU framework shall be observed and taken into account. The emphasis has been laid on the prevention and countering terrorism which can affect air transports, though the usefulness of the so called all-hazards principle in crisis management arrangements shall be studied, too.

As final conclusion the article aims at making recommendations for the development of the Finnish crisis management system as part of the EU arrangements on the basis of the conclusions from the theoretical study and exercises in the Project Aether as well as from other relevant research activities.

1. From the Cold War to New Threat Scenarios: Development of the Finnish Crisis Management System

✓ *1.1 Background*

The experience taken from the Second World War and Cold War has strongly affected the development of the Finnish crisis management system. Security and defence policy has been based on the doctrine of "total defence" which includes both military and civil elements.

During the Cold War the total or "comprehensive" defence principle was intended to use the whole national capacity against military threats, as the worst case a massive attack on Finland. The Finnish defence doctrine was rather similar to the doctrines of Sweden, Austria and Switzerland.

The general planning and coordination for the total defence was authorized to the *National Defence Council* established in 1957. The Council was the highest advisory body for the Government and the President of the Republic in preparations for national defence. There was already functioning the *National Board of Economic Defence* (from 1956) which planned and coordinated stockpiling of strategic materials and other economic preparations for emergency situations. The *Civil Defence Act* (1958) ordered the construction of bomb shelters in the cities and regulated the duties of citizens for protection of the people in the crisis situations keeping in mind the massive bombardments during the World War II.

A Finnish specialty has been the courses for national defence which are held for the higher civil servants and military leadership as well as for leading persons of the economic life and journalists. The national defence courses in Helsinki have lasted four weeks, as the provincial courses have been shorter. At present, those courses are still organized in the same way as during the Cold War, and they have been one of the most important means in developing and maintaining the comprehensive defence system and other emergency arrangements. It also hints why the traditional thinking of security matters is still deep rooted in the administration as well as among the people.

The decision making in the crisis situations during the Cold War was regulated with the instructions by the National Defence Council and legal provisions by the Parliament. In the legislation a strict dichotomy was between the normal situation and the state of war. The wartime conditions were well defined and regulated. The problem was that the decision-making

procedures in all kinds of disturbances and crises under the level of a war situation were rather vaguely defined and legislated. The basic idea was: if we have a good preparedness for a total war we can well handle all the less dangerous situations, too, possibly with some improvisation according to the special demands of the actual crisis. In time the need to develop procedures for the "grey zone" between peace and war became urgent, but it was not until the end of the Cold War as the new legislation was completed.

The most likely and urgent emergency or crisis situations during the Cold War were economic by nature. That is why the Parliament passed already in 1970 an economic emergency bill with the complete name *Act on safeguarding the population's subsistence and national economy under emergency conditions*. It was also called "Rationing Powers Act" because the emphasis was laid on the rationing and regulating measures of currencies, prizes, raw materials etc. It could be used in all situations which were endangering the national economy and population's living conditions. In such cases the government had rapid and effective regulation powers for economics, and the decisions had to be submitted for Parliament's approval afterwards.

However, there was a high threshold for using the economic emergency act. During the oil crisis 1973–1974 the Government issued some regulations based on that legislation but they could have been made also according to the normal arrangements by a decree and then to be accepted by the Parliament afterwards. Also the severe economic recession in the early 1990s passed with normal governmental powers, although there were many discussions about the possibilities to use the emergency legislation for regulating the economy.

✓ *1.2 Emergency Situations*

The need to have a general emergency powers act was widely recognized during the 1980s, and a committee drafted some proposals. After a lengthy political and juridical process in 1991 the Parliament passed a quite new **Emergency Powers Act** (1080/1991) simultaneously with the **State of Defence Act** (1083/1991) which replaced the old State of War Act. They specified the conditions which could lead to enhanced authorization of powers in crisis situations, as well as they set respectively frames for the decision making.

The Emergency Powers Act is still valid in spite of some slight amendments in 2000. The Government proposed a new act (HE 3/2008 vp) on the base of a committee work 2005, but the legislation process in the Parliament has been suspended because there were difficulties in defining the role of the President of the Republic in the decision making.

The Emergency Powers Act (1991) aims to secure the livelihood of the population and economy, to maintain legal order as well as constitutional and human rights, and to safeguard the territorial integrity and independence of Finland in emergency conditions. It can be applied before or beside the State of Defence Act which gives additional powers for the Government in the defence against an armed aggression.

The emergency conditions (defined in 1991) are as follows

(1) An armed attack against Finland, as well as war and the aftermath of war.
(2) A serious violation of the territorial integrity of Finland and a threat of war against the country.
(3) War or a threat of war between foreign countries and a serious international crisis implying the threat of war and requiring immediate action for the increase of the defensive readiness of Finland, as well as other specific conditions outside Finland having a comparable effect, if they may pose a grave danger to the foundations of national existence and well-being (amendment 2000).
(4) A serious threat to the livelihood of the population or the foundations of the national economy brought about by hampered or interrupted import of indispensable fuels and other energy, raw materials and goods or by a comparable serious disruption of international trade.
(5) A catastrophe.

Those cases will be defined as emergency conditions if the authorities cannot control the situation with regular powers.

It is remarkable that the emergency conditions mentioned above concern only situations which are linked to an armed conflict in or outside Finland, have serious economic effects or are defined as natural or man-made catastrophes. Terrorist attacks or other terrorist activities, even in a large scale, are not mentioned in the list of emergency conditions. However, it may be possible to interpret a large-scale terrorist attack against Finland (or even just against Finnish citizens and interests) to be a case of a war-like armed aggression, as the terrorist attack against the United States on 11 September 2001 was seen as an aggression defined in the article 5 of the Charter of NATO, the Washington Treaty 1949.

Decision making in the emergency situations

(1) In emergency conditions the Government may be authorised by Presidential Decree to use the emergency powers.
(2) The Decree shall be issued for a fixed period which may not exceed a year at a time.

The Decree shall indicate the emergency powers that the Government is authorised to use and, if they are not to be used throughout Finland, their territorial limits.
(3) The Decree shall be immediately submitted to the Parliament. The Parliament shall decide whether the Decree is to apply as such or whether it is to be repealed in full or in part and whether it is to remain in force for the period provided or for a shorter period.

After the Cold War in 1992 the *National Defence Council* made a new general definition of a crisis situation, in particular in view of provision for emergency planning. New perceived threats (below the level of an emergency situation and war) were named as **normal-time disturbances** that may for example result from the major breakdown of the national data systems. They were due to be handled with normal administrative powers, but it was seen important to take those measures more explicitly into the emergency legislation and planning. The planning directive was smoothly modified in the new issue of 1999, but the basic principles remained intact.

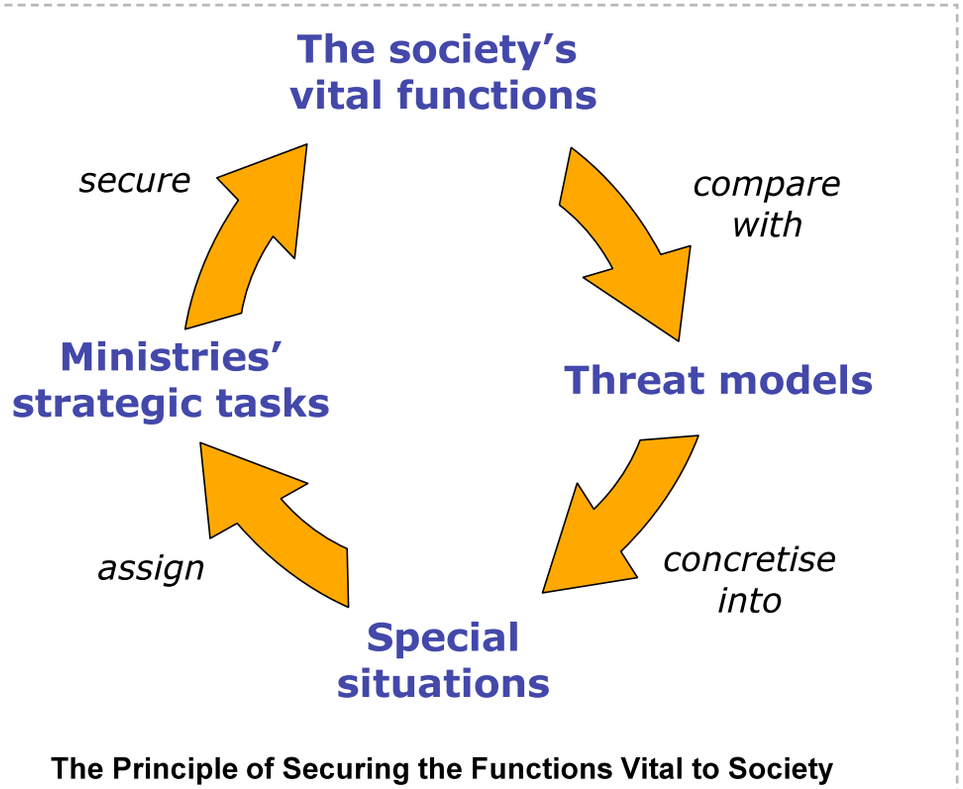
✓ *1.3 The Present Preparedness System*

Increasing national and international interdependency and the simultaneous societal developments required a new assessment of Finland's security more comprehensively in the early years of the 21st century. A new strategy from the viewpoint of functions vital to guarantee the

security of the population and society as well as the freedom of action for the state leadership was created and published in November 2003 under the title *Government Resolution on Securing the Functions Vital to Society*.

The revised strategy and new government resolution in November 2006 aimed especially to conform to the anticipated development in the security environment of Finland in the near future. It also took into account the increasing internationalization as well as changes in the security environment and societal structures. Special attention was paid to the consequences of Finland's membership in the European Union. International interdependency and the activities of the EU and international organizations, such as UN and NATO, had created new forms of cooperation that could also enhance the resiliency of Finnish society in crisis situations.

The Strategy for Securing the Functions Vital to Society (SFVS, Government Resolution 23.11.2006)[3] harmonized the ministries' preparedness activities, adhering to both the division of duties provided in the Government Rules of Procedure and to coordination provisions. Society's vital functions have to be secured in accordance with the arrangements for normal conditions.



The Principle of Securing the Functions Vital to Society

Figure 1: The principle of securing the functions vital to society (2006)

3) In Internet: http://www.defmin.fi/index.phtml?l=en&s=335

Ministries have been obliged to include all of the measures required by the Resolution in their standard operating and financial plans. Each ministry directs its respective administrative sector's preparedness as well as relevant legislative improvements. The activities of the business community and non-governmental organizations (NGOs) were also considered but not exactly articulated or defined, nor have the private entities given a clear role and mandate in the national exercises or planning, despite all the strategies and political declarations.

The strategy (resolution) has been compiled from the viewpoint of societal functions that are vital in all situations. It also describes the threat scenarios that can jeopardize vital functions, including the most important special situations within each scenario. A ministry primarily responsible for preparedness and situation management has been designated to each special situation in accordance with its mandate. Other ministries support the competent ministry. In order to secure society's vital functions, strategic tasks required by the security environment have been assigned to ministries.

The resolution set desired end states for vital functions as well as requirements related to sustaining and developing the ministries' strategic tasks. Furthermore, the resolution assigned the focus areas for development as well as the standards for the organizing of monitoring and preparedness exercises.

Each ministry, within its mandate, directs and monitors the implementation of measures relating to securing vital functions and the required development of capabilities. The *Security and Defence Committee*, cooperating with the meeting of the ministerial heads of preparedness, is responsible for the joint monitoring of the strategy. The monitoring provides for the updating of the strategy as well as for coordinating total defence development measures. It also facilitates the informing of the political leadership on the situation.

The Government ordered the review of the strategy and resolution 2006 (SFVS) so that it has been published in December 2010 as *Strategy for Securing the Society*. There was no need to build a new preparedness and crisis management system but rather to "polish" some descriptions and terminology as well as to rethink the adequacy of threat scenarios to the present and future conditions in Europe.[4]

The general purpose of the security strategy has been, in line with the objectives of the Finnish security and defence policy, to secure the vital functions of society, which means more detailed: to safeguard the country's independence, preserve security in society and maintain the livelihood of the population. What is missing from this list is the idea of protecting Finnish interests abroad, a statement many European countries such as Italy or Sweden have included in their national strategies during recent years.

The strategy sets out the Government's guidelines for ministries. It concretises the report on the Finnish security and defence policy and augments other Government guidelines concerning various sub-topics of security.

The strategy coordinates the administrative sectors' measures required for preparedness and securing vital functions by defining

4) Interview with Aapo Cederberg (Committee for Security and Defence Policy) 6 April 2010.

- Vital functions of the society and their desired end states
- Common threat scenarios and associated special situations, including preparedness obligations
- The ministries' strategic tasks required for securing functions, including development requirements, and
- focus areas, the schedule, monitoring arrangements and exercises.

On the one hand, the strategy aims to avoid duplication of development efforts and, on the other hand, to prevent a situation in which capabilities required for securing the vital functions are not developed. Ministries are to direct the preparedness of their administrative sector and related legislative measures on the basis of the Resolution.

The actors and their responsibilities according to the strategy:

The President of the Republic conducts Finland's foreign policy in cooperation with the *Government* (i.e. more accurately named *State Council*). The Government is responsible for national preparation of decisions to be made in the European Union, and decides on concomitant Finnish measures, unless the decision requires the approval of Parliament. The *Cabinet Committee on Foreign and Security Policy* prepares decisions for the Government meetings if they include important aspects of security and foreign policy.

The Prime Minister directs the activities of the Government and oversees the preparation and consideration of matters that come within the mandate of the Government.

Important matters of foreign and security policy and other matters concerning Finland's relations with other states, associated significant internal security or total national defence issues and the coordination of these measures are handled at the *joint meeting* of the President of the Republic and the Cabinet Committee on Foreign and Security Policy.

The Government directs, supervises and coordinates the securing of functions vital to society. Each *competent ministry* does the same within its respective administrative sector. In order to facilitate preparedness and to instigate activities, all *competent authorities* employ their statutory powers, which are already quite exhaustive in normal conditions.

In emergency conditions the Government may be authorized to use the additional powers provided in the *Emergency Powers Act*. The decision to begin using powers pursuant to the *State of Defence Act* is taken by Presidential Decree, subject to a Parliament decision. Separate provisions are adopted on the powers of the President of the Republic, the Prime Minister, relevant ministers and the Chief of Defence in dealing with military command matters relating to the Defence Forces.

Government decisions are made either at plenary sessions or within the ministry concerned. The ministries cooperate with each other as necessary, under the leadership of the competent ministry.

In addition, ministries direct the state provincial offices and other subordinate sectors of administration within their respective mandates.

The *Prime Minister's Office* assists the Prime Minister in the overall management of the

Government and in coordinating the work of the Government and Parliament. The Office coordinates the preparation and consideration of EU-related matters. Similarly, the Office coordinates the dissemination of Government information and organizes the general conditions and services for the proper functioning of the Government. The Prime Minister's Office is responsible for the Government's collective preparedness for emergency conditions. The Office has also a relatively new element called Situation Centre which seeks and provides situational picture and crisis information about domestic and international crisis situations both for the staff of the Prime Minister´s Office and other agencies within Government Council.

The *Permanent Secretaries* have the task of directing and supervising the activities of their respective ministries. They are responsible for preparing the administrative sector's objectives, monitoring their implementation and ensuring the preparedness and security of the sector. The *Meeting of Permanent Secretaries* and the *Meeting of Heads of Preparedness* are permanent cooperation bodies. The Meeting of Permanent Secretaries and the supporting Meeting of Heads of Preparedness coordinate the administrative sectors' crisis management activities and assist the Prime Minister's Office with regard to the Government's common preparedness for emergency conditions. When the matters being dealt with so requires, the Secretary General of the President of the Republic participates in the meeting of the permanent secretaries. *The Meeting of Preparedness Secretaries* assists the ministerial heads of preparedness.

Government crisis management activities are described in more detail later on.

The Ministry of Defence is responsible for coordination of the comprehensive defence activities. *The Security and Defence Committee* assists the Ministry of Defence and the Cabinet Committee on Foreign and Security Policy on matters relating to national defence and its coordination. The Security and Defence Committee monitors changes in the security and defence policy situation and evaluates their effects on comprehensive defence arrangements. It is also tasked to coordinate the national defence measures which consist of both military and civil activities.

Appropriate ministries direct the various fields of activity for which *regional administrations* are responsible. *Municipalities* play a key role in preparedness, as it is their specific duty to organize basic services and to safeguard society's vital functions under normal conditions. The municipal managers, together with the municipal boards, direct preparedness in accordance to the law.

The National Emergency Supply Agency (NESA) has duties on security of supply. It is responsible for all planning and operative activities for the purpose of maintaining and developing the country's security of supply. The objective is to safeguard economic activities necessary to the population's livelihood, the national economy and national defence during emergency situations and serious disturbances to normal life. Today the core activity is to secure the functioning of technical systems, especially the critical information and communication systems.

Threat scenarios and emergency situations

The Government has prepared and trained for multiple potential threat scenarios over the years. A "threat" here means a general description of disturbances in the security environment which, should they materialize, could jeopardize the security of society, the livelihood of

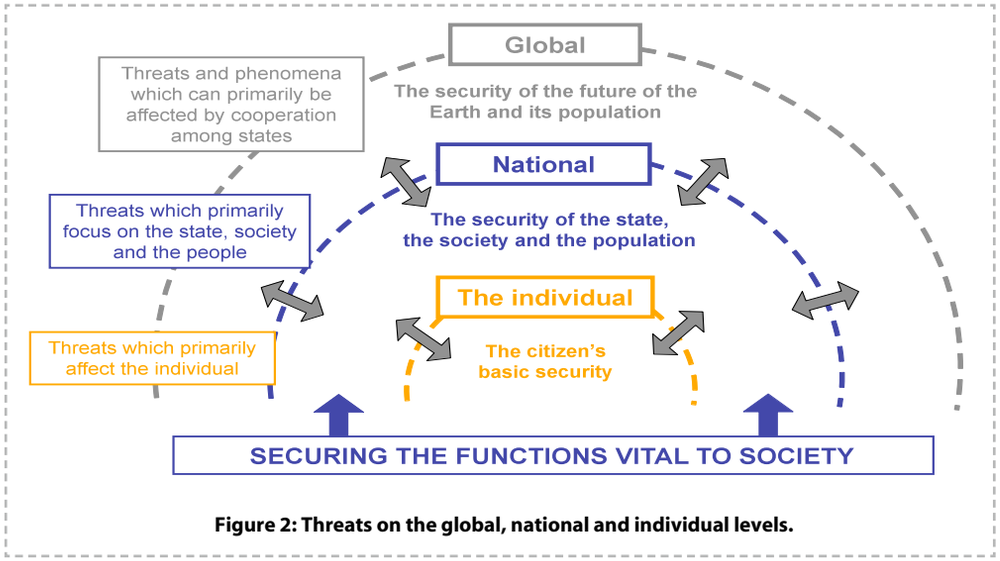


Figure 2: Threats on the global, national and individual levels.

the population or the sovereignty of the state. These kinds of situations fall between the threats against the individuals and the global threats. Because of existing interdependency between the threat levels, no clear boundary lines can be defined.

Threat scenarios have not been profoundly altered since the previous resolutions (2003 and 2006). However, some details and headings have been amended to better respond to the current security environment. The threat scenarios (threat models) included in the *Strategy for Securing the Society* (2010) are:

- Severe disturbances in the electricity grid
- Severe disturbances in information networks – cyber threats
- Severe disturbances in transport systems and logistics
- Severe disturbances affecting the societal infrastructure technology
- Severe disturbances in food services
- Severe disturbances in banking systems
- Disturbances in public finances
- Severe disturbances affecting health and welfare of the population
- Major accidents, natural disasters and environmental threats
- Terrorism as well as organized and other serious crime
- Threats against the security duties of border guards
- Political, economic and military pressure
- Use of military force against Finland.

Threats against society's vital functions may arise individually or several may emerge simultaneously. The origins, exact targets and objectives of such threats are difficult to predict and they might emerge as asymmetric threats with multiple directions. It is equally hard to anticipate their scope, and whether or not their consequences might transfer from one of the levels mentioned above to another. Threat probability estimates also vary and can rapidly change. Even extensive preparedness is not enough to anticipate or prevent all threats. Ultimately, an assessment system capable of predicting and monitoring them is required. This system must be able to analyse security trends, compile scenarios and detect even weak signals concerning changes in the security environment.

In the *European Union* threats may involve member states in different ways and also affect Finnish society. Preparedness system must observe the factors which pose a danger to the population and society even in normal conditions. The relative importance of threats varies from country to country. Terrorism is the most serious threat cited in the *European Security Strategy* as well as in the largest European countries. In Finland terrorism is not regarded as potential threat per se but more likely a possible asymmetric threat against targets of other nations, possessing property, businesses etc. in the Finnish territory.

The description of the threat scenarios in the strategy is comprehensive and adequate serving as a good basis for detailed planning. The invented threats are not equal by risk potential, and they are very different by nature. Therefore, the threats must be categorized especially for the planning of countermeasures.

One of the most important dividing lines of threats goes between natural and man-made disasters, on one hand, and active hostilities against the state and society, on the other. In the latter case the crisis situation includes more uncertainties and protracted potential for escalation which can mean new attacks and losses. The management of this type of crises demands active, flexible leadership and well-functioning command systems. However, the crisis management organization and planning of countermeasures should, as far as possible, be based on a common structure, i.e. in the contingency planning according to "all-hazards"[5] principle. It is useful especially for economic reasons but also for the sake of securing the efficiency.

The government resolution also defines the threat and emergency categories in details,[6] which signify unanticipated or sudden threats or events in normal, abnormal or emergency conditions that can endanger the security of the society or population. Those situations may require non-standard situation management and communications and a particular model situation can be included in several threat scenarios.

Threat scenarios are maintained as part of state administration's normal prediction and follow-up work and are updated during the time when the strategy and government resolution is reviewed. On the basis of the described scenarios, the competent authorities compile *more detailed threat estimates for their own fields of responsibility*. These estimates specify the origin of the threat, the target, the form it takes, its probability, the way it affects the authorities' capability to carry out their tasks as well as response options.

Preparedness responsibilities regarding emergency situations

Preparedness for various disturbance and emergency situations is one component in each administrative sector's overall preparedness arrangements. Preparedness encompasses

5) About the concept "all hazards" see e.g. Geary Sikich, *"All Hazards"* Crisis Management Planning, http://206.180.235.135/byauth/sikich/allhz.html

6) See Annexes 2 (Threat models) and 3 (Possible disturbance and emergency situations) of the *Government Resolution* 16.12.2010. They list situations of different categories of threat scenarios, and the ministries which are responsible for the management of the actual cases (i.e. a competent ministry and supporting ministries).

all measures required to ensure that duties can be discharged as smoothly as possible in all security situations. Such measures include, inter alia, contingency planning, advance preparations and preparedness exercises.

Preparedness is based on threat scenarios as well as on the key tasks required to manage emergency situations. The tasks include information gathering, the maintenance of a situation picture, making forecasts, prevention measures and maintaining preparedness for crisis management.

The threat environment, preparedness as well as the management of an emergency situation must also be examined from a geographical perspective. A global crisis and, especially, a crisis within the EU, may rapidly influence or alter the policies and decision-making in Finland. Conversely, a crisis affecting Finland may escalate into a European or global crisis. Furthermore, it is increasingly common for Finnish organizations and citizens to operate or dwell in areas more crisis-prone than Finland.

With regard to **preparing for disturbance and emergency situations,** the administrative sector within whose mandate the matter primarily belongs is the competent one. The aim is to **maintain unchanged the line of authority** for securing society's vital functions, organizations operating in normal conditions as well as the distribution of duties and responsibilities in special situations. Ministries take the development of preparedness legislation into account within their respective administrative sectors. It must be possible to promptly launch the required measures in a prognostic manner, albeit often on scant information. Controlling the situation may necessitate a rapid transfer of additional resources from other administrative sectors, the business community or from elsewhere in society.

The **competent ministries** bear the responsibility for organizing exercises dealing with emergency situations as well as making the required inter-sector cooperation arrangements and fulfilling the obligations related to the EU.

Functions vital to society include:

- Management of Government affairs
- International activity
- National military defence
- Internal security
- Functioning of the economy and infrastructure
- The population's income security and capability to function, and
- Psychological crisis tolerance

A desired end state (aim) has been established for each function, thus, making it possible for ministries to determine their respective **strategic tasks** as well as relevant **maintenance and development needs**.

Finland's membership in the European Union, activity within the United Nations, under the auspices of NATO's Partnership for Peace programme, and in other international venues have been taken into consideration as the descriptions of the mentioned functions, their desired aims and the development requirements for the strategic tasks were compiled.

✓ *1.4 Principles of the Decision Making in Crises*

Disturbance or emergency situations which jeopardize the society and population can rapidly turn out to be a crisis with surprises, high risks, potential for escalation and lack of time for decision making. Such a situation can no more be handled with normal administrative routine; instead it needs special methods but not necessarily an improvised ad hoc leadership or additional powers by the emergency legislation (Emergency Powers Act).

In well-functioning **crisis management arrangements**, the line of authority is clear, situations are proactively managed (and trained) and sufficient resources are immediately put into use. Inter-sector coordination bodies, such as the meeting of permanent secretaries and the meeting of the heads of preparedness, assist in the coordination of measures. Whoever is responsible for situation management is also responsible for the content of communications.

Pursuant to the Constitution, the *Prime Minister* directs the activities of the Government (State Council) and oversees the preparation and consideration of matters that come within the mandate of the Government.

The President of the Republic, within her/his powers, participates in decision-making concerning matters which affect Finland's relations with foreign states as well as security and defence policy. She/he is the supreme commander of the Defence Forces.

When the Prime Minister so decides or the competent minister proposes it, matters are brought before the *Government* (State Council) to be dealt with in the manner agreed on with the Prime Minister. On the initiative of the Prime Minister, either the joint meeting of the Cabinet Committee on Foreign and Security Policy (CCFSP) and the President of the Republic or just the Committee may prepare the Government decisions. The Committee is augmented by inviting the competent minister and pertinent experts to attend. The other cabinet committees deal with issues pertaining to their mandate.

Decisions required by the situation are made at the *Government plenary session*, by introduction of the *competent ministry* or some other *competent authority*.

In the present system of crisis management the *Prime Minister's Office* provides the basic support in matters relating to the situation picture, premises and communications. The *Government Communications Unit* supports the Government. Other necessary authorities, companies and organizations are also included in activities required for situation management.

The meeting of the permanent secretaries and *the meeting of the heads of preparedness* are permanent cooperation bodies. The level of situation management and coordination is determined by the seriousness and the extent of the situation. Top state leadership may also launch the required measures.

The crisis management system takes into account the obligations imposed on the member states by the EU's emergency and crisis coordination arrangements (CCA). Ministries are responsible for issues relating to the EU within their respective mandates. The function of the Government Secretariat for EU Affairs is to coordinate preparation and handling of issues relating to the European Union.

Crisis management model and cooperation between authorities

According to the s**tate's crisis management model**, the *competent authority* (officials from on-site leader to the ministry level) initiates measures as per its regulations and informs the preparedness organization of its administrative sector. *The Prime Minister's Office* runs the *Government Situation Centre* which builds on cooperation among ministries and supports Government-level management.

The *ministry* empowered by the law to do so leads activities and coordination among ministries, when required. The Prime Minister's Office makes certain that a competent ministry has been designated.

The *permanent secretary* bears primary responsibility for the preparedness of his/her administrative sector as well as for managing the security situation. The measures of different administrative sectors and, when necessary, the business community and NGOs, are coordinated by the *permanent secretaries' meeting*. The meeting is chaired by the State Secretary of the Prime Minister's Office, or the permanent secretary of the competent ministry.

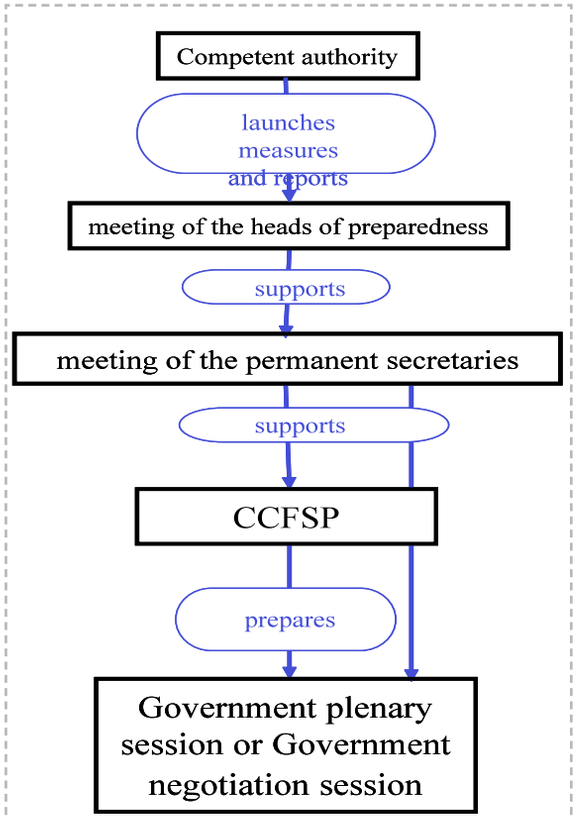


Figure 3: Crisis management model and levels of coordination (basic scheme).
CCFSP = Cabinet Committee on Foreign and Security Policy.

The *meeting of the heads of preparedness* supports permanent secretaries with regard to operational activities. The *Security Chief of the Government* (Head of the Government Situation Centre) chairs the meetings of the heads of preparedness or they can be chaired by the head of preparedness of the competent ministry, depending on the case in question.

The *Security and Defence Committee* is responsible for the longer term planning and preparations of the comprehensive national defence, and therefore, the crisis management model developed for acute crisis situations does not impinge on the role or tasks of the Committee.

The operational capabilities of the state leadership as well as the required support organization and systems are maintained through regular table top and live exercises.

In the new Government Resolution 2010 (p. 56) the above described scheme has been somewhat elaborated and simple function lines added with possibilities to make more direct contacts from one level to another level of decision making as well as build coordination contacts between authorities. This scheme emphasizes the normal preparation procedures of decisions with several supporting elements. It is still useful to ask how the decision making in crises could be clarified and made as simple as possible. The system containing many alternative procedures and all normal-time administration routines can be too time-consuming and complicated in a severe crisis situation.

The present crisis management model as such is clear in theory and meets the demands for legality and administrative efficiency, but we have not much experience of its function in new types of crises. Some lessons learned from the latest emergency situations and exercises signal that serious difficulties can emerge in surprising, complicated and multidimensional crisis situations, for example in a case of terrorist attacks.

✓ 1.5 Maintenance of the Situational Awareness and Communications

A prognostic and real-time situation picture shall be compiled to support Government decision-making and communications. The shaping of a more comprehensive situation picture will be achieved by taking into account and utilizing effectively the authorities' pre-existing or future information technology environments. Cooperation and planning that serves the compilation of the situation picture has been improved among the different sectors of administration. Cooperation between the gathering of information, the compiling of the situation picture and communications has also been intensified and tested. The range of instruments for gathering information is widened by, for instance, developing the monitoring of open information sources. There are still many practical difficulties to overcome.

National structures tap into the cooperation with the EU's Situation Centre (SitCen) and sector officials, e.g. FRONTEX concerning situations on the external borders of the EU.

Government level

The Government Situation Centre, which relies on cooperation among ministries and is run by the Prime Minister's Office, is organized and shall be reinforced according to the actual needs so that it can support Government-level civilian crisis management (Government, Cabinet Committee on Foreign and Security Policy, meeting of permanent secretaries, meeting of heads of preparedness) in all security situations.

The present arrangement of the situation centre with a permanent staff has been in effect from September 2007. It is working continually (in 24/7 principle) with security police professionals and keeps contact with other situation centres in Finland (e.g. Foreign, Interior and Defence Ministries) as well as with EU authorities in Brussels. The situation centre follows also other information sources, international news services, TV and Internet news etc.[7]

The ministries' situation centres are operative even in normal conditions and their staff must regularly participate in exercises. As premises are being developed, particular attention is paid to rapidly emerging situations which may demand enlarging the situation centres without

7) Timo Härkönen, *Tilannekuvatoiminta, valmiuspäälliköt*, PM Valtioneuvoston kanslia 7.3.2008.

delay to command centres.

The Government Situation Centre upholds awareness of the general situation and makes analyses for Prime Minister and Government. It can also alarm the other situation centres and relevant operational instances and specialists in an emerging crisis situation. If needed, the Government Situation Centre shall be enlarged and then built part of *Government's crisis command centre*.[8]

Contacts to the European Union's crisis management organisation are maintained by sector authorities and the Government Situation Centre. The latter has direct communication line to the EU Council's *Joint Situation Centre* (SITCEN)[9], which can alert the EU *Crisis Coordination Arrangements* (CCA) and the Community mechanism for facilitating reinforced cooperation in civil protection via ARGUS communication system. CCA is a cross-sector crisis management function on the political level which would and could be activated in case of a large crisis situation affecting several nationalities and European interests.[10]

The Finnish **sectoral surveillance** system is based on the principle where each sector authority will remain in conducting their normal tasks and responsibilities during special situations or crises. The sectoral data and intelligence information is produced and disseminated through several parallel and partly overlapping channels.

The main information providers are the Ministry of Defence, the Defence Staff, the Ministry of Foreign Affairs, the Ministry of the Interior (incl. the Border Guard, rescue services, Criminal Police and Security Police SUPO) and the Ministry of Environment. The situation picture and surveillance data are collected to the situation centres of the above mentioned authorities. The underlying principle is that these centres will further enhance the situational picture of the Government Situation Centre which upholds awareness of the general situation and makes analyses for the Prime Minister and Government. However, this principle needs still to be clarified and elaborated within various sectors of the government.

The general rule is that those running the activities are also responsible for the content of the communications. Other authorities provide support. Each authority is responsible for disseminating information about their activities. However, coordination, contacts and cooperation are of particular significance. *The Government Communications Unit* is responsible for the Government's and the Prime Minister's communications, as well as for coordinating the dissemination of official information.[11]

Both the communications of the Ministry for Foreign Affairs, responsible for international communications, and the communications of other key ministries in the situation are to be linked into crisis communications arrangements at as early a stage as possible.

As the crisis escalates, communications are further intensified and communications con-

8) Timo Härkönen, *Kriisijohtamismalli ja tilannekuva* (Crisis management model and situation picture) 14. 4.2008.

9) See e.g. Andrew Rettman, "EU diplomats to benefit from new intelligence hub", EUobserver. 22.2.2010. http://euobserver.com/9/29519

10) Sanna Kjellén, *Survey of EU warning systems*, Krisberedskapsmyndigheten 5.9.2007, p. 9.

11) *Government Communications in Crisis Situations and Emergencies*, Prime Minister's Office Publications 20/2008.

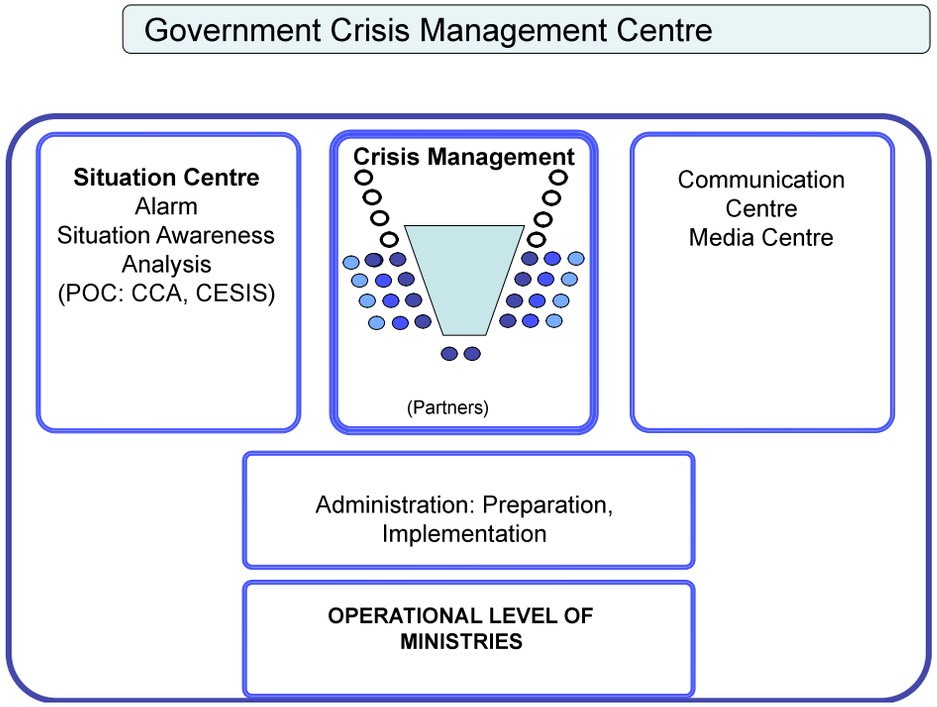


Figure 4: Government Situation Centre as a core enhanced to Crisis Management Centre.
Source: Timo Härkönen

trol may be centralized in the Prime Minister's Office. If necessary, a **Government Information Centre** is established. The Centre can issue orders to state authorities as regards the content of information. The authorities and the media work in close cooperation, but the proper functioning and independence of the media should be guaranteed.

According to the Government strategy the information service has a role in maintaining overall psychological crisis tolerance. Communications maintain the psychological and social fabric of society and help strengthen confidence in the authorities. Communications should also serve to prevent rumours, combat negative opinion making and prepare for information operations. Crisis communications and relevant responsibilities are included in the strategic tasks of the Prime Minister's Office.

Functioning of Government communications

The ability to support the Government and the Prime Minister through communications has to be maintained in all situations. This encompasses the coordination of inter-authority communications, dissemination of correct and timely information to the general public and the media as well as every ministry's responsibility for disseminating information concerning issues within its own administrative sector. However, in recent crisis situations the governmental information service has been in difficulties.

The Prime Minister's Office established a working group to prepare new guidelines for crisis and emergency conditions communications. A uniform evaluation system has been developed for the purpose of monitoring and assessing Government communications. A number of measures are being taken to develop the authorities' joint telephone and internet-based communication services. Examples include the setting up of a citizens' portal to serve crisis communications.

There are also some improvements concerning personnel. Duty and standby arrangements for communications staff are already in operation, and a sufficient number of civil servants are selected, earmarked and trained for crisis communications. The problem is that demands for an ever more effective crisis communication are still increasing by the technological and media cultural developments. The official, administration's communication and information system cannot be as flexible and rapid as are the various news and free information services and internet servers, but it has to be credible and effective enough to build a sound basis for relevant information for the citizens as well as administration's officials. It has also operational tasks in maintenance of situational awareness of the administration and various rescue services or law-enforcement forces.

Regional and local information systems

The regional administration in Finland is going through a profound change. At the beginning of 2010 started a new regional structure for general administration, and simultaneously police and rescue services got a new organisation and command structure. The ongoing change of the regional administration affects also the organisation of local rescue services, especially the arrangements of the alarm service.[12]

The information flow in the regional and local police and rescue services goes mainly internally within their sectors and without many connecting possibilities over sector lines. The new regional administration system cannot effectively take lead in emergency situations because the earlier provincial governments (lääninhallitus) have been replaced by institutions without operational powers. At present the government level leads directly the local rescue services and police authorities which can cooperate locally and form rescue service areas made up of a few municipalities. The responsible authority for rescue services is the municipality. There shall be 22 rescue service areas - consisting of cooperative municipalities - under the Ministry of the Interior. This is one thing demanding good cross area and sector communications as well as information services, because there are no more responsible regional rescue administrations.[13]

Summing up communication challenges

The good situational awareness at every level of the crisis management organisation is a crucial factor for success. At present there are many old and new problems starting with difficulties in understanding of special terms horizontally between service and administration sectors and vertically from the first responders up to the government level. *A very serious problem is the*

12) *See Hallituksen esitykset: HE 59/2009* (Government proposal with backgrounds). In internet: www.finlex.fi/fi/esitykset/he/2009/20090059 and *Valtion kriisijohtamisen toteuttaminen alue- ja paikallishallinnossa*. Työryhmän loppuraportti, Valtioneuvoston kanslian julkaisusarja 15/2009.

13) See Anssi Kuusela – Pekka Visuri – Timo Hellenberg, *Pelastustoimen tietovirrat erityistilanteissa. Analyysi pelastustoimen ja valtion keskushallinnon välisistä tietovirroista YETT-strategian mukaisissa erityistilanteissa.* Pelastusopiston julkaisu, B-sarja 2/2010, pp. 43-49.

insufficient interoperability of the information and communication technologies used by the rescue services, law-enforcement forces and the administration. There are many solutions for improvement of the interoperability, but they are expensive and becoming rapidly outdated. Also the training of the key personnel to use the modern communication technology is a very demanding task.

In the latest crises and exercises the managing of the information and communication technology has been rather difficult for the leaders who are not practised to use them in their everyday duties. They have also difficulties with the terminology which should be used orally or written in messages without delays. Therefore, they prefer direct contacts face to face or with telephones. That is a good practice as such if it is possible, but often the distances and overloading of the tele-networks make direct contacts impossible. One solution is to enhance video-conference capabilities. It can combine the benefits of a direct personal contact and rapid overcoming of the distances. However, the telephone or video conferences need a good infrastructure, especially many prepared and credibly functioning situation centres as well as special-trained and experienced personnel to exploit the technological advantages of these means.[14]

✓ *1.6 Some Findings and Critical Questions*

The Finnish crisis management system has theoretically a **clear strategy** and – at least so far - **well functioning structure** as well as rather **clearly defined procedures for decision making**. This was also noticed in the guidelines by the Government for the revision the strategy paper (SFVS) 2006.[15] The committee made reviews for the strategy working on the basis of the comprehensive security and national defence approach, and the Government accordingly issued a new resolution on 16. December 2010.

A special committee studied the organization of the preparedness system and published its report on 22 December 2010.

The strategy and guidelines for maintaining the preparedness are so far updated. We must, however, ask some critical questions on the basis of several research analyses[16] on the emergency situations and exercises during the latest decennium:

- Why there are still surprises, misunderstandings and mismanagement which have often been seen in actual crisis situations?
- Why sectoral thinking seems to be very much dominating the pattern of tactical

14) Lessons-learned from Kuusela et al (2010), pp.18 and 83-98 and Anna Mikkonen, *Valtioneuvoston tilannetietoisuuden muodostuminen lentoliikenteeseen kohdistuvassa CBRN-terrori-iskussa*, Aether-projektin työpaperi (Engl. The situational awareness of the State Council in a case of terrorist action against air transport with CBRN means, Working paper in Project Aether) November 2009 , pp. 7-14.

15) Interview with Matti Piispanen (Committee for Security and Defence Policy) 19.11.2009.

16) First and foremost is the case Tsunami 2004. *See The natural disaster in Asia on 26 December,* 2004, Investigation report A2/2004 Y, Helsinki 2005 (Onnettomuustutkintakeskus, Aasian luonnonkatastrofi 26.12.2004): www.onnettomuustutkintakeskus.fi/31811.htm

On search and rescue exercises e.g. *SAR-Prosessit,* toim. Hannes Seppänen ja Vesa Valtonen (Maanpuolustuskorkeakoulu, Taktiikan laitos 2/2008), pp. 34-38.

and strategic behaviour?
- What is the role of contingency planning?
- How important is training and independent evaluation?
- What are the essential duties and means in crisis management?
- What is the level of using external expertise i.e. private-public partnership?

In spite of advanced technology the most important reason for surprises and communication difficulties seems to be the human factor. The situational awareness is the basis for all crisis management measures, and therefore, the well trained and motivated personnel is indispensable for key tasks of the emergency preparedness organization. Observing of signs for early warning ensures rapid shaping of an accurate situation picture, and enhancing the situation awareness can improve crisis management capacity remarkably. There are, however, problems in cooperation between the first responders, different rescue services and governmental institutions concerning the situational awareness and distribution of relevant information.[17]

It is obvious that the role of planning is often misunderstood also in the Finnish crisis management. There can be a good strategy and well-written, detailed emergency plans, but in a real crisis the leaders still have to improvise practical measures because the prepared plans are too complicated, not up-dated and too much time consuming, or they are otherwise not suitable to the actual situation.

An often experienced tendency in crisis situations is that the leaders use ad hoc organisations and unofficial, direct communication and consulting methods. They can sometimes work, but there are always high risks of failure, too, because of the over-reliance on the capacity of a few persons to make improvised, bold and accurate decisions, and give right orders as a "hero" of the situation. For the large government systems the "ad hoc leadership" cannot be an optimal way to organize crisis management.

A useful basis for assessment and improvement of the planning and execution methods could be the traditional *Clausewitzian philosophy*. In the war-like situations, according to Carl von Clausewitz, the foreseeing of developments is always uncertain, if not impossible, and all kinds of frictions make a detailed and far-reaching planning irrelevant. That is why the military organisations have favoured simple planning methods and clear chains of command for fighting situations. The main task of the military leader has been "to bring order to the chaos of the battle".

As an application concerning the present emergency preparedness we have to foresee that crises always emerge as a surprise for the administration and citizens, and a perfect management of crises is an illusion. We must be prepared to counter all kinds of surprises and backlashes without losing the grip in handling the measures.

About the nature of planning Clausewitz argued that in the war situations
- A *plan* is valid only until the first engagement with the enemy and
- *Friction* is an essential factor in all war operations.[18]

It is useful to ask: How can those theses concerning the nature of war be applied to the present and future peace-time crisis management? For example, what kind of planning and technical preparations are optimal, as well as, what is the role of training and critical research?

17) See Kuusela et al (2010).

18) Carl von Clausewitz, *On War* (orig. 1832, ed/trans. Michael Howard and Peter Paret, Princeton University Press, 1976), books II-IV.

These matters will be discussed later in connection of counter-terrorism.

Summing up some of those findings in this chapter which can serve as a basis for the development of the Finnish crisis management system:

- The Finnish comprehensive defence doctrine is a well functioning and integrated system – but we must ask: Is it too heavy and clumsy for the new, complicated threat situations in the "grey zone" between small, normal-time hazards and the armed conflicts?
- Decision-making in the swiftly emerging and changing crisis situations seems to be too much terraced and segmented.
- The principle of legality of governance and the independence of authorities are highly appreciated features in the Finnish crisis management and a positive aspect as such, but are the procedures too slow for new threat situations?
- Guarding the bureaucratic sectors is notable in the administrative practices and unwillingness to use a so called external (objective) expertise and evaluation is evident.
- There is – especially on the government level - clearly need for a more comprehensive, accurate and timely situational awareness which should be based on the integrated situation picture.
- Those problems are significant concerning the counter-terrorism duties, because in the Finnish administration terrorism is seen only as a variation of criminality, not as a strategic means of fighting new types of war (cf. the US "war against terrorism" and vice versa).

2. Securing Air Passenger Transports Against CBRN Threats

✓ *2.1 Problem of Terrorism against Passenger Flights and Countermeasures*

Terrorist actions against the air transports were rather common in the 1960s and 1970s. The most usual threat was **hijacking of an airplane** in order to have people freed from jails or to get money for weapons. The actors were usually national liberation movements or other politically motivated groupings, e.g. Palestinians fighting against Israel or leftist organisations like RAF (Rote Armeefraktion) in Germany. The kidnappings of planes and passengers by single persons who only wanted to get out of the country to freedom were in fact no terrorist actions because they lacked larger political aims.

During the 1990s the hijackings almost ended. The security measures in the airports became more effective and the political motives were diminishing. The airport checks of passengers and improved luggage control made airplanes safer against both hijackers and attempts to use time-ignited explosive devices.

A totally new type of attacks began with the terrorist strike by al-Qaida against New York and Washington in September 2001. It was a large-scale **suicide attack** with most powerful means considered as a signal disaster that changed all. Also the counter measures were quite exceptional globally leading to unprecedented response not only by US Government but also its worldwide allies and friends. Europe got its part soon after in terms of London and Madrid

bombings.

The threat of hijacking is not totally vanished, and the security measures against it are still effective. For example, the British fighters have been alerted a dozen times during 18 months until March 2010 to follow and also intercept suspect flights nearing or already being in the British airspace.[19]

During the last years it has been very seldom that someone could try to get into the airplane as passenger with conventional weapons like pistols or explosives, because the security measures have improved so much. Still, there is some evidence which show that it is possible to smuggle explosive or otherwise dangerous material into the passenger flights.

The al-Qaida type international terrorist organisations have much experience and capability to find smart solutions to circumvent the improved security checks. They always probe new methods and technologies which can eliminate security controls. Also the best check technologies have weak points and practical difficulties when used, and only a multilayered and comprehensive mixture of intelligence about terrorists, profiling of passengers and various technical controls combined can secure the flights against terrorists and other violence.[20] However, an absolute safeguarding is impossible, and therefore we must be prepared for disasters resulting from a succeeded terrorist attack.

In countering the terrorist threat the most important task is to analyse the **strategy** used by terrorist organisations. Their methods change up to the political and societal situation as well as development of technology and countermeasures. The common feature by the present international terrorist organisations is a good organisation, experienced specialists for the use of high tech devices or destructive materials, clear political aims and a strategy which likes traditional military thinking with new unconventional means.

The main purpose of a terrorist act seems to be the rising of the public attention to their political aims and the power to reach them. The strategic reason of the terrorists is not to make large disasters with many human casualties but to build an impression of their ability to use further and escalatory violent means. That is the crucial deterrent effect of terrorist actions. Of course, there are exemptions in which only the violence and casualties as such can be the aim of a terrorist action.

✓ *2.2 New Threats and Problems*

As a result of the better checks and improved security technologies the threat of an unconventional attack against air transport has been more probable. It is a real possibility that terrorists can use also CBRN (chemical, biological, radioactive and nuclear) materials as terror weapons against airplanes. This threat is assessed very high by the analyses and programmes of the European Union, and also the United States has made large efforts to cope with that kind of threat.

19) See "RAF scrambles fighter jets after passenger flight terror alerts", *The Independent*, 29 March 2010.

20) See e.g. House of Commons Home Affairs Committee, *Counter-Terrorism Measures in British Airports*. Ninth Report of Session 2009-10, 24 March 2010.

In the internal strategy of the European Union[21] the main concerns include "terrorism in any form" and "serious organised crime" which very probably can also affect air transports. According to the EU counterterrorism strategy the CBRN threats are becoming ever more important, and special action plans have been made to counter them.[22]

A basic assumption in the Aether scenario is that the potential terrorists have also new unforeseen means to deliver dangerous material into the airplane, enough for a fatal attack against such an important strategic target. In this occasion it is not essential to assess how probable that kind of action can be and what the chances are for terrorists. We must assume that it can succeed if a well organized terrorist group has decided to do such an attempt.

✓ *2.3 New Threat Environment and Related Problems*

Some recent incidents can demonstrate the actual threats against air transports. They have rapidly effected drastic measures for improved security and been studied then more carefully in order to assess the relevance of those immediate restrictions and improved control measures.

An attempt to bring down an airplane nearing Detroit on December 25, 2009 was a striking example of new threats. A Nigerian national Umar Farouk Abdulmutallab tried to detonate an explosive device onboard a flight from Amsterdam to Detroit. The device did not explode because of a failure in the ignition attempt, and then the passengers and the crew restrained the man to try again the ignition. He had the explosive material tight in his underwear, and he had gone through security checks in Amsterdam. He was not on the terrorist watch list of American intelligence services, though they had watched him, yet without issuing a warning.

The incident rapidly caused a massive alert and large-scale improvement of security measures. The *U.S. Government* after a preliminary study published findings in a Presidential Memorandum, as follows:[23]

- "A failure of intelligence analysis, whereby the counter-terrorism (CT) community failed before December 25 to identify, correlate, and fuse into a coherent story all of the discrete pieces of intelligence held by the U.S. Government related to an emerging terrorist plot against U.S. Homeland organized by al-Qaida in the Arabian Peninsula and to Mr. Abdulmutallab, the individual terrorist;
- A failure within the CT community…run down all leads, and track them through to completion; and
- Shortcomings of the watch list system…"

The most significant findings were that the U.S. Government had sufficient information prior to the attack to have potentially disrupted the plot, but the intelligence community failed the analysis to "connect the dots" because of the insufficient cooperation between the various

21) Council of the European Union, *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, Brussels 8 March 2010. http://register.consilium.europa.eu/pdf/en/10/st07/st07120.en10.pdf

22) *See EU Action Plan on combating terrorism* 26 November 2009: http://register.consilium.europa.eu/pdf/en/09/st15/st15358.en09.pdf , pp.17-18.

23) *White House Review of the December 25, 2009 Attempted Terrorist Attack and Memorandum* for Secretary of State and others January 7, 2010.

services. A series of human errors occurred, and "information technology within the CT community did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information".

After that attempt the U.S. Government issued many enhanced measures for air security against terrorism and told that there have been increasing warnings concerning al-Qaida threat especially from Yemen. The administration had already 4000 air marshals securing the passenger planes, and they were to be added with hundreds of new persons. Also the full-body scanners in airports should be used more than before.

An example of a hazard, though without a direct terrorist dimension, was also an incident which occurred in a Finnair flight from Hong Kong to Helsinki in November 2009, as a passenger had placed several litres of fuel and tens of mobile telephones with batteries into his luggage. It was found out in the automatic luggage control after the landing in Helsinki. The luggage was dangerous because of the fire hazard.[24]

3. Finnish Crisis Management in the Case Aether

✓ *3.1 First Measures*

Alarm and first information

Information about health problems among the passengers in the airplane goes first to the Finnair's air controllers and medical advisers. Soon, after it becomes clear that it can concern a more serious matter than usual illness case, also the Russian and Finnish air controls shall be alarmed.[25]

After some additional information on the scale and quality of the problems also national and regional emergency centres and rescue services will be alerted, and the political leadership gets information through Government Situation Centre. It is not easy to estimate the exact time which should be needed for that alarm and information process because the situation is very complicated and unforeseen. We must suppose that there are many frictions and misunderstandings before the political leadership has a good overview of the situation.[26] It can be estimated that the Government Situation Centre could inform the political leadership in 1–2 hours after the first information on the unusual severe health problems in the airplane.

Rescue services

The first alarm to the rescue services[27] comes by the regional air control which reports of health problems in the airplane. It is not clear what is going on, and therefore the services cannot immediately give a general alarm or specify the problem.

24) See "Finnairin lennolla räjähdysvaara", *Helsingin Sanomat* and Ilta-Sanomat 12 March, 2010.

25) Interview with Kaarlo Karvonen, security chief of Finnair, May 2010.

26) See Mikkonen (2009).

27) http://www.pelastustoimi.fi/en/ and http://www.pelastustoimi.fi/media/pdf/esitteet2006/2006_pelastus_en.pdf

After learning that there are many passengers with severe health problems, the leadership of the rescue services must immediately alarm the medical teams and prepare a command post for rescue operations. It can use the prepared instructions for those measures. After the first situation analysis the most urgent problem shall be the organization of medical care and preparations for catastrophe management. An important task of the rescue leadership is to call the experts to research the cause of health problems in the airplane.

The Social and Health Ministry has a central role in the first call of experts and the analysis of the situation. For this duty it has a preparedness unit which can start measures immediately after the alarm from the air control and rescue services.[28]

The role of rescue services in a CBRN threat case is one of the main questions in the Aether studies, and it should be elaborated in further research efforts.

Police

According to the Finnish legislation the first responder and competitive authority in a case of terrorism is police. However, it can be very problematic to define if there is a terrorist action or not, because of weak or contradictory warning signals. Exactly this is the case in the Aether scenario as the first information of the symptoms is about health problems and, therefore, also the following emergency measures are of medical art. No terrorist has been identified in the airplane, and the signs hinting to a terrorist action become clearer only after a foreign terrorist group has issued an ultimatum with specified demands.

The role of police is problematic in this case which is utterly complicated and full of surprises. Normally the police start countermeasures against criminals or terrorists and begin the crime investigations in order to find out the persons who are guilty. If the suspected terrorists are in far-away countries, there must be a good cooperation between national and international police organisations and with political and rescue leadership. The Aether-type terrorist case has many difficulties concerning police duties.

✓ *3.2 Decision Making In the Finnish Crisis Management: A Critical Assessment*

The critical problem for the strategic-political decision making at the first stage is that the information is very vague and signals only to health problems. Obviously the first information, during 1–2 hours, about health problems in the airplane can be ignored almost totally at the government level.

The definition of the danger and decisions concerning relevant counter measures are complicated and time-consuming. The case is not like those in the usual search-and-rescue exercises, but it needs rapid cross-sector measures between rescue and medical services as well as police forces with no exact knowledge about the cause of the problems.

After the identification of a CBRN material and a terrorist threat, it is important that the political leadership can immediately decide the crisis management arrangements, especially the management structure and responsibilities for operational at-place measures as well as

28) Sosiaali- ja terveysministeriö, *Valmiusyksikkö*, esitteitä 2008:13.

the dissemination of information and cooperation with foreign countries and international services.

A special problem is information service because of the totally new and complicated situation. We have also some Finnish experiences which show that a very centralized information policy is inevitable. For example the first hijacking of an airplane to Helsinki in 1977 was at first shocking for the Government which had to decide collectively in a plenary meeting the principles of what to do and what to tell publicly. The tight decision making and centralized information policy were useful in that new situation which had many unforeseen risks and political pressures.[29]

The disaster in the nuclear power plant in Chernobyl 1986 showed especially the information difficulties which are connected with the radiation and radioactive materials. The accident was very surprising and happened in a far-away country, but the radioactive cloud reached Finland rather soon. The administration had many problems with the special terms and difficulties as generating adequate information, and so the confusion spread about dangers and need of protection. The preparations for that kind of disaster were insufficient, and it took too much time to make up clear-speak, well understandable information to the public. One reason was that the emergency planning for radioactive fall-out was made at the first place for a war-situation and secondarily also for an accident in a Finnish power plant. The pre-defined intensities for a radiation alarm were too high for a fall out from an accident in a distant country, and it was difficult to make rapid changes in the alarm and information services which could be more suitable for that kind of accident.[30]

We must assume that in the Aether case many difficulties can be like in the Chernobyl disaster in 1986. The rescue services are not experienced to handle CBRN threats, especially in a terrorism context. In the Aether-type situation the local and regional operative leadership probably have extensive problems with the terminology and effective practices, and at the strategic-political levels the difficulties in the decision-making can be immense, too. Therefore, a centralized and integrated strategic leadership is inevitable. Also communications with and between several agencies, countries involved and the intergovernmental context at large demands matured and politically experienced leadership, not only a sector approach based on specialized administrative assessment.

A terrorist attack with CBRN material demands that the high political and strategic leadership should be alarmed without delay, and the Government situation centre must be advanced to a command centre as soon as possible.

One of the biggest challenges will be how to clarify, confirm and conduct the right kind of situational picture among several different, multi-cultural stakeholders from both private and public spheres.

In the case of a terrorist attack with CBRN materials the problems of decision making and adequate conducting of response are rather similar as in the military operations. This does not mean that only trained military personnel can delivere these duties, but the organization and procedures

29) *See Suomi ja kriisit* (2003), pp.85-96.

30) Ibid. pp. 207-220.

of the civil administration must resemble the charasteristics of the military leadership in crisis management.

All preparations for that kind of terrorist attack should be done according to the above mentioned demands for the leadership and crisis management organization.

This kind of emergency situation can be managed only by means which are effective for rapid reactions during the critical hours for resolute counter-measures.

A strict legalistic and civil-administrative approach in managing a most threatening terrorist attack cannot be useful. Therefore, more studies and training, including cross sectoral and cross border exercises, for crisis management are further needed.

Bibliography

✓ Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", Brussels, 8 March 2010.

✓ Ehdotus uudeksi valmiuslaiksi (proposal for a new emergency act). Valmiuslakitoimikunnan mietintö (16.12.2005): Oikeusministeriö, komiteanmietintö 2005:2.

✓ European Union Counter-Terrorism Strategy, December 2005.

✓ Forsberg, Tuomas – Pursiainen, Christer – Lintonen, Raimo – Visuri, Pekka (eds), Suomi ja kriisit. Vaaran vuosista terrori-iskuihin. Gaudeamus, Helsinki 2003.

✓ Galera-Lindblom, Patrick – Henriksson, Anu and Lange, Stefanie, "The Early Warning System against Terrorism Attacks on the Ferry Traffic in Sweden" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Government Communications in Crisis Situations and Emergencies, Prime Minister's Office Publications 20/2008. Orig. Valtionhallinnon viestintä kriisitilanteissa ja poikkeusoloissa. Valtioneuvoston kanslia 10.9.2007. Valtioneuvoston kanslian julkaisusarja 15/2007.

✓ Hallituksen esitys Eduskunnalle valmiuslaiksi ja eräiksi siihen liittyviksi laeiksi. HE 3/2008 vp.

✓ House of Commons, Home Affairs Committee, Counter-Terrorism Measures in British Airports, Ninth Report of Session 2009-10, 24 March 2010.

✓ Härkönen, Timo, Kriisijohtamismalli ja tilannekuva (Crisis management model and situation picture) PM, 14. 4.2008

✓ Härkönen, Timo, Tilannekuvatoiminta, valmiuspäälliköt, PM, Valtioneuvoston kanslia 7.3.2008.

✓ Kjellén, Sanna, Survey of EU warning systems (revised version). Krisberedskapsmyndigheten 2007-09-05.

✓ Kokonaismaanpuolustuksen yhteensovittamisen strategia. Puolustusministeriö 2007.

✓ Kokonaismaanpuolustus (Total national defence). PM Turvallisuus- ja puolustusasiain komitea, Helsinki 15.4.2008.

✓ Kuusela, Anssi – Visuri, Pekka – Hellenberg, Timo, Pelastustoimen tietovirrat erityistilanteissa. Analyysi pelastustoimen ja valtion keskushallinnon välisistä tietovirroista YETT-strategian mukaisissa erityistilanteissa. Pelastusopiston julkaisu, B-sarja 2/2010.

✓ Mikkonen, Anna, Valtioneuvoston tilannetietoisuuden muodostuminen lentoliikenteeseen kohdistuvassa CBRN-terrori-iskussa, Aether-projektin työpaperi (Working paper in Project Aether) November 2009.

✓ Natural disaster in Asia on 26 December, 2004. Investigation report A2/2004 Y, Helsinki 2005.

✓ Nikula, Piia - Hellenberg, Timo, "EU crisis coordination arrangements and decision-making" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Parmes, Rauli (toim.), Varautumisen käsikirja. Tietosanoma, Helsinki 2007.

✓ Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Pursiainen, Christer – Hellenberg, Timo – Kivelä, Hanna-Mari, Puolustusvoimat ja sisäinen turvallisuus, Aleksanteri Papers 2:2004, Helsinki 2004.

✓ Report on the Implementation of the European Security Strategy – Provideng Security in a Chanching World, Brussels 11 December 2008.

✓ Rescue Services Strategy 2015. Ministry of the Interior publications 14/2008.

✓ Riskien hallinta Suomessa. Esiselvitys. Sitra, Helsinki 2002.

✓ Safety first. Internal security Programme. Government plenary session 8 May 2008. Publications of the Ministry of the Interior 25/2008. (Orig. Turvallinen elämä jokaiselle. Sisäisen turvallisuuden ohjelma. Sisäasiainministeriön julkaisuja 16/2008).

✓ SAR-prosessit. SAR-työryhmän loppuraportti, toim. Seppänen, H and Valtonen, V. Maanpuolustuskorkeakoulu, Taktiikan laitos, Helsinki, julkaisusarja 1, 2/2008.

✓ Siviilikriisinhallinnan kansallinen strategia. Sisäasiainministeriön julkaisuja 19/2008.

✓ Sosiaali- ja terveysministeriö, Valmiusyksikkö, esitteitä 2008:13.

✓ Suomen kokonaisvaltainen kriisinhallintastrategia. Ulkoasiainministeriö 13.11.2009.

✓ The Strategy for Securing the Functions Vital to Society. Government Resolution 23.11.2006.

✓ Valtion kriisijohtamismalli. Valtioneuvoston kanslian muistio 26.3.2008.

✓ Valtion kriisijohtamismallin toteuttaminen alue- ja paikallishallinnossa. Työryhmän loppuraportti. Valtioneuvoston kanslian julkaisusarja 15/2009.

✓ Valtioneuvoston asetus (Government decree) 7.6.2007 valtioiden rajat ylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajat ylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehdyn sopimuksen (ns. Prümin sopimus) voimaansaattamisesta.

✓ Varautuminen yhteiskunnan häiriötilanteisiin ja poikkeusoloihin. Puolustusneuvosto, Helsinki 1999.

✓ Visuri, Pekka – Hellenberg, Timo, "Finnish crisis decision making system, cooperation of authorities and communications" in Preventing Terrorism in Maritime Regions. Case Analysis of the Project Poseidon. Edited by Timo Hellenberg and Pekka Visuri. Aleksanteri Papers 1:2009.

✓ Volanen, Risto, "Siviilikriisien johtaminen demokraattisessa oikeusvaltiossa" in Monen monta demokratiaa. Kauko Sipposen juhlaseminaari eduskunnassa 25.4.2007. Eduskunnan tulevaisuusvaliokunnan taustajulkaisu 3/2007.

✓ Yhteiskunnan turvallisuusstrategia (Engl. Security Strategy for Society). Valtioneuvoston periaatepäätös 16.12.2010.

Interviews

✓ Cederberg, Aapo, Colonel, Committee for Security and Defence Policy, 6 April 2010.
✓ Karvonen. Kaarlo, security chief of Finnair, 19 May 2010.
✓ Piispanen, Matti, Committee for Security and Defence Policy, 19 November 2009.

Magnus Normark: The Swedish Crisis Management System and the National Strategy to Combat Terrorism

1. Introduction

In an early Saturday morning, 25 September 2010, a Pakistan International Airlines Boeing 777 from Toronto destined for Karachi in Pakistan requested an emergency landing at Arlanda International Airport outside Stockholm, Sweden. The air traffic control at Arlanda Airport was alerted by a pilot that a passenger may have carried explosives on board the plane. The initial information about the suspected individual had been called-in to the Canadian police by an anonymous Canadian woman. The phone call was made after the flight had departed Toronto airport on Friday afternoon.

The information about the potential threat was taken seriously by all involved. Swedish Police initiated cooperation with Canadian and US security agencies in order to identify the suspect while the Pakistani Airline crew made preparations for emergency landing at Arlanda airport. The aircraft circulated over the Baltic Sea on 2000 meters altitude for 30 minutes while dumping the jet fuel into the ocean before descending towards Arlanda for an emergency landing shortly after 07:30 in the morning. According to the Stockholm county police, the mood on the plane was calm, which may be because passengers were not informed about the real reason why the plane landed at Arlanda until they were evacuated.

After the landing the plane was immediately escorted to a site in the outskirts of the airports landing strip number three. 20 local police units and the national task force had been called to the airport to deal with the situation. All the passengers were evacuated within two hours, one individual of Canadian citizenship was apprehended and questioned suspected of planning to sabotage the airplane. The plane, all passengers and their luggage were then searched for explosives but no such materials where found. Eight and a half hours after the emergency landing the passengers were allowed to board the plane again and carry on their journey towards Karachi, via Manchester, England.

Two anti-terrorist policemen secure one of the passengers, suspected of carrying explosives onboard the Pakistan International Airlines Boeing 777 at Stockholm Arlanda International airport September 25, 2010. (AP Photo/Fredrik Persson)

Currently there is a heightened threat level in many countries throughout Europe, including Sweden, due to indications of planned terrorist attacks. The threat from non-state actors has to a high degree put the national crisis management system in an increasingly demanding situation, in trying to adapt the system to a more diffuse, dynamic and challenging security agenda.

✓ *1.1 Objectives and Methodology*

The objective of this paper is to describe the rather unique character of the current Swedish crisis management system in the European context. Furthermore this paper aims at describing the national strategy to combat terrorism and finally elaborating on the immediate response to an act of terrorism with a focus on national intergovernmental cooperation within a scenario framework.

The paper is a revised version of a previous study within the framework of the Project Poseidon; Preventing Terrorism in the Baltic Sea (EU DG JHL) and has been further elaborated in line with the aims and goals of the current project Aether. The study is primarily based on a literature review and qualitative interviews with representatives of Swedish agencies within the crisis management sector.

2. The Political and Administrative System in Sweden

Sweden is a constitutional monarchy and a parliamentary democracy. Political power rests with the government who answers and is accountable to the parliament (Riksdag). The Parliament passes laws, determines taxes and state expenditures, and so forth. The government's policies and decisions are implemented by the ministries via the governmental agencies. The governmental agencies are each linked to a ministry but work independently implementing laws and taking decisions within their own areas of responsibility and have their budgets. The regional level is organized into 21 counties, each with a county governor and a county administrative board, directly subordinate to the government. At the local level, there are 290 municipalities, each with a Municipal Executive Board, which is appointed by an elected municipal council (Lundgren 2009, Civil Contingencies Agency, 2009).

✓ *2.1 The "Swedish Model"*

In the Swedish constitution, the Constitution Act (one of the 4 Swedish Constitutions - *Grundlagar*) governs the relationship between the government and authorities. There is a ban on ministerial governance, which means that the government must act collectively and that the authorities may autonomously decide on matters relating to their authority and to law enforcement:

- The government's collective decision-making means that the government must act as a collective and, likewise, the responsibilities it holds are also collectively assumed by the government. For a government decision to be legitimate there

must be at least five ministers present at a Cabinet meeting. The individual ministers may not interfere with the affairs of the public authorities, since the public authorities answer to the government and not to an individual Ministry. Similarly, a minister may not make decisions on behalf of the government (Lundgren 2010).

- All government agencies answer to the government (except of those that are expressly governed by the parliament) and will generally follow the regulations and directives issued by the government. The authorities, however, are independent on some issues. The constitution says, "No authority, not even the parliament or the municipal governing body, may determine how an administrative authority shall act in a particular case concerning the exercise of authority, not even if the matter is directly related to a civil or public authority or to law enforcement." The authorities themselves interpret and apply the laws that concern their area of responsibility. If the Government believes that one agency's interpretation of a law is wrong, the Government may, instead, propose changes in the law (Lundgren 2010).

3. The Foundations of Swedish Crisis Management System

A new Swedish crisis management system was introduced in 2002. It emerged from the former civil defense system. The system is based on *everyday administrative structures, geographical territorial responsibility* and the *principles of responsibility, similarity, and vicinity*. The principle governing *regular administrative structures* means that no specific legislation may come into effect during an emergency or emergency-like situation; the normal laws apply even in the event of an emergency. In Sweden, there is no "crisis act" governing responsibility in crises at the national level and the government cannot proclaim a "state of emergency". The government is expected to pursue collective decision-making even in a crisis, and ministerial governance is still forbidden in a crisis, just as during normal conditions (Lundgren 2010). *The principle of responsibility* connotes that the same parties, which normally are responsible for an area or activity, should continue to be responsible for these same activities even in times of crisis (Government Bill 2008/09: 1, p 71). *The principle of similarity* means that the normal organization structures and location of activities should as much as possible be the same during an emergency or a crisis. *The principle of vicinity* means that a crisis should be managed at the lowest possible level which in turn gives the municipalities a significant role in the Swedish crisis management system (Government Bill 2005/06: 133, p 51). *The principle of geographical territorial responsibility* means that, during a crisis, there must be an actor responsible for coordinating resources and activities within a certain geographical area. The geographical territorial responsibility exists on three levels: the national (the Government), the regional (the County Administrative Boards) and the local (the Municipalities). The coordination of resources and activities should be done without taking over responsibilities from the other actors (Government Bill 2007/08: 92, p 77; Lundgren 2010).

4. Actors within the Swedish Crisis Management System

✓ *4.1. The Local Level: The Municipalities and the County Councils*

The Swedish crisis management system is highly decentralized and the Swedish municipalities have a large degree of autonomy. Following the principle of responsibility, the municipalities and the county councils also play an important role in civilian emergency planning and preparedness. The local government's area of responsibility also includes the great responsibility of coordinating all activities within the geographical area in the event of a crisis (Lundgren 2009). The responsibility of the municipalities and the county councils is regulated in the Act on Measures to be Taken by Municipalities and County Council in Preparedness for and during Extraordinary Incidents during Peace Time and Periods of Alert. The act aims to reduce the vulnerability of municipalities and county councils in their work so that they will have the capacity to deal with peace time emergencies and crises. The act regulates planning and preparations for the handling of complex, extraordinary incidents that demand coordinated management between various societal activities at local and regional levels (The Act on Measures to be Taken by Municipalities and County Council in Preparedness for and during Extraordinary Incidents during Peace Time and Periods of Alert).

✓ *4.2. The Regional Level: The County Administrative Boards*

At the regional level the County Administrative Boards are responsible for the coordination of risk and vulnerability analyses. During a crisis, they are responsible for coordinating the relevant measures taken by the relevant actors (Swedish Civil Contingencies Agency, 2009). The County Administrative Boards shall before, during and after a crisis promote coordination and cooperation of the measures taken within the county (The Government Ordinance Containing Instructions for the County Administrative Boards). During a crisis the county administrative boards hold geographical territorial responsibility in the county. This means that they shall coordinate the activities of the municipalities, counties and agencies, as well as coordinate information to the public and to representatives of the mass media and follow decisions made by the government concerning prioritizing resources and time (The Emergency Preparedness and Alert Ordinance).

✓ *4.3. The National Level: The Government and the Government Offices*

The government holds the geographical territorial responsibility at the national level. The government's responsibility for crisis management primarily concerns strategic issues while the responsibility for managing and coordinating operational activities of national character lies on the authorities. (Lundgren 2010) The Government Offices, with all the ministries together, make up one single authority. Following the principle of responsibility, every ministry is responsible for planning and handling crises within its own area of responsibility (The Government Ordinance contains instructions for the Governmental Offices). The Ministry of Defence is responsible for Defense and Emergency Preparedness (Government Bill 2008/09: 1, p 21).

In March 2008, the Crisis Management Coordination Secretariat was established at the Swedish Government Offices. This has contributed to a more obvious role with a clearer responsibility for the Cabinet Office in terms of crisis management, coordination and cooperation with the authorities during a crisis. The Prime Minister's Office directs and coordinates the work of

the Government Offices, and during a crisis the Prime Minister's Office is responsible for keeping the Prime Minister informed about the situation and the potential consequences concerning the developments in society and the Government Offices. The Crisis Management Coordination Secretariat is responsible for the development, coordination and follow-up of the crisis management capacity in the Government Offices (Lundgren 2009). During a crisis, the Secretariat's functions include monitoring the emergence and development of potential crisis situations both nationally and internationally, triggering the alarm, and providing status reports, as well as making assessments on how each event of the crisis can and/or will affect Swedish society (Government Offices of Sweden 2008).

4.3.1. The Agencies

In the Emergency Preparedness and Heightened Alert Ordinance, the government regulates the demands put on government authorities at the national and regional levels. The aim is to ensure that government authorities, through their work, reduce societal vulnerabilities and develop a good capacity for the activities during peace time emergencies and crises as well as during periods of heightened alert (Swedish Civil Contingencies Agency 2009). Some authorities have a special responsibility for planning and preparedness in order to enhance the ability to handle a crisis, to prevent vulnerabilities, and to withstand risks and threats. Those authorities shall, in particular, cooperate with the county administrative boards and with other government agencies, municipalities, county councils, associations and companies. During a crisis, these authorities shall also keep the Government informed about the consequences and measures taken (The Emergency Preparedness and Heightened Alert Ordinance). The authorities which have a particular responsibility for emergency preparedness in Sweden are divided into six so-called areas of cooperation:

- Technical infrastructure;
- Transportation;
- Hazardous substances (including chemical, biological, radiological, nuclear);
- Economic security;
- Coordination and information by geographical area; and
- Protection, emergency response and care.

Within each coordination area, various agencies are collectively responsible for coordinating and planning activities in order to reduce vulnerabilities and to enhance crisis management capabilities. The Swedish Civil Contingencies Agency (MSB) is responsible for the overall planning and resource allocation process concerning these six areas of cooperation. MSB shall also ensure that the agencies working in the different coordination areas interact regularly (Swedish Civil Contingencies Agency in 2009, Prop. (001/02: 158).

The Swedish Civil Contingencies Agency (MSB)

The Swedish Civil Contingencies Agency (MSB) became operational on 1 January 2009. The agency was created through a merger between the Swedish Rescue Services Agency, the Swedish Emergency Management Agency, and the Board of Psychological Defense (Lundgren 2009), and is a government agency under the Ministry of Defense. MSB shall contribute to the development and support of Sweden's emergency and crisis preparedness, act to prevent vulnerability, and develop reduction measures. MSB shall also encourage and stimulate coordination between relevant stakeholders in order to prevent, minimize, and manage emergencies and crises and their

consequences, as well as provide follow up and an evaluation of Sweden's emergency and crisis preparedness work (Swedish Civil Contingencies Agency 2009). Likewise, MSB shall also have a capability to provide support resources and foster coordination among relevant authorities in the event of a disaster or crisis. Furthermore, MSB should also be able to assist the Cabinet Office with support and information in connection with serious accidents and emergencies (The Government Ordinance containing instructions for the Swedish Civil Contingencies Agency).

The National Board of Health and Welfare

The National Board of Health and Welfare is responsible for activities related to health care, social services, health protection, and disease control. The National Board is also responsible for the coordination of protection against infectious diseases at the national level; for example, by monitoring developments on the county level, initiating joint actions between different stake holders, and taking the necessary initiatives needed in order to maintain effective disease control in the country. The agency may also be asked by the government to coordinate the use of health care resources during a severe national crisis (The Public Health Act). In its coordinating role, the National Board of Health and Welfare carries out contingency planning for infectious diseases in accordance with its authority and responsibilities under the Communicable Diseases Act (2004:168), the Ordinance (2006:942) on Contingency Measures and Emergency Measures, and the Ordinance (2007:1202) with instructions for the National Board of Health and Welfare (The National Board of Health and Welfare 2009).

The LFV Group (- Swedish Airports and Air Navigation Services)

The LFV Group operates and develops the state-owned civil aviation airports. The Group is also responsible for peace time air navigation services for civilian and military aviation. The LFV Group operates as a state enterprise. The organization is not funded through government taxes, instead earns its income from those services and products available at the airports managed by the LFV Group and from the Air Navigation Services. The LFV Group is required to pay a set dividend to the state (The LVF Group 2010a). On 3 December 2009 the Swedish Parliament decided to divide the LFV Group and create a limited liability company encompassing the airport. The new company, Swedavia, started its operation on 1 April 2010. Such a division of the LFV Group is logical considering the different business aspects of the airport and air traffic control (The LVF Group 2010b). The Air Navigation Services (ANS) is a separate division within LFV, and is responsible for air traffic control, briefings, telecommunications, and weather information for civilian aviation. ANS operates two control centers, airport and tower services, and terminal approach control centers in 37 places around the country (The LVF Group 2010c). The Air Traffic Control Tower at Arlanda airport controls planes that are approximately two minutes from the airport. Air traffic controllers in the air traffic control tower manage all traffic on the takeoff and landing runways and taxiways. All aircrafts in the Swedish airspace have to submit a flight plan for their flight; for example, involving controlled airspace or flights crossing the border into Swedish territory. The Flight Planning Center (FPC) conducts flight planning services, which means that they receive and transmit flight plans and provide the pilots with necessary information regarding the weather and military exercises (The LFV Group 2010d).

The Transport Administration

The Swedish Transport Administration began operations on 1 April 2010. It is a public authority that takes on responsibility for long-term planning of the transport system for road, rail, maritime and air traffic.

The authority is also responsible for the construction, operation and maintenance of public roads and railways. The Swedish Transport Administration includes activities and operations that before 1 April 2010 were undertaken by the Swedish Rail Administration and the Swedish Road Administration, as well as certain activities that were undertaken by the Swedish Maritime Administration and the Swedish Institute for Transport and Communications Analysis.

The National Police Board

The National Police Board may request assistance from the Armed Forces to fight terrorism if the aid is necessary in order to prevent, or otherwise penalize, an act that may constitute a crime under the Act 2003:148 on the penalty for terrorist offenses or if the intervention requires resources of a particular type that the police do not have access to. The Government shall give its consent before aid is issued by the Armed Forces. The Armed Forces are to provide assistance if the agency has resources that are appropriate and if it does not lead to serious obstacles in the agency's regular activities. Personnel from the Armed Forces, who are mobilized and used by the Police during such conditions, must be under the command of a military commander, who in turn must be under the direct authority of the Police (Lundgren 2009).

4.3.2 National Cooperative Areas in the Field of Crisis Management

Certain authorities have a specific responsibility for societal emergency management i.e. to reduce societal vulnerability and to deal with emergencies and disasters when they occur. These authorities are divided into groups based on identified cooperative needs, known as cooperative areas (CA). The decision on this can be found in the Ordinance on Emergency Management and Increased Preparedness. (2006:942)

The aim of the CA, through preventive work and in cooperation with authorities and other interested parties, is to identify how emergency management ought to and can be strengthened.

Strengthened emergency management can be achieved, for example, by jointly planning and executing projects, which in turn creates a unified approach to the measures that ought to be taken, public-private cooperation, exchanges of information, cooperation during international work, and research.

Joint planning primarily covers measures that increase this capability and measures that as a pre-condition require cooperation between several stakeholders. In other words, the CA work together to increase emergency management capabilities, to benefit from synergy results, and to ensure that necessary cooperation between stakeholders functions correctly in the event of a crisis. The role of the MSB (Swedish Civil Contingencies Agency) in the CA is partly to provide administrative support and partly to contribute to the work as one of the competent authorities. There are currently six national cooperative areas: Technical infrastructure (CATI), Transportation (CAT), Hazardous substances (CAHS), Economic security (CAES), Protection, rescue and care (CAPRC) and Geographic responsibility (CAGR). (The Swedish Civil Contingencies Agency, 2010)

Cooperative Area Transportation (CAT)

This CA aims to ensure the provision of basic transportation to meet societal needs in the event of peacetime emergencies and during periods of increased preparedness. CAT is currently working on:

- A collective basic course in order to strengthen joint emergency management capabilities.
- Strengthening the authorities' capabilities to respond and manage an incident with chemical, biological, radiological and nuclear materials (CBRN). This is done in cooperation with the Cooperative Area Hazardous substances.
- Risk and vulnerability – Dependency analyses are made in order to find common vulnerabilities and the potential of converging effects.
- Cooperation and dialogue with the private sector with the aim of strengthening the crisis management capabilities.

Participating authorities and actors in CAT are the Swedish Transport Administration, Swedish Transport Agency, Swedish Maritime Administration (SMA), Swedish Energy Agency, Swedish Armed Forces, County Administrative Board (Blekinge), The Municipalities (Ronneby) and County councils of Sweden (Västerbotten).

Hazardous substances (CAHS)

This CA aims to ensure that society is able to prevent risks and threats and deal with emergencies, as they occur, in the field of CBRN. CAHS is currently working on:

- Joint threat and risk assessment
- EU and other international cooperation
- Cooperation on research and development
- Support to regional stakeholders etc.

5. The National System to Combat Terrorism

The Swedish Security Service, which is the central actor for counter-terrorism intelligence in Sweden, issues directions on how the legislation is to be applied and supervises security issues, by checking that the authorities comply with the existing laws and regulation and that their protection is adequate in relation to the activities carried out (CODEXTER 2006 & Swedish Security Service 2007).

The national strategy to meet the threat of terrorism (*En nationell strategi för att möta hotet från terrorismen*)[1] drawn up by the Government in 2007 provides a framework of principles to be applied and proposes measures to be taken in counter-terrorism. The strategy uses a broad concept of terrorism covering not only the planning and execution of terrorist offences, but also propaganda distribution promoting violent acts, financing of indoctrination and recruitment for suicide bombing, and training in guerrilla warfare and the production of bombs.

On the basis of the EU Counter-terrorism Strategy of 2005, four pillars have been defined in the national strategy: to prevent (*förebygga*), to protect (*skydda*), to pursue (*avvärja*), and to respond (*konsekvenshantering)*. The strategy emphasizes the need for cross-border cooperation and sector policies, and proposes coercive measures. As long as measures follow the principles of an open, democratic society, these shall increase in proportion to the seriousness of the crime

1) Government Communication 2007/08:64. National responsibility and international commitment: A national strategy to meet the threat of terrorism.

and the degree of difficulty in investigating it (Ministry of Justice 2007).

Since 2003 the Act on Criminal Responsibility for Terrorist Offences (2003:148) is the central penal legislation against terrorist activities in Sweden, and is aimed at ensuring compliance with the commitments from the European Union's Framework Decision on Combating Terrorism of 2002. The act consists of a list of certain actions that may lead to penalties under the Swedish Penal Code. An action is to be regarded as a terrorist offence if it has the potential to seriously damage a state or an intergovernmental organization, intimidate a population or a group of the population, or compel a government to make a certain decision. Accordingly, terrorist offences may be murder, kidnapping, sabotage, hijacking, spreading poison or contagious diseases, and the illegal handling of chemical weapons (CODEXTER 2006).

✓ *5.1 Prevent*

The preventive counter-terrorism methods in Sweden are based on the notion that terrorist activities also are a threat against democracy. These measures are directed against propagation on the grounds of terrorism, both within the country and abroad. In this context, the risk factors identified in the national strategy are, among others, violent environments, widespread social changes, social and geographical segregation, and ethnic and cultural discrimination (Ministry of Justice 2007).

The Department of Integration and Gender Equality bears the main responsibility for prevention. The Department is therefore responsible for coordinating integration policies, introducing immigrants into Swedish society and initiating anti-discrimination measures. The Government's integration policy is carried out in all policy areas and implemented through general measures oriented towards, for example, labor, education, housing and public health (Ministry of Integration and Gender Equality 2008). Operationally, the preventive work against terrorism is directed towards preventing the creation of the very foundation of violent radicalization as early as possible so that police force intervention might not be necessary. For this reason, the primary measure is to build and enhance a dialogue between various government authorities and the public. Locally, this implies an open dialogue between the local authorities and the local police with schools, religious associations, non-profit organizations, and political parties. The Swedish Security Service is tasked with identifying and impeding extremist behavior and radicalization through mainly two activities: keeping a presence in environments where violent social circles may be found and where young people are often recruited; and warning teachers, parents and religious leaders concerning the risks and consequences of extremist activities in society (Ministry of Justice 2007).

Prevention is also carried out through legal penalties against the public encouragement of recruitment and training of terrorist activities, the divulgation of terrorist propaganda, and information on the production of bombs. Those measures are however difficult to apply since the principles regarding freedom of the press and expression should be followed. Voluntary measures taken by the mass media as well as Internet operators therefore play an important role in preventing the divulgation of terrorism related information (Ministry of Justice 2007).

Likewise, terrorism prevention takes place abroad through the development of aid programs as well as capacity building efforts under the UN and the EU in order to strengthen

counter-terrorism abilities of the recipient country. Here, the breeding grounds, such as poverty and conflicts, are addressed and the role of young people is enhanced. In addition, the role of fundamental law enforcement institutions and their proper working capacity is considered elementary for combating terrorism. Another example of the terrorism prevention abroad is participation in UN and EU peacekeeping operations in which Swedish military troops, observers, police officers, and civilian experts participate (Ministry of Justice 2007).

✓ *5.2 Protect*

According to the national strategy to meet the threat of terrorism, the protection of individuals, social institutions and their functions by reducing vulnerability is the main task for the Swedish State. Therefore, the protective measures aimed at improving border security, the protection of transport and means of transportation, critical infrastructures, and social institutions and their functions, as well as preventing the supply of weapons and dangerous substances for illegal use across borders are all extremely important activities (Ministry of Justice 2007).

The Swedish Civil Contingencies Agency plays a key role in counter-terrorism as it enhances coordination between the public authorities and private enterprises in order to build and strengthen crisis management capacity within each of the six coordination areas in the Swedish crisis management system. Each coordination area functions as an exchange forum for the authorities and various interested stakeholders involved in crisis preparedness, such as terrorist attacks. The Swedish Civil Contingencies Agency is also responsible for the coordination and strategic planning in protection against dangerous substances, including chemical, biological, radiological and nuclear agents (The Emergency Preparedness and Heightened Alert Ordinance).

The coordination area for "protection, rescue and care" in the Swedish crisis management system consists of seven authorities: the Swedish Coast Guard, the Swedish Transport Agency, the National Police Board, the Swedish Maritime Administration, The National Board of Health and Welfare, the Swedish Rescue Service Agency, and the Swedish Customs Service (SEMA 2008).

Besides being responsible for the task of protecting Sweden, its citizens and institutions, as well as foreign institutions located in the country, from persons who may threaten their security, the Swedish Security Service also plays a central role in the execution of protective measures against terrorism. The Security Service provides intelligence, risk assessments, and methodological know-how to the authorities and operating companies involved in border control and maritime safety. In their work on protecting important infrastructures and institutions, the Security Service also performs record checks on individuals, which form part of the security screening procedures carried out by other authorities and form a basis for decisions concerning for example employment (Swedish Security Service 2007).

✓ *5.3 Pursue*

The Swedish Security Service has been the main actor in Sweden in identifying and following up networks and individuals who are involved in terrorism both in the country and internationally. The institutional framework for counter-terrorism in Sweden has however been modified according to a broader model, the so called Joint Terrorism Analysis Center (JTAC). The core of the JTAC model is a center where authorities from the intelligence community are

brought together in order to analyze and carry out risk assessments on terrorist threats. Since 2009 the main center for this risk assessment is the National Center for the Assessment of Terrorist Threats, which is a working group within the Counter-Terrorism Cooperative Council (Nicander and Leijonhielm 2008).

The Center for the Assessment of Terrorist Threats is composed of the Swedish Security Service, the Military Intelligence and Security Service, and the National Defense Radio Establishment. The group has the task of following terror threats facing Sweden and Swedish interests. In fact at least once a month, if not more often depending on the circumstances, they make a joint assessment on these types of threats which are then presented to the Government Offices and the members of the Counter-Terrorism Cooperative Council (Swedish Security Service 2007).

The Swedish Security Service gathers intelligence information from open and secret sources on the local, national and international levels. Internationally, the Security Service collects intelligence information through liaison officers stationed at various key European locations as well as through cooperation with other countries' security and intelligence services. The risk assessments produced by the Security Service are used as a basis for alerting both public and private organizations on potential terrorism hazards as well as an element in more comprehensive risk assessments produced by other governmental agencies. The Security Service also cooperates directly with the authorities, mainly the members in the Counter-Terrorism Cooperative Council, in monitoring activities since these provide intelligence information under different agreements (Lundström 2008).

Within the Swedish Police Service, the National Criminal Investigation Department works independently both administratively and operationally from the Swedish Security Service. The National Criminal Investigation Department provides technical and Internet surveillance as well as investigation and criminal intelligence support to the police in cases involving crimes with nationwide or international ramifications. The Department is also the national contact center for all the police organizations and coordinates their activities. Within the Department, the International Police Coordination unit is the contact point between the Swedish Police Services and international authorities including the Interpol, Europol and Sirene (NCID 2008).

In order to secure the communication between the Security Service and the National Criminal Investigation Department, routines exist for intelligence exchange and the use of different channels for data collection. In addition, the Security Service's regional units cooperate with the 21 independent police authorities (Lundström 2008).

The Military Intelligence and Security Service is a directorate of the Swedish Armed Forces and is an important contributor in the intelligence community in Sweden, especially in terms of international surveillance. It is responsible for Sweden's military intelligence such as acquiring and presenting information that is of military importance regarding foreign powers and managing the security for vital divisions and agencies of the Swedish Armed Forces (Ministry of Justice 2007).

The National Defense Radio Establishment also plays an important role in providing intelligence from abroad. It is a civilian government agency and is subordinate to the Ministry of Defense. It is responsible for intelligence gathering (via interception of signals) and for supporting and maintaining IT security for government authorities and state owned companies. In addition, the Establishment receives assignments from several authorities, including the Swedish Government, the Security Service, and the Military Intelligence and Security Service (FRA 2008).

✓ *5.4 The Counter-Terrorism Co-operative Council*

The Counter-Terrorism Cooperative Council was established in 2005 and is made up of thirteen government agencies, represented by their Directors General or similar. The function of the Council is to work towards strengthening Sweden's ability to prevent terrorism by better co-coordinating the activities and information exchange of these agencies. The Council, which is based on the EU Strategy on Counter-Terrorism and the Swedish Government's national strategy to meet the threat of terrorism, is made up of the following agencies:

- The Armed Forces
- The National Economic Crimes Bureau
- The National Defence Radio Establishment
- The Prison and Probation Service
- The Swedish Civil Contingencies Agency (MSB)
- The Swedish Coast Guard
- The Swedish Migration Board
- The National Criminal Police
- The Swedish Security Service
- The Swedish Defence Research Agency
- Swedish Customs
- The Swedish Prosecution Authority
- The Swedish Radiation Safety Authority

✓ *5.5 The National Centre for Terrorist Threat Assessment*

The Counter-Terrorism Co-operative Council appoints working groups when necessary and for various themes. There is a permanent working group called the National Centre for Terrorist Threat Assessment (Nationellt Centrum för Terrorhotbedömning, NCT), made up of representatives of the Security Service, the Military Intelligence and Security Directorate and the National Defence Radio Establishment.

The NCT produces long- and short-term strategic assessments of the terrorist threat against Sweden and Swedish interests. The NCT is also tasked with producing strategic analyses of incidents, trends and international developments with a limited focus on terrorism that may affect Sweden and Swedish interests abroad. (Security Service 2010)

✓ *5.6 Border Control*

The Swedish Customs Service cooperates nationally and internationally on combating organized crime through intelligence exchange with the Swedish law enforcement authorities, mainly the National Criminal Investigation Department and the Security Service. Internationally, the Customs Service has direct contact with law enforcement authorities abroad, and actively par-

ticipates in Europol, where a liaison officer is situated. Liaison officers are also strategically located in other countries to provide information and intelligence (Swedish Customs Service 2008).

The Swedish Migration Board is responsible for issuing permits for people visiting and settling in Sweden and for granting asylum. In order to prevent the entrance of persons affiliated to terrorist groups, decisions taken by the Migration Board are based on assessments and recommendations made by the Security Service. Specifically, under special procedures and requirements, expulsion and refusal of entry cases are intervened by the Security Service who recommends that a foreign individual may be refused entry or expelled (CODEXTER 2006).

✓ *5.7 International Cooperation*

Cooperation between other intelligence organizations in bordering countries is well-established. This concerns both official and informal channels. Swedish legislation on mutual assistance in criminal cases is general and regulates the cooperation related to counter-terrorism action. It is based on the assumption that it should be possible to provide assistance at the international level to the same extent and under the same conditions in which national procedures apply. Mutual assistance can take place when arresting suspects or gathering evidence through questioning and apprehending suspects as well as in the interception of telecommunication and control of goods transport. The main instrument for international cooperation in criminal matters is the Council of Europe Convention of 1959 on Mutual Assistance in Criminal Matters and the additional protocol to this convention (CODEXTER 2006).

✓ *5.8 Terrorism Financing*

Swedish legislation is in line with the standards provided by the Financial Act on Task Force (FATF), which is a forum for international cooperation against money laundering and the financing of terrorism (Ministry of Justice 2007). Penalties for financing terrorism are found in the Act on Criminal Responsibility for the Financing of Particularly Serious Crimes in Certain Cases (2002:444), which since 2002 implements the UN Convention for the Suppression of the Financing of Terrorism. The Act contains sanctions on the collection, provision or reception of funds or other assets that are intended to be used to support particularly serious crimes such as terrorist activities. In this context, financial institutions are required to check all transactions that may be suspected of supporting terrorism and other serious criminal activities, and to report these activities to the police authorities (CODEXTER 2006).

Coercive measures preventing the financing of terrorism involve cooperation between many authorities including the Security Service, the Finance Police, the Prosecution Authority, the National Economic Crimes Bureau, the Swedish Customs Service, the Swedish Financial Supervision Authority, and the Swedish National Tax Agency, as well the private sector and private financial institutes (Ministry of Justice 2007). In the implementation of measures against financing of terrorism, the National Economic Crimes Bureau is the coordinator for the actions against combating economic crime. Specifically, the Bureau proposes preventive measures to government agencies and the intelligence community regarding how economic crimes can be effectively combated (CODEXTER 2006).

The Swedish Financial Supervision Authority exercises the supervision of financial institutions and issues regulations on matters relating to the fight against financing terrorism. The authority is also responsible for freezing the assets of institutes financing terrorist activities (CODEXTER, 2006).

Within the National Criminal Investigation Department, the Finance Police is responsible for gathering, processing and analyzing intelligence information on criminal or terrorist related financing activities. In order to proceed with a formal investigation, information must be handed over to the National Criminal Investigation Department and the Swedish Prosecution Authority (NCID 2008).

6. The Immediate Response to an Act of Terrorism

Sweden has been spared from the violent acts of terrorism during the past decades. Even if the terrorist threat for a long time has been assessed as low by the national intelligence and security agencies, the threat can quickly escalate as an effect of complex interaction of seemingly minor events. In a situation where a terrorists attack has occurred, for instance at an airport or targeting an aircraft in Sweden, the rescue service, police and medical first responders are the first at the scene, in the same way as when responding to an accident. The first priority at the scene is to save lives. An investigation of the crime is not initiated until the initial rescue response is completed.

The initial information regarding the terrorist attack would normally come to the national response agencies' attention through the SOS-Alarm center which can be reached by the public special emergency call number 112 in Sweden for getting help from all the emergency services and the police. The SOS Alarm centers are accessible 24 hours every day and co-ordinate the dispatching of the emergency services. A terror attack onboard an aircraft would initially be reported by a pilot to the airport command tower, which then triggers the national chain of alarm. In an effort to increase the ability to quickly establish a situational awareness and early coordination and cooperation between the air security command and control center and the police authority, a joint command and control facility has been established at Arlanda International airport.

In the next stage the first responders arrive to the scene of the attack and initiate the work with a priority to save lives. The first responders need always take into account that the scene of the crisis can be a crime scene where forensic leads and evidence have to be preserved in a correct way for the possible subsequent investigation. The police take charge over the scene, seal off the concerned area and establish a specific area for handling of victims. If the initial assessment of the situation is that the number of victims is high, a temporary crisis management group is established on the closest larger hospital. The National Center for Terrorist Threat Assessment may elevate the current threat assessment if there are indications of an act of terrorism. The Security Service establishes a close coordination with the local police.

During the third stage of handling the crises the victims are rushed to hospital or potentially to different hospitals if the number of victims is high in accordance with directions from the local County Administrative Board. The local County Council takes preparations to establish a crisis management board in order to facilitate rapid decision making during the crisis. At the Government level the Crisis Management Coordination Secretariat is briefed of the incident by

the NCT. The crime scene investigation is initiated by the police.

In the following stages the investigation has concluded that the incident is the work of a potential terrorist which brings the responsibility from the police to the Secret Service to continue the investigation in cooperation with the Swedish Prosecution Authority's office for security related cases. The Counter-Terrorism Cooperative Council assembles and assesses the situation with support from NCT and coordinates issues of common concerns like the handling of the growing media attention.

7. Conclusions

The Swedish civil crisis management system is a highly decentralized system which due to the basic framework of sectorial responsibility structure leads to challenges for the central government to be able to oversee the national crisis management capabilities and planning as a whole. The national crisis system is by tradition foremost dimensioned and shaped by the possible occurrence of natural accidents and hazards with the general perspective that resources and preparedness for such naturally occurring incidents and accidents still is relevant in the event of antagonistic threats and terrorist attacks.

Everyday structures and processes apply during a crisis which should be managed by lowest possible level as far as possible. Not until the local resources are starting to become insufficient or the effects of the crisis spread to a regional area are the regional level and finally, if necessary, the central level involved in actively responding to the crisis.

The concept of Cooperative areas is an important forum for the development and planning of the Swedish crisis management capabilities, not only for coordinating the development of capabilities but also for joint funding of various measures. Furthermore the creation of the PM's office Crisis Management Coordination Secretariat has contributed to a strengthened government crisis management capability and facilitated a better ability for central oversight of the national capabilities as well as enhanced the cooperation towards the authorities.

Bibliography

- ✓ Lundgren, Jenny (2009). *Krishantering i Sverige* (Crisis management in Sweden). Unpublished manuscript. Stockholm: CRISMART.
- ✓ Lundgren, Jenny (2010). *Organisering och reglering* (Organization and regulation) Unpublished manuscript. Stockholm: CRISMART
- ✓ The National Board of Health and Welfare (2009), National plan for pandemic influenza – including a basis for regional and local planning. Article no. 2009-126-204.
- ✓ The Swedish Civil Contingencies Agency (2009), *International CEP handbook 2009: Civil Emergency Planning in the NATO/EAPC Countries*. ISBN: 978-91-7383-020-1.
- ✓ CODEXTER – Committee on Experts on Terrorism (2006). *Profiles on counter-terrorist capacity: Sweden*. Council of Europe.
- ✓ Swedish Security Service (2007). *Security Service 2007*. The Swedish Security Service, Stockholm.
- ✓ Ministry of Integration and Gender Equality of Sweden (2008). *Integration and diversity*. Published 2004, last updated 2008. Available at: http://www.sweden.gov.se/sb/d/2188/a/19443 (downloaded 8 October 2008).
- ✓ Ministry of Justice of Sweden (2007). *National responsibility and international commitment: A national strategy to meet the threat of terrorism.* Government Communication 2007/08:64. Ministry of Justice 2007. Swedish Government Offices, Stockholm
- ✓ NCID – National Criminal Investigation Department of Sweden (2008*). Polisens risk- och sårbarhetsanalys 2008*. Rikspolisstyrelsen, Stockholm.

Interviews

- ✓ Lundström, Michael (2008). The Swedish Security Service, Stockholm (25 August 2008). Interviewer Patrick Galera-Lindblom.
- ✓ Nicander, Lars and Leijonhielm, Jan (2008). Center for Asymmetric Threat Studies (CATS), Stockholm. Interviewers: Patrick Galera-Lindblom, Anu Takala, and Stefanie Lange (27 August 2008).

Acts and Ordinances

- ✓ The Act on Measures to be Taken by Municipalities and County Council in Preparedness for and during Extraordinary Incidents during Peacetime and Periods of Heightened Alert. *(Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap)*
- ✓ The Emergency Preparedness and Heightened Alert Ordinance. *(Förordning (2006:942) om krisberedskap och höjd beredskap)*
- ✓ The Government Ordinance Containing Instructions for the County Administrative Boards. *(Förordning (2002:864) med länsstyrelseinstruktion).*
- ✓ The Government Ordinance Containing Instructions for the Government Offices *(Förordning (1996:1515) med instruktion för Regeringskansliet).*
- ✓ The Government Ordinance Containing Instructions for the Swedish Civil Contingen-

cies Agency. *(Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap)*.
- ✓ The Public Health Act *(Hälso- och sjukvårdslag (1982:763)*.
- ✓ The Emergency Preparedness and Heightened Alert Ordinance. *(Förordning (2006:942) om krisberedskap och höjd beredskap)*

Government Bills

- ✓ Prop. (2008/09:1) 2009 Budget Proposals. Government Bill *(Budgetproposition för 2009)*.
- ✓ Prop. (2001/02:158), Society's Safety and Preparedness. Government Bill *(Samhällets säkerhet och beredskap)*.
- ✓ Prop. (2005/06:133), Cooperation during crisis: For a Safer Society. Government Bill *(Samverkan i kris – för ett säkrare samhälle)*.
- ✓ Prop. (2007/08:92), Increasing Crisis preparedness: For the sake of Safety. Government Bill *(Stärkt krisberedskap – för säkerhets skull)*.

Internet

- ✓ Government Offices of Sweden (2008). http://www.regeringen.se (2008-09-15).
- ✓ The LFV Group (2010a), http://www.lfv.se/en/Start-page/About-LFV/LFV-Group/ 2010-03-12.
- ✓ The LFV Group (2010b), http://www.lfv.se/en/Start-page/About-LFV/LFV-is-divided/ 2010-03-12.
- ✓ The LFV Group 2010c) http://www.lfv.se/en/Start-page/About-LFV/Management-and-organisation/ 2010-03-12.
- ✓ The LFV Group 2010d) http://www.lfv.se/sv/LFV/Om-LFV/LFVs-verksamhet/Flygtrafiktjanst/ 2010-03-12.
- ✓ FRA - National Defense Radio Establishment (2008). http://www.fra.se (downloaded 14 September 2008).
- ✓ SEMA – Swedish Emergency Management Agency (2008). http://www.krisberedskapsmyndigheten.se (downloaded 14 October 2008).
- ✓ Swedish Customs Service (2008). http://www.tullverket.se (downloaded 10 October 2008).
- ✓ Security Service (2010). http://www.sakerhetspolisen.se (downloaded 29 April 2010)

Jan Leijonhielm: The Russian System Concerning Air Traffic Security and Incidents

1. Introduction

In the Aether scenario a Finnair flight is contaminated with an unknown CBRN agent. The plane will fly in Russian airspace for approximately five hours. When knowledge about severe health problems is conveyed to Russian authorities a number of questions arise: What if it is perceived to be a terrorist attack? Will Russian airspace control ask the plane to land in order to prevent a crash on Russian territory or will it let it pass in hope of reaching its destination? What if the pilot would consider it too risky to continue the flight and ask for landing permit? Where does the decision lie, with the civil air-traffic control or the military one, and what will be the role of Russian emergency authority, EMERCOM? Will the counterterrorism authorities have any say in the matter? What rules and practises apply to this situation? What will the communications inside Russia and with responsible authorities abroad look like? In case of an emergency landing or crash, who is responsible for the emergency operations, EMERCOM or counterterrorism authorities?

A number of similar questions point to the possible existence of a grey zone of uncertainty, where decisions will have to be made quickly. Even if the Aether scenario does not develop into a Russian active or operational participation, there are several reasons for analysing possible Russian options and patterns in this context, if we are to discuss a realistic scenario, in particular since the Russian air security sector for the present is undergoing a number of changes.

2. Methodology

Russian authorities have never encountered or handled the particular problems in the Aether scenario and open research or rules on this particular subject hardly exist in Russia. Furthermore, institutions, authorities and persons related to this field have shown a reluctance to be interviewed or hand over relevant material, possibly because of the unclear rules, but also probably due to the fact that many details in civil-military cooperation in the field of air security are considered a military secret. The study will for those reasons focus on available open sources, present patterns and factors which can be viewed as an outer framework for Russian handling of CBRN-threats concerning air safety.

3. Outline of the study

The study aims to describe relevant Russian authorities' modus operandi and responsibilities regarding air traffic control and security in order to establish which may be relevant to the Aether project and in a wider context how these fit in with international cooperation. Thus the

structure and tasks of EMERCOM will be looked into. Technical systems, like the GLONASS system and the joint CIS air security agreements will be briefly described, as they form a framework for the air security sector in Russia. Earlier experience is partly relevant and of a certain value, but recent experience, apart from terrorist attacks in the early 1990-ies, is lacking. Russia´s international cooperation, mainly with NATO, but also with IATA has lately grown in importance and will also be scrutinized.

4. The Russian Emergency System

EMERCOM (Emergency Control Ministry) or The Ministry of Emergency Situations (Министерство по чрезвычайным ситуациям - МЧС России) was established on January 10, 1994 by president Boris Yeltsin. The complete official designation is Ministry of the Russian Federation for Affairs of Civil Defence, Emergencies and Disaster Relief (Министерство России по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий). Some consider the real date of birth of the agency as December 27, 1990, when the Russian Rescue Corps was established and assigned the mission of rapid response in the case of emergencies.[1] The Ministry has since its start been headed by Sergei Shoigu. He was appointed by President Yeltsin in November 1991 and is thus the only minister who has kept his post since then. He is also one of Russia´s most popular political figures, often ranking just below Prime minister Putin and President Medvedev in popularity polls, although the fires in summer 2010 somewhat decreased his popularity.[2]

The overriding responsibilities consist of information cooperation tasks aimed at providing safety of the population and territories on the Federal, Interregional and Regional levels; Russian Emergency Rescue Service (RUERS) forces handle management, organization and conducting interdepartmental cooperation while solving the tasks on emergency prevention and relief.

The main tasks of EMERCOM are:

1) working-out and implementation of the state policy in the field of civil defence, protection of population and territories against emergencies, providing fire safety and also people safety on water bodies within the competence of Emergency Control Ministry of Russia;

2) organization of preparation and approval in accordance with established order of drafts of normative and legal acts in the field of civil defence, protection of population and territories against emergencies, providing fire safety and also people safety on water bodies;

3) implementation of management in the field of civil defence, protection of population and territories against emergencies, providing fire safety, people safety on water bodies, and also management of activity of federal executive authorities

1) From the official EMERCOM site at www.emercom.ru and Wikipedia "EMERCOM"

2) see f e ITAR Tass 5th of August

within the framework of a single state system of prevention and liquidation of emergencies;

4) implementation of normative regulation for the purposes of prevention, prediction and mitigation of consequences of emergencies and fires, and also implementation of special, licensing, supervisory and control functions on questions related to the competence of Emergency Control Ministry of Russia;

5) implementation of activity on organization and conducting of civil defence, urgent response to emergencies, protection of population and territories against emergencies and fires, providing people safety on water bodies, and also realization of measures on emergency humanitarian response including outside the Russian Federation.

It is thus to be noted that EMERCOM is the leading authority in emergencies on land and at sea, while mainly lacking jurisdiction concerning air safety and airspace, with the exception stated in the National Emergency Management Centre´s tasks (paragraph 7) below, concerning high risk cargo and the use of the GLONASS system in this context .

5. The National Emergency Management Centre

At the end of 2006 the Government set EMERCOM of Russia the task to take all the necessary measures to establish a National Emergency Management Centre (NEMC).

This task was done fairly quickly. Already in 2007 the NEMC came into existence and assumed the task of managing the forces and facilities of the State System of Emergency Prevention and Relief, Civil Defence in critical emergency conditions.

At present similar centres have been created and function in a number of European States. However, there are no analogues to the Russian firmware set of decision making assistance, developed specially for the NEMC.

The NEMC information resources base consists of reference-information data bases available in any operating mode.

NEMC tasks:[3]

1. Conducting continuous monitoring of the territory of the country and the state of Russian Complex System for Informing the Population, named "Tsunami", the system of objective control of objects
2. Forecasting of the possible emergencies and calculation of the scenario of the possible natural and technogenic emergencies
3. Conducting video control for the state of critically important facilities for the national safety
4. Automatization of the data base management processes and the processes on emergency of any level prevention and relief

3) From the official EMERCOM site at www.emercom.ru

5. Automated information collection about the economic entities by means of Unified Duty Dispatch Service "112", EMC RC and the subjects of the Russian Federation, issuing the classified information to the management
6. Automated informing of the population in case of a threat or any information about an emergency with an opportunity of a feedback in real time mode by using the All-Russian Complex System for Informing the Population
7. Organization of control and accompanying of the naval (river), above the ground, air deliveries on the territory of the Russian Federation as well as abroad with the use of the system GLONASS-GPS, controlling the delivery of the high-risk cargo, humanitarian aid cargo
8. Organization of the receiving and the transmitting of the data along all the networks on the territory of the Russian Federation as well as abroad
9. Automated development, preparation and presentation of suggestions to the management to make decisions

The NEMC consists of the following subdivisions of the EMERCOM:

- NEMC management, operational-analytical centre, emergency response centre, telecommunications centre, space monitoring centre, IT development centre.

NEMC has the following centres in its organizations:

- EMC of the regional centres EMERCOM of Russia, headquarters EMERCOM of Russia in the city of Moscow and the Kaliningrad Region;
- EMC of the headquarters EMERCOM of Russia in the subjects of the Russian Federation.

EMERCOM of Russia conducts immediate management of the work of the NEMC, which means that the senior EMC EMERCOM of Russia coordinates the work of the subordinate EMC and duty dispatch services of its level. NEMC conducts informational interaction with the crisis centres in other countries. With the aim of informational interaction and to provide the work of the headquarters of the FSBI NEMC the following organizations are subordinate to it:

- the EMC of the regional EMERCOM centres of Russia;
- the duty service of the All-Russian Emergency Monitoring and Forecasting Centre ("Antistikhia" EMERCOM of Russia);
- the duty service of the Centre for Situational and Mathematical Modelling of Technogenic Emergencies and Catastrophes of the FSI All-Russian Scientific-Research Institute for Fire Defence;
- the duty of the Centre to provide decision-making for the All-Russian Scientific-Research Institute for Civil Defence and Emergency Relief Problems, EMERCOM and other expert organizations.

The EMERCOM has long been regarded as a relatively efficient authority in the Russian context. This could be partly explained by the high popularity rates the responsible minister Shoigu has received in popularity polls. The ministry has however existed within the framework of a highly corrupt society, not least in the state sector. The widespread fires in Russia during August 2010 have thus clearly showed that there exist a number of grave malfunctions and corruption in the EMERCOM authority and the protection systems it has created.[4]

4) See for example Nezavisimaya Gazeta 5th of August and ITAR Tass 5th of August.

6. The Role of the Russian Civil Defence System

In September 1971 the Ministry of Defence took control of the Soviet civil defence system. However, after the Cold War ended, the civil defence mechanisms were considered to no longer meet the new requirements, among them a modern strategy towards new threats.[5] The Civil Defence Forces also turned out to be unprepared for "normal" large accidents and catastrophes, apart from being the main responsible authority for nuclear accidents and attacks. In 1991, by an Order of the President of the Russian Federation, the Civil Defence Forces were transferred to the Russian ministry for emergency operations, EMERCOM.

The Civil Defence Forces are a state military organization that includes military formations—commands, units and organizations included in the composition of EMERCOM. Today, the Civil Defence Forces are part of the single state system for disaster prevention and relief. They form the foundation of the Ministry's rapid reaction forces and perform special tasks in war- and peacetime.

Their main tasks are emergency rescue work in the zones of large accidents and catastrophes, detection and designation of areas of radioactive, chemical and biological poisoning, as well as special measures to protect people and decontaminate equipment, buildings and territories. In other words, these forces would be responsible for handling the effects of a possible landing or crash on Russian territory in the Aether scenario.

7. The CIS Air Defence System

As the Finnair flight also flies through or close to other CIS countries' territories, these countries' air traffic control may be involved in the Aether scenario. If the flight is considered as a possible danger if believed to be carrying terrorists, the CIS air defence system, much dominated by Russia, may be involved, and is for this reason briefly described below.

The Collective Security Treaty Organization (CSTO) (Russian: Организация Договора о Коллективной Безопасности) or simply the Tashkent Treaty (Russian: Ташкентский договор) first began as the CIS Collective Security Treaty which was signed on 15 May 1992, by Armenia, Kazhakstan, Kyrgyzstan, Russian Federation, Tajikistan and Uzbekistan. Azerbaijan signed the treaty in 1993, Georgia in 1993 (left in 2001) and Belarus in 1993. The treaty came into effect on 20 April 1994. Turkmenistan and Ukraine are not members, but associated.[6]

The Council's agreement to cooperate in air defense generally reflects greater acknowledgement among its members of the importance of the air defense system. Russia still plays a leading role in promoting cooperation both in air defense and celebrations of military and political history.

5) A general background to the role of the Soviet and Russian civil defence system can be found at http://www.fas.org/nuke/guide/russia/agency/cd.htm

6) http://www.globalsecurity.org/military/world/int/csto.htm

Few CIS members can boast an elite air defense system; among them are Russia, Kazakhstan, Azerbaijan and Ukraine, while Armenia, Belarus, Kyrgyzstan, Moldova and Tajikistan have weaker or no air defense. All CIS states with stronger air defense systems strongly depend on Russian supplies of key components. In the Aether scenario, the Kazhakstan air defence system would be the most likely to be concerned.

Throughout the 1990s, the CIS was often considered a paper organization with limited potential for development. In contrast, its military wing the CSTO, has been rapidly developing over the past few years, not least because the Central Asian states have been seeking stronger relations with Russia. [7]

On February 4, 2009, an agreement to create the Collective Rapid Reaction Force (KSOR) (Russian: Коллекти вные си лы операти вного реаги рования (КСОР)) was reached by five of the seven members, with plans finalized on June 14. The force is intended to be used to repulse military aggression, conduct anti-terrorist operations, fight transnational crime and drug trafficking, and neutralize the effects of natural disasters. Belarus and Uzbekistan initially refrained from signing on to the agreement.[8]

The CSTO is probably better known in the Central Asian states than in Russia.[9] The Central Asian mass media cover CSTO military training and summits in greater detail, while the Russian public is perhaps more familiar with the activities of NATO. Some experts claim that for some time the CSTO was the only functioning mechanism within the CIS. Moscow's view is that the CSTO is an eastern equivalent to NATO and has tried to implement that vision through international recognition, an effort that has been met with little interest from NATO, which organization has preferred to negotiate bilaterally with the CSTO member states, as the organization has been regarded as too much dominated by Russia.

8. The Russian Civil Air Traffic Control System

Presently in the Russian Federation air traffic management and air navigation service are provided by the *United Air Traffic Management System (UATM)*, created in 1973, and consisting of civil and military subsystems. Due to distinctions in principles of management, legal and economic bases of UATM subsystems functioning, this system has limitations and significant system drawbacks.

The basis of UATM system´s technical support to a great extent uses physically outdated traditional radio technical systems which have served out their service life for different types of equipment in the range from 56 to 85 per cent. There is no proper automated interaction of all systems participating in air navigation support of flights. These systems are not interconnected by an organisational-functional structure, a fact that prevents their coordinated development. The analysis shows that the existing UATM system, taking into account present air traffic intensity, is capable of supporting *only the average* statistical indicators for safety and efficiency of flights,

7) http://www.globalsecurity.org/military/world/int/csto.htm

8) http://www.rferl.org/content/CSTO_Rapid_Reaction_Exercises_Get_Off_To_Discouraging_Start/1808735.html

9) Krasnaya zvezda, May 6 2003

but it has had no strategic prospects, and in the near future its maintaining as it stands would lead to the degradation of flight safety and efficiency indicators and to a serious lagging behind. [10]

To anticipate the coming situation and to eliminate the above mentioned drawbacks a Federal Target Programme of the Russian UATM system modernisation for the period between 2009 and 2015 has been developed. To achieve the objective of the Federal Programme of UATM system modernisation it would be necessary to solve the following problems:

- To implement an infrastructure of a united airspace search and rescue system and of up-to-date aviation search and rescue complex using Glonass satellite navigation equipment. No implementation has yet been accomplished.
- To implement an integrated military-civil air traffic control systems. No full implementation has yet been accomplished.

The working conditions for Russian air traffic controllers have several times resulted in protests and strikes, recently in May 2010 when controllers covering the Southern Federal District or half of Russia´s European territory went on strike because "deceit, intimidations, blackmail and a totalitarian method of management in regard to dissident workers are ordinary practice in State ATM Corporation," as one official said.[11] It appears that air traffic control and security is not only plagued by traditional turf battles between authorities, but also suffering from old Soviet malpracitises. Corruption in a large number of varieties is a highly present factor in Russia, as president Medvedev himself has repeatedly said, and the air traffic sector is obviously not free from it.

9. The Russian GLONASS System[12]

GLONASS is basically a Russian military positioning system based on satellites. GLONASS was originally started as a Soviet military project in October 1982. Fully developed the system will consist of 24 satellites, of which 3 will make up a reserve. The project has periodically suffered from economic problems, which has resulted in delays, but after an agreement with India, a full financing has been accomplished. The system is expected to be fully operational in 2010.

A GLONASS disadvantage is that controlling segments for the satellites only exist within the territory of the former Soviet Union. This has the effect that it may take up to several hours before a faulty satellite can be detected and attended to. Russia intends to launch a global satellite emergency response system in 2013. The creation of this system, called ERA GLONASS, began in 2009 and should be partly operational at the end of 2012 and reach its full capacity in 2013. The main task is to improve road safety, a serious problem in Russia with a very high death rate.[13]

In order to cover the whole territory of Russia, 12 new GLONASS satellites were due to be

10) (http://www.icao.int/inexses/Presentation/Day2/2c_7_Savitsky_Text_en.pdf). "Future Air Traffic Management System of the Russian Federation"

11) ITAR Tass 6th of May 2010

12) (Russian: ГЛОНАСС; ГЛObальная НАвигационная Спутниковая Система, GLObalnaja NAvigatsionnaja Sputnikovaja Sistema)

13) "Russia to launch global satellite emergency response system in 2013", TASS 9th January 2009

launched before the end of 2010. In order to cover the whole Russian territory, an estimated 18 satellites will be needed.[14] The system can also monitor other modes of transport with hazardous cargoes and this may apply to the Aether scenario, when the system is fully launched. If cargoes of this type will be monitored, it seems probable that civilian planes, even foreign ones, could be included.

10. Cooperation with EU, NATO, IATA and Separate Countries in the Air Security Sector

✓ *10.1 EU*

Against normal international practice, Russia obliges air carriers to pay high sums for the overflight of Russian territory. These overflight payments have created a cost burden of around €300 million per year for EU airlines when flying between Europe and the Far East. Therefore, the European Commission has undertaken significant efforts to reduce these payments. A solution to the Siberian overflight problem is sought in the framework of Russia's accession to WTO.

In order to improve the EU's negotiating position, the Council of Ministers formally authorised the European Commission in March 2006 to negotiate an agreement with Russia on Siberian overflight payments. The negotiations aimed at adopting commonly agreed principles regarding the phasing out of the overflight payments during a transition period and the framework for overflights from 2014 on, including an increase in overflight rights for EU airlines which is vital for their commercial purposes. Following the political pressure, Russia finally agreed to put an end to the current system of overflight payments in 2014.[15]

Under the accord, European airlines will no longer be obliged, from 1 January 2014, to pay royalties to the Russian firm Aeroflot to obtain the right to fly over Siberia, a frequent route for Asian destinations. Present payments were anchored in the obligation for airlines to conclude a commercial agreement with Aeroflot set out in a bilateral agreement between member states and Russia. All royalty payments will be abolished no later than 31 December 2013 and airlines will only have to pay air navigation charges in line with the international convention in force (Chicago Convention). All new frequencies granted, as from the entry into force of the agreement, will be free of surcharges. The new system will be based on transparency and cost-based fees and charges (surcharges collected today do not correspond to payment for any air service).[16]

Russia has a number of bilateral agreements on overflight rights with a number of countries. The Finland - Russian Federation Air Services Agreement was signed in 1993 and seems to be working without major problems. Some bilateral agreements have however encountered problems, e.g. the Austria - Russian Federation Air Services Agreement which was signed in 1993 and in between 1993 and 2009 was complemented by several further accords. The current agreement does not yet conform to the both countries' law and although Austria has tried several times in the past to achieve joint agreements in conformity with the law, Russia has rejected such agreements.

14) Ibid

15) http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/810&guiLanguage=de

16) http://goliath.ecnext.com/coms2/gi_0199-7441379/EU-RUSSIA-AGREEMENT-AT-LAST.html

✓ *10.2 NATO*

The cooperation with NATO has primarily focused on a limited number of questions. In the Aether context counterterrorism, proliferation issues and crisis management stand out as the most pertinent. NATO and Russia have also in 2010 started a testing phase of a joint system for air traffic coordination related to the fight against terrorism. The system will provide a shared radar picture of air traffic and early notification of suspicious air activities. If an aircraft starts behaving erratically, the air traffic coordination system offers increased visibility and transparency to rapidly ensure coordination in the European airspace. The new system has two coordination centres in Warsaw and Moscow and local coordination sites in Kaliningrad, Rostov-on-Don, Murmansk, Warsaw, Bodö and Ankara.

In these countries, training and entry-level exercises are already ongoing. The development of a joint air traffic coordination system is a tangible result of the NATO-Russia Councils Cooperative Airspace Initiative (CAI). Canada, France, Greece, Hungary, Italy, Luxembourg, Norway, Poland, Russia, Turkey, the United Kingdom and the United States, have so far contributed more than Euro 10 million to the CAI project. The CAI system is expected to be operational in 2011 and is open for participation by other nations.[17]

The creation and upstart of the CAI system should be regarded as a victory for Moscow, which repeatedly has tried to interest NATO in cooperation in these fields, but received a very weak response from this organization.[18]

✓ *10.3 IATA*

The International Air Transport Association (IATA) and Russia concluded in 2009 an agreement with the Interstate Aviation Committee (IAC, also known by its Russian abbreviation MAK) to improve aviation safety throughout the Commonwealth of Independent States (CIS).19 The agreement can be said to mark a new phase of closer cooperation between IATA and Russia.

The expanded agreement adds specific points to IATA's existing cooperation partnership with the IAC including:

- Promoting IATA Operational Safety Audits (IOSA), IATA's Integrated-Airline Management System (IAMS), IATA Safety Audits for Ground Operations (ISAGO) and other similar initiatives and their realisation in the deployment of professional resources of IAC.
- Development and enhancement of civil aviation infrastructure in the states united by IAC, including implementation of the ICAO standard for Reduced Vertical Separation Minima (RVSM) and Performance-Based Navigation.

One of the main reasons for the agreement was the safety performance of the CIS which is far below the global average. All IATA airlines - including 15 in the CIS are on the IOSA Registry.

17) KUNA 291803 Apr 10

18) See for example Ivanov (2007ahttp://www.iata.org/pressroom/pr/Pages/2009-04-16-01.aspx) Russian minister of defence Ivanovs speech at NRC informal meeting at www.mil.ru.eng/1866/12078/details/index

19) http://www.iata.org/pressroom/pr/Pages/2009-04-16-01.aspx

Russia and IATA continue their cooperation with emphasis on the following factors:

Improving safety: Alongside working with IAC, IATA is encouraging the Russian government to make IOSA a requirement for all airlines registered in Russia.

Bringing infrastructure charges in line with global standards: Russia has an international obligation to ensure non-discrimination for infrastructure charges. "The current discriminatory system of charges does not comply with international standards and must change, according to IATA.

Bringing transparency to fuel pricing: In 2008 the cost of fuel at Moscow's airports was 12 per cent higher than in Western Europe. Following IATA's call for greater transparency, the gap has narrowed.

Promoting IATA e-freight: After achieving 100% e-ticketing, the next big challenge is to implement e-freight. To make this a reality, Russia must sign the Montreal Convention 99 recognising electronic air way bills.

Finding Global Solutions for the Environment: Russia has made visible progress on making air traffic more efficient. In 2008, a total of 131 routes were optimized. Work on a further 42 routes will take effect by the end of May.

Moving forward with liberalisation: With Russia's carriers active in seeking international partnerships, the archaic ownership limitations of the bilateral system are clearly visible.

11. Earlier experience concerning terrorist-related incidents

Russia has experienced two serious attacks on civil aeroplanes, carried out simultaneously in 2004 by Chechen female terrorists who managed to carry explosives with them when boarding. The two planes both crashed and about 90 passengers and crew were killed.

In March 2006 President Vladimir Putin signed into federal law the bill on Countering Terrorism. The bill authorises the shooting down of hijacked planes *if it appears* (author's italics) that terrorists intend to use them to attack key facilities or populated areas.[20] The bill did not clarify the meaning of `if it appears´, possibly this was also the intention. It seems however futile to speculate further on such a vague definition. The bill was complemented by a decree known as the "Measures to Implement the Federal Law on Countering Terrorism" that was issued on 6 June 2007. The decree regulates the use of weapons and military equipment by the Armed Forces of the Russian Federation to eliminate the threat of terrorist acts committed in the air.[21] Although the decree gave the military the ultimate power to give the order to shoot down civilian planes hijacked by terrorists, it remains unclear what was going to happen if the plane, as in the Aether scenario, is not hijacked by terrorists, but carrying dangerous cargo or a presumed terrorist acting as a human biological bomb on board. The well-known case of shooting down the Korean Air Lines (KAL) flight 007 in 1983 by a Russian fighter aircraft, occurred almost 30 years ago. The precedent may however still apply to the current situation when the rules of

20) For the Federal Law no. 35-FZ of 6 March 2006 on Counteraction Against Terrorism, see http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/apologie__inciter - online in June 2006. See Article 6 and Article 7 in particular; pp. 3-4.

21) For the decree no. 352, see http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/apologie__inciter - online in April 2008; p. 2.

engagement remain as vague as they are.22 In addition, co-operation between various civilian aviation organisations remain weak and there is also lack of rules for internal civilian aviation organisations coordination. As a result, many initiatives to streamline procedures and make business more efficient have been postponed for years.

As to international comparisons, the Russian state-owned company Aeroflot is regarded as one of the airlines which have more than 100 per cent lower security results than the average, mostly depending on the above mentioned two terrorist attacks in 2004. Other regional airlines from former Soviet states, with the exception of the Baltic states, have generally a much worse record and few are allowed to land at European airports (see above chapter 8). Russian airport security has earlier been the responsibility of the airport in question, but has recently been transferred to a central authority.

12. Conclusions

The study shows that Russian handling of air traffic security so far has suffered from outdated technical systems and bad management of air traffic control, even if making a much better performance than other CIS-members. The creation of central and regional centres for emergencies, increased international cooperation, especially with NATO in the CT-field, and a modernisation of the technical standards, including a joint and working civil-military control function may however improve the situation.

In the Aether scenario there still exist a number of uncertainties, which prevent any firm conclusions. Given the present Russian rules, experience and management of air safety in this context, the main conclusion will thus be that we cannot with any certainty say how the Russian authorities will react. It seems however probable that any decisions will be forwarded from regional civil air control to military regional authorities as the military authority supersedes the civilian in these matters and from these to central military air control and the Commander-in-Chief of the Russian Air Forces, who certainly will inform the political leadership. It also seems very likely that the Russian Security Council will be informed and probably convene to discuss the matter. Time is however a critical factor, to what extent depending on when Russian air traffic control receives the report from the plane. Two decisions seem possible: to order the plane to land in order to prevent a crash in populated areas, if the pilots were to be incapacitated, or to let it pass, perhaps along a different route. The pilots' own judgement of the situation and possible request for landing would probably be adhered to, according to international rules. Communication with international relevant authorities will possibly be handled by the national emergency centre, NEMC, but probably also through political channels and perhaps through the new Russia-NATO counterterrorism cooperation function.

22) In support of vague rules of engagement another incident may be mentioned, namely the flight of Mathias Rust from Finland to Moscow in late May 1987. The Soviet fighters never received permission to shoot him down, in part because Rust flew at a low altitude and, as a result, his aircraft was not detected by the Soviet Air-Defence Forces. In addition, since Rust flew on the route from Finland to Moscow, via one of the most densely populated urban areas, the Russian military were reluctant to shoot his plane and, as a result, paid dearly for the consequences. After that unfortunate incident number of top military officials were demoted and left the service in disgrace. What is evident is that commanders of the former Soviet Air Force learned a great deal from the Mathias Rust landing near Red Square in Moscow in 1987.

Daniele Del Bianco & Marina Andeva: Compliance of the Italian Civil Aviation System within the EU Guidelines

ABSTRACT: "To what extent and how does the Italian civil aviation system comply with the European Union guidelines on security?" Bearing this research question in mind, the paper discusses the state-of-the-art of the Italian context of civil aviation security within the larger EU regulatory framework and its recent discussions for revision and modification. Relevant legislative tools and consequent organisational structures of national civil aviation systems are analysed starting from the milestones developed by the international community and the EU on security in aviation systems. The recent development of the EU security regulatory framework is explained with insights and measures to be introduced. Within this context the Italian national aviation system is analysed both in terms of organisational and operative structures. More in details, the paper develops the following issues: the Italian legislation with reference to the EU guidelines, a brief overview of the National Security Programme, the organisational structure of the relevant stakeholders/authorities and an analysis of the criticalities in the Italian civil aviation system. As a conclusion, the paper analyses the effective compliance of the Italian Civil Aviation System with the EU guidelines. The analysis is carried out by comparing the EU and Italian civil aviation system graphic models thus bringing forward a reference model for the self-assessment of the Member States' effective Compliance with the EU guidelines.

1. Introduction

Airline travel is one of the safest modes of public transportation in the world. Airports are expanding and growing to unprecedented levels due to more affordable airfares and increasing public acceptance of air travel. Moreover, we are witnessing the evolution of airports into *aerotropolis* (Kasarda 2005, Del Bianco 2007). Airports have, in fact, developed into complex urban systems complete with banks, hotels, gas stations, car rental agencies, leisure services providers, etc. and are located at the virtual centre of an interconnected industry-service-infrastructure system. Moreover, within the enlarged European Union political context, airports often represent the only (standing) administrative border of the Member States (in the Schengen Treaty area). The evolution of airline travel and of airports, paralleled to the EU enlargement process, have made airports most sensitive targets witnessing a rise of common criminal activities (airline ticket fraud, narcotic smuggling, distraction theft, etc) and international terrorist threats. Moreover, the high concentration of people on large airliners, the potential high lethality rate of attacks on aircrafts, and the ability to use a hijacked airplane as a lethal weapon provide an alluring target for terrorism.

Such issues are trans-national in nature and cannot be tackled autonomously at the national level. The international community and the EU have continuously developed and adapted regulatory frameworks disciplining the security of national civil aviation systems. This paper is primarily concerned with the application of the EU guidelines on the security of national

civil aviation systems in Member States. More precisely the paper aims at answering the following research question, "To what extent and how do Italy and other selected member states comply with the EU guidelines on civil aviation system security?" [1]

The paper is thus structured in two parts focusing respectively on the EU and Italian (i.e. national) levels. Each part is organized as follows. First part: a brief review of the foundation of the international civil aviation system, the EU regulatory framework is presented. More specifically the following aspects are tackled: 1) the introduction to the EU law; 2) the civil aviation system within the Community law; 3) the civil aviation system as a critical infrastructure; 4) measures to reduce CBRN threats and recent developments on the introduction of new security measures; 5) the guidelines for the civil aviation organisation structure. Second part: the Italian context is explored in terms of: 1) the introduction of the legal framework; 2) the civil aviation security within the Italian law; 3) the organisational structure of the Italian civil aviation system. Finally, the paper sketches a number of conclusive remarks on the criticalities singled out in the research on the Italian civil aviation system with regards to security highlighting some original and replicable best practices and makes a short comparison with the civil aviation systems of other selected EU Member States.

2. From 9/10/1934 To 11/09/2001. The Foundations of the International Civil (Aviation) Security System and Its Recent Developments

The foundations of the international civil aviation security law were laid out in the First World War period, bringing forward a completely new perspective especially regarding to the safe and fast transport of goods and people. Moreover, the experienced war period made it much more evident that the new technological developments and advanced means of transport require specific international awareness. The focus at that time was mainly on the legal establishment and protection of an exclusive sovereignty of the states over the air space and freedom of passage for persons and goods. Most of the legal work relating to the security of international civil aviation was undertaken by the League of Nations or thereafter by the United Nations. The League of Nations, which was impelled to act in response to the increase of international terrorist activities following World War I, made several attempts to deal multilaterally with the problem. Its initial efforts towards multilateral accord were directed towards the establishment of an International Convention for the Prevention and Punishment of Terrorism. In spite of these attempts, governments took concrete actions against terrorism only after a major terrorist attack on 9 October 1934, which resulted in the assassination at Marseilles of King Alexander I of Yugoslavia, during his visit to France, and the murder of the French Foreign Minister, Mr. Louis Barthous, who was officially receiving the King in Marseilles. The Yugoslav Government made a

1) ISIG researchers carried out a preliminary review of literature resources (i.e. International conventions and agreements, EU and Italian legal acts) and conducted a number of in depth interviews with qualified respondents (i.e. safety and security airport managers, air security experts, airport plans developers and police authorities). It should be noted here that, given the matter at hand, specific and detailed information are considered as classified documents to which ISIG researchers could not access. However, to know, for instance, the specific actions taken by the Italian border police in the event of an act of unlawful interference, would have been beyond the scope of the paper. Thus, the analysis of the national civil aviation system, its compliance with the EU guidelines and the discussion with informed agents on the overall organisational and operative aspects were privileged. Finally, the data here presented, extrapolated from the interviews are used only in aggregate form and the names or qualifications of the respondents are not disclosed.

request to the Council of the League of Nations to investigate the incident (McWhinney, 1987).

The first steps to "make arrangements for the immediate establishment of provisional world air routes and services" and "to set up an interim council to collect, record and study data concerning international aviation and to make recommendations for its improvement"[2] were made by the International Civil Aviation Conference organized in response to the invitation from the United States Government in Chicago from 01.11.1944 to 07.12.1944. The main results of this conference were the Convention on International Civil Aviation (later in the text Chicago Convention) and the establishment of International Civil Aviation Organization (ICAO), "endorsing its role at ensuring security and safety of international civil aviation in creating and preserving international civil aviation friendship and understanding among the nations and peoples of the world"[3].

In 1944 no one foresaw security threats as today and the need to address them. When security did arise as a serious issue in the late 1960s, the Chicago Convention was adopted to provide an international framework for addressing acts of *unlawful interference*[4]. In the years since, ICAO has become the world leader in developing aviation security policies and measures at the international level and the enhancement of aviation security worldwide remains a key objective.

New and emerging threats to civil aviation are a constant cause for concern to the aviation community. Grave threats such as those posed by the carriage of dangerous pathogens on board, the use of cyber technology calculated to interfere with air navigation systems, and the misuse of man portable air defence systems are real and have to be addressed with vigour and regularity. The International Civil Aviation Organization has been addressing these threats for some time and since the events of 11 September 2001 continues to do so on a global basis.

Since the events of 11 September 2001 took place, the most critical challenge facing international civil aviation remains to be the compelling need to ensure that the air transport industry remains constantly efficient and its consumer is assured of sustained regular, safe and secure air transport services.

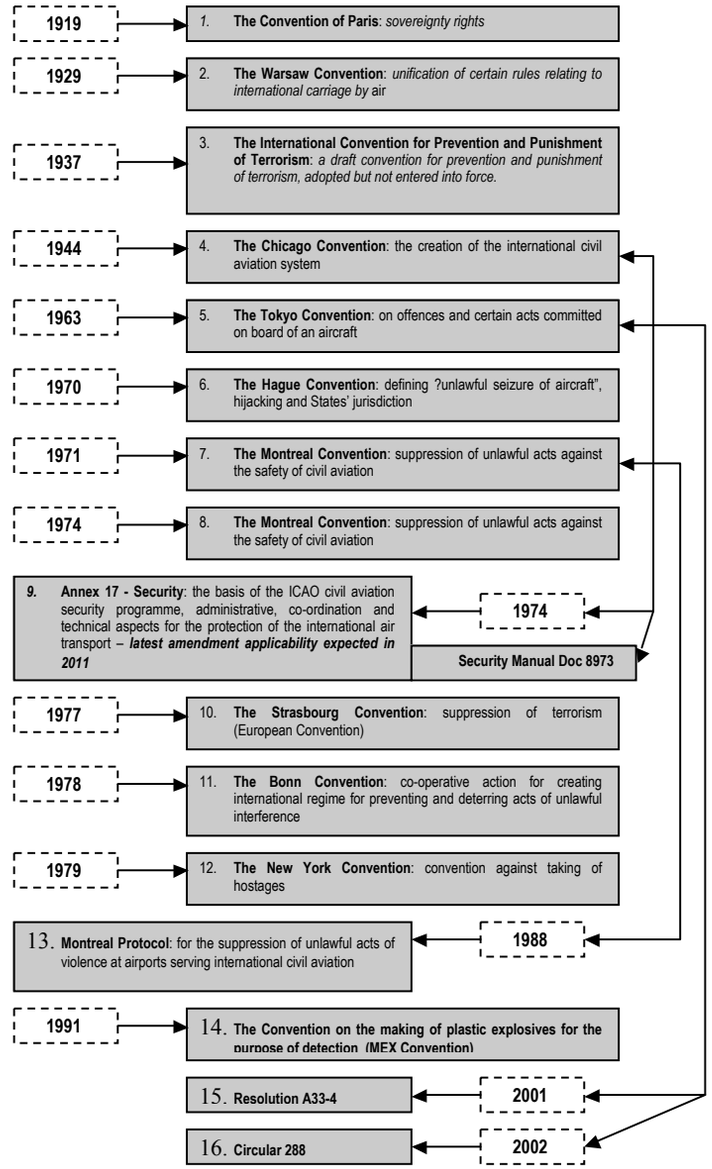
At the 33rd Session of the Assembly, held from 25 September to 5 October 2001, ICAO adopted Resolution A33-1 entitled "Declaration on misuse of civil aircraft as weapons of destruction and other terrorist acts involving civil aviation". This Resolution urged all Contracting States to intensify their efforts in order to achieve the full implementation and enforcement of the multilateral conventions on aviation security, as well as of the ICAO Standards and Recommended Practices and Procedures (SARPs) relating to aviation security, to monitor such implementation, and to take within their territories appropriate additional security measures commensurate to the level of threat in order to prevent and eradicate terrorist acts involving civil aviation. In 2002, a high level ministerial conference on aviation security was held in the Headquarters of ICAO as an instrument for review and development of a global strategy for strengthening aviation security with the aim of protecting lives both in the air and on the ground, restoring public confidence in air travel and promoting the health of air transport in

2) Proceedings of the International Civil Aviation Conference

3) Preamble – Convention on International Civil Aviation

4) In very broad terms it encompasses any act of taking control, damaging or putting safety at risk involving an aircraft or airport.

order that it can renew its vital contribution to the world economy (ICAO, 2002). The High Level Ministerial Conference came to several conclusions and adopted numerous recommendations containing guidance for follow up action (Abeyratne, 2010).[5]



Graph 1 The International Civil Aviation (Security) Legal Framework: main landmarks
Source: Elaboration made by ISIG on the historical developments of the International civil aviation law

5) For detailed outline of the most important international conventions and protocols see Appendix A.

3. Towards Common Security Measures for a Common Sky: The European Union Civil Aviation Security System[6]

Transport is at the forefront of European Union policy concern. The EU air transport in particular and the civil aviation legal system is a combination of common rules concerning the internal market, services and licenses, passengers' rights, air safety, the management of the air transport and single European sky, environmental protection, international civil aviation cooperation and air security as a whole. Within the EU, the aviation security up until recently has been addressed fundamentally on a national level. On the international level, on the other hand, as explained in the previous chapter, the standards and recommended practise have been laid down by ICAO for states to implement without binding force and mechanisms to guarantee their complete and proper application.

Matters of the civil aviation and its security within the European Union are in the competence of the Directorate General for Energy and Transport, the Directorate General for Freedom, Security and Justice and the European Aviation Safety Agency that is a centrepiece of the European Union's strategy for aviation safety.

✓ *3.1. EU Common Rules on Aviation Security*

The EU civil aviation legal system (safety and security) is mainly regulated by the secondary legislation and the "soft law" of the European Union Law[7]. After September 11th aviation security moved up the political agenda in the EU, bringing the aviation security under the EU regulatory framework in order to establish common rules in the field of civil aviation security and harmonizing rules across the Union with binding effect.

3.1.1. Regulation 2320/2002

The EU adopted its first common rules in 2002 with the ***Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules***

6) As defined by the European Union critical infrastructure means an asset, system or art thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. The air transport falls within this definition as a European Critical Infrastructure sector. In order to respond to terrorist attacks involving critical infrastructures, the European Union (the Council) has adopted a Directive (2008/114/EC of 8 December 2008) on the identification and designation of European critical infrastructures and on the need assessment of the protection. Within this directive it is established a procedure for the identification and designation of European critical infrastructures ('ECIs') and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. This directive was the first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection, agreed on after the Commission's Communication on critical infrastructures adopted in 2004, the Green Paper on European programme for critical infrastructure protection in 2005, the Justice and Home Affairs Council call for proposal for a European programme for critical infrastructures protection (EPCIP) and the Council's conclusion on the EPCIP in 2007. For a full account of Critical Infrastructures and the protection at the EU and international level consult Del Bianco ed. (2008), ProAdrias - Protecting the Adriatic Seaways, Gorizia.

7) More on the sources of European Union Law in Appendix B

***in the field of civil aviation security*.** The main objective of this Regulation was to establish and implement appropriate Community measures in order to prevent acts of unlawful interference against civil aviation[8]. In order to realize the objectives, the Regulation clearly stated that the means of achieving them are the common basic standards on aviation security and the appropriate compliance monitoring mechanisms.

The provisions of this Regulation established: 1) a system of *unannounced inspections*[9]; 2) more rigorous *screening of passengers, luggage and staff*; 3) requirement for Member States to introduce *national security programmes* within 3 months following the entry into force of the Regulation, in order to ensure the application of the common standards based on the recommendations of the European Civil Aviation Conference (ECAC)[10] and the standards laid down in the Annex of the Regulation; 4) for coordination and monitoring of the implementation of the national civil aviation security programme, a requirement from Member States to designate a *responsible appropriate authority* that within 6 months following the entry into force of the regulation ensures a development and implementation of a national civil aviation security control programme so as to guarantee the effectiveness of its national civil aviation security programme[11]. The security control programme should be based on best practices and allow for the swift detection and correction of failures, providing as well, that all airports situated in the Member State (further in the text MS) concerned, shall be regularly audited under the responsibility of the appropriate authority assigned[12]. Member States remain free to apply more stringent security measures provided that they are "relevant, objective, non-discriminatory and proportional to the risk that is being addressed"[13].

The common standards referred in this Regulation14 treated the questions of: 1) airport

8) Article 1 (1)

9) In order to ensure that the provisions of the regulation are properly performed, the Commission conducts, in cooperation with the appropriate authority of the Member State, unannounced inspections, including inspections of a suitable sample of airports, taking into account the information obtained from national civil aviation security quality control programmes. The Commission will be assisted by a Committee composed of representatives by Member States and chaired by the representative of the Commission. In this Regulation was also established that the Commission assisted by the Security Committee, considers, together with the ICAO and the ECAC, the possibility to develop a mechanism to assess whether flights coming from third country airports meet the essential security requirements.

10) Founded in 1955 as an intergovernmental organisation, the European Civil Aviation Conference is an organization on European level that seeks to harmonise civil aviation policies and practices among its Member States and, at the same time, promote understanding on policy matters between its Member States and other parts of the world. ECAC's mission is – to promote the continued development of a safe, efficient and sustainable European air transport system. It enjoys active co-operation with its sister organisations through Memoranda of Understanding and with the European Commission, EUROCONTROL, the Joint Aviation Authorities Training Office and the European Aviation Security Training Institute, and works closely and cooperatively with other regional organisations and individual Contracting States of ICAO, including the United States, on a range of civil aviation issues of common interest (training activities in the security, safety and environmental fields).

11) Article 5 (3)

12) More on the Commissions' Inspection determining the Member States level of compliance with the legal provisions on aviation security, see Appendix C

13) Article 6

14) Two years after, this regulation has had a minor amendment with the *Regulation No 849/2004 of the European Parliament and of the Council of 29 April 2004* introducing terminology modifications concerning the monitoring of the implementation of the Regulation.

security; 2) aircraft security; 3) passengers[15]; 3) cabin and hold baggage; 4) cargo, courier and express parcels; 5) mail, air carrier mail and materials; 6) air carrier catering stores and supplies; 7) air carrier cleaning, stores and supplies; 8) staff recruitment and training; 9) guidelines for equipment classification of prohibited articles.

3.1.2. Repealing Regulation 2320/2002

With the ***Regulation No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security***, the Regulation 2320/2002 was repealed[16] because of the "*need to revise it in the light of the experience gained seeking the simplification, harmonization and clarification of the existing rules and the improvement of the levels of security*". The purpose of this new regulation was to establish *revised common rules* to protect civil aviation against acts of unlawful interference that jeopardise the security of the civil aviation and also to provide a basis for a common interpretation of the Chicago Convention. The appliance of this regulation refers to all airports or parts of airports located in the territory of a MS that are not exclusively used for military purposes, to all operators including air carriers providing services at the airports and to all entities applying aviation security standards that operate from premises located inside or outside airports and provide goods and/or services to or through the airports. Here, the aviation security is meant to be "*a combination of measures and human and natural resources intended to safeguard civil aviation against acts of unlawful interference that jeopardise the security of the civil aviation*"[17]. For the first time, this Regulation introduces the term of disruptive passenger[18] and the in-flight officers (known as 'sky marshals')[19]. Each Member State retains the competence to decide whether to deploy in-flight officers on aircraft registered in that MS and on flights of air carriers licensed by it as well as to ensure that such officers are government personnel who are specially selected and trained. Apart from the general measures and the common basic standards[20] set out in this Regulation, it is allowed for a MS to derogate from the common basic standards and to adopt alternative security measures that provide an adequate level of protection on the basis of local risk assessment (i.e. size of the aircraft, nature, scale or frequency of operations, etc).

3.1.3. Supplementing the EU Common Rules on Aviation Security

In spring 2009, the Commission adopted the ***Regulation (EC) No 272/2009*** in order to *supplement the common basic standards on civil aviation security*[21], to respond to the need to

15) More on the body scanners as security measure see Appendix D

16) Article 23 of the Regulation No 300/2008

17) Article 3 (2) Idem

18) Potentially disruptive passenger according to the Regulation 300/2008 is a passenger who is either a deportee, a person deemed to be inadmissible for immigration reasons or a person in lawful custody.

19) Under the Article 3 by definition the in-flight officer is "a person who is employed by a state to travel on an aircraft or an air carrier licensed by it with the purpose of protecting that aircraft and its occupants against acts of unlawful interference that jeopardise the security of the flight".

20) The common basic standards stated in the Annex of the Regulation, threat (as in the Regulation 2320/2002) the questions of the airport security; demarcated areas of airports; aircraft security; passengers and cabin baggage; hold baggage; cargo and mail; air carrier mail and air carrier materials; in-flight supplies; airport supplies; in-flight security measures; staff recruitment and training; and the security equipment.

21) Laid down in the Annex to Regulation (EC) No 300/2008 repealing Regulation (EC) No 2320/2002.

adopt general measures supplementing the common basic standards in the field of screening, access control and other security controls as well as in the field of prohibited articles, third country recognition of equivalence, staff recruitment, training, special security procedures and exemptions from security controls.

In January 2010, the Commission adopted the ***Regulation (EU) No 18/2010*** *amending Regulation (EC) No 300/2008* as far as specifications for *national quality control programmes* in the field of civil aviation security are concerned. In this regulation the Commission is introducing another Annex (Annex II) where new specifications are introduced such as certification[22], security audit[23], and tests[24]. This Annex describes the powers of the appropriate authority, the objectives and content of the national quality control programme, the compliance monitoring, methodology, security audits, inspections, tests, reporting procedures, activities of the auditors and the follow up activities.

Since the adoption of Regulation (EC) 2320/2002, the Commission has continuously worked with MS and industry representatives to develop and - where necessary - revise the legal provisions governing aviation security. 2008 was a period of particularly intense activity during which details were added or amendments made to existing provisions, with the text also being recast in appropriate legal forms, against the background of a fundamental revision of the whole legislative package, building on the experience of the last five years.

3.1.4. Civil Aviation Security Programmes

In order to achieve the objectives set out by the European Union (with the Regulation 2320/2002) to establish and implement the appropriate Community measures in order to prevent acts of unlawful interference against civil aviation, each MS should adopt, apply and maintain a *National Civil Aviation Security Programme*. The programme should ensure the application of the common standards that are referred to: 1) the airport security (airport planning requirements, access control, screening of staff, items carriers and vehicles, physical security and patrols); 2) aircraft security (searching and checking aircraft, protection of aircraft); 3) passengers and cabin baggage (screening of passengers, separation of passengers, screening of cabin baggage, screening of diplomats); 4) hold baggage (reconciliation of hold baggage, screening of hold baggage, protection of hold baggage); 5) cargo, courier and express parcels; 6) mail; 7) air carrier mail and materials; 8) air carrier catering stores and supplies; 9) air carrier cleaning, stores and supplies; 10) security control on general aviation; 11) staff recruitment and training (national aviation security training programme, security staff, other staff)[25]; 12) equipment used in support of aviation security.

22) According to this regulation certification is a formal evaluation and confirmation by or on behalf of the appropriate authority that a person possesses the necessary competencies to perform the functions of an auditor to an acceptable level as defined by the appropriate authority.

23) A security audit is an in-depth examination of security measures and procedures in order to determine if they are being fully implemented on a continual basis.

24) A 'test' is a trial of aviation security measures, where the appropriate authority simulates intent to commit an act of unlawful interference for the purpose of examining the effectiveness of the implementation of existing security measures.

25) In the Annexes of the EU regulations regarding the civil aviation basic security standards are stipulated the guidelines for training and accrediting of the security personnel. More specifically, in the Regulation 2320/2002, there is a part dedicated to the Staff Recruitment and Training (Part 12, Annex to Regulation 2320/2002); more on the criteria for civil aviation security training see Appendix E.

The Regulation 2320/2002, Regulation (EC) No 1217/2003 and the Regulation 300/2008, establish also a *National Quality Control Programme*. The programme should enable a MS to check the quality of civil aviation security in order to monitor compliance both with this Regulation and with its national civil aviation security programme[26].The programme should allow for the swift detection and correction of deficiencies. It should also provide that all airports, operators and entities responsible for the implementation of aviation security standards that are located in the territory of the concerned Member States, should be regularly monitored directly by, or under the supervision of, the appropriate authority.

The Regulation 300/2008 is setting up also *Airport Security Programme, Air Carrier Security Programme* and an *Entity Security Programme*. Every airport operator should draw up, apply and maintain an Airport Security Programme that must describe the methods and procedures to be followed by the airport operator in order to comply with the Regulation and with the National Civil Aviation Security Programme of the MS in which the airport is located. This programme must also include internal quality control provisions describing how compliance with these methods and procedures is to be monitored by the airport operator and must be submitted to the appropriate authority, which may take further action if appropriate.

Every air carrier shall draw up, apply and maintain an Air Carrier Security Programme[27]. The programme should describe the methods and procedures which are to be followed by the air carrier in order to comply both with the Regulation and with the national civil aviation security programme of the MS where the services are provided. It should also include internal quality control provisions describing how compliance with these methods and procedures are monitored by the air carrier. This programme should as well be, upon request, submitted to the appropriate authority which may take further action if appropriate. Where an air carrier security programme has been validated by the appropriate authority of the MS granting the operating licence, the air carrier shall be recognised by all other Member States as having fulfilled the requirements of being in compliance with the Regulation and the national civil aviation security programme (emphasised)[28]. Every entity under the national civil aviation security programme that applies the security standards should draw up, apply and maintain a security programme. The programme should describe the methods and procedures to be followed by the entity in order to comply with the national civil aviation security programme of the MS. It should be drawn, in respect of its operations in that MS, and should, as the previous programmes, include internal quality control provisions describing how compliance with the methods and procedures is to be monitored by the entity itself.

To implement security measures at national level, the Regulation and its amendments find it necessary for each Member State to designate a single appropriate authority responsible for the coordination and the monitoring of the implementation of the aviation security programmes. One or more bodies or entities may be involved in the aviation security and the appropriate authority should be responsible for their coordination. In order to ensure the effectiveness of its national civil aviation security programme, a Member State should provide the appropriate authority with necessary enforcement powers. The officials mandated by the Commission, that shall be assisted by a Committee composed of representatives of the Member States and chaired by the representative of the Commission, are conducting inspections related to the implementation of the measures.

26) Art 11(1), Regulation 300/2008

27) Art 13(1), Regulation 300/2008

28) Art 13(3), Regulation 300/2008

✓ *3.2. EU Implementing Measures on Aviation Security*

The Community law concerning the civil aviation security has two different regulations, ones that lay down the common rules for civil aviation security and others regarding the measures for implementing the common basic standards on civil aviation security. A number of these regulations will be explained in this section.

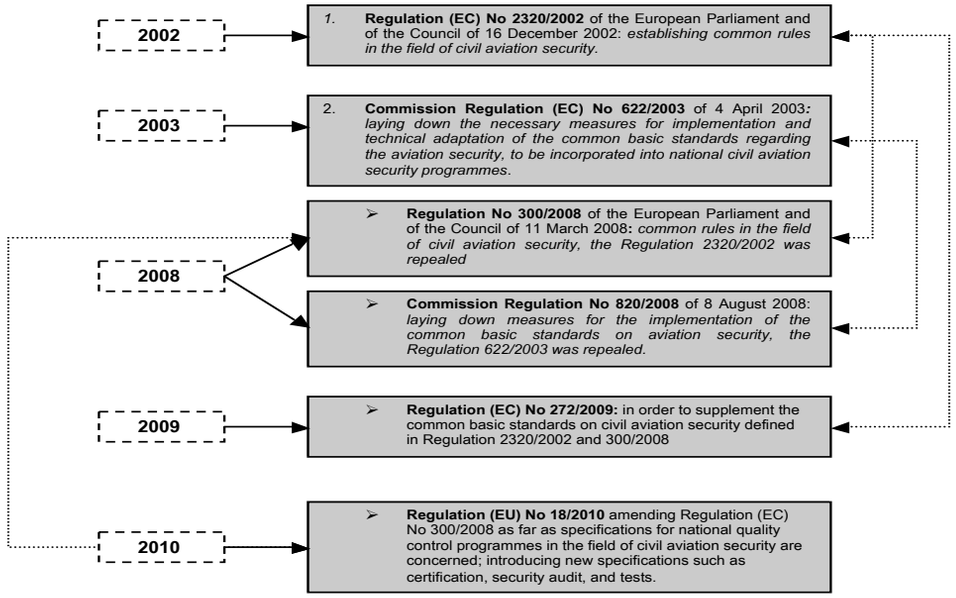
The ***Commission Regulation (EC) No 622/2003 of 4 April 2003*** laid down the necessary measures for implementation and technical adaptation of the *common basic standards regarding the aviation security, to be incorporated into national civil aviation security programmes*. The measures introduced in this Regulation were not officially published in the Official Journal of the European Union due to the fact that according to this Regulation those measures were set out to be secret and confidential and made available only to persons duly authorised by a MS or the Commission.

The detailed measures for aviation security set out in Regulation 622/2003 were amended 14 times[29] until the Regulation was repealed with the ***Commission Regulation No 820/2008 of 8 August 2008 laying down measures for the implementation of the common basic standards on aviation security***. In order to improve the transparency of the implementing measures so far adopted, the Commission has reviewed the secret measures contained in the Regulation 622/2003 as successively amended, in the light of the criteria set out in the Regulation 2320/2002[30]. It decided not to keep the measures as secret and publish them in the Official Journal of the European Union. However, this Regulation states that it remains essential to keep secret certain measures such as certain detailed procedures, concerning: 1) screening of vehicles entering security restricted areas; 2) search of aircraft and of passengers; 3) treatment of disruptive passengers; 4) screening of unaccompanied hold baggage; 5) usage of explosive detection systems and 6) control of cargo and mail, as well as technical specifications for screening equipment. According to this Regulation, these measures should be adopted separately by means of a decision addressed to all Member States. Member States may allow new technical methods or processes, for security controls, in place of those laid down in this Regulation. These methods and processes may be used for the purpose of evaluating a new way of performing the security control concerned and they should not affect negatively the overall level of security being attained. It is obligatory for the Member State to notify the Commission and the other Member States of the proposed new method or process and to receive from the Commission a positive reply[31] in order to introduce them. The measures for implementation and technical adaptation of the common basic standards regarding the aviation security have the same structure as in the Regulation 2320/2002. Whereas no provision has been enacted, the provisions of this regulation are the same as the provisions in the Regulation 2320/2002. There is a description of the types of guns, firearms, weapons, pointed/edged weapons, sharp objects,

29) Some of the amending Regulations were the Commission Regulation No 240/2006 of 10 February 2006 and the Commission Regulation No 831/2006 of 2 June 2006

30) Article 8 Dissemination of information where the measures related to the performance criteria and acceptance tests for equipment, the details procedures containing sensitive information, the detailed criteria for exemption from security measures the specifications regarding the compliance monitoring and the inspections reports shall be secret and not published and only available to the appropriate authorities of the Member States which shall communicate them only to interested parties on a need-to-know basis, in accordance with applicable national rules for dissemination of sensitive information.

31) The Commission's evaluation period is maximum 18 months with the possibility to be extended to maximum 12 months.

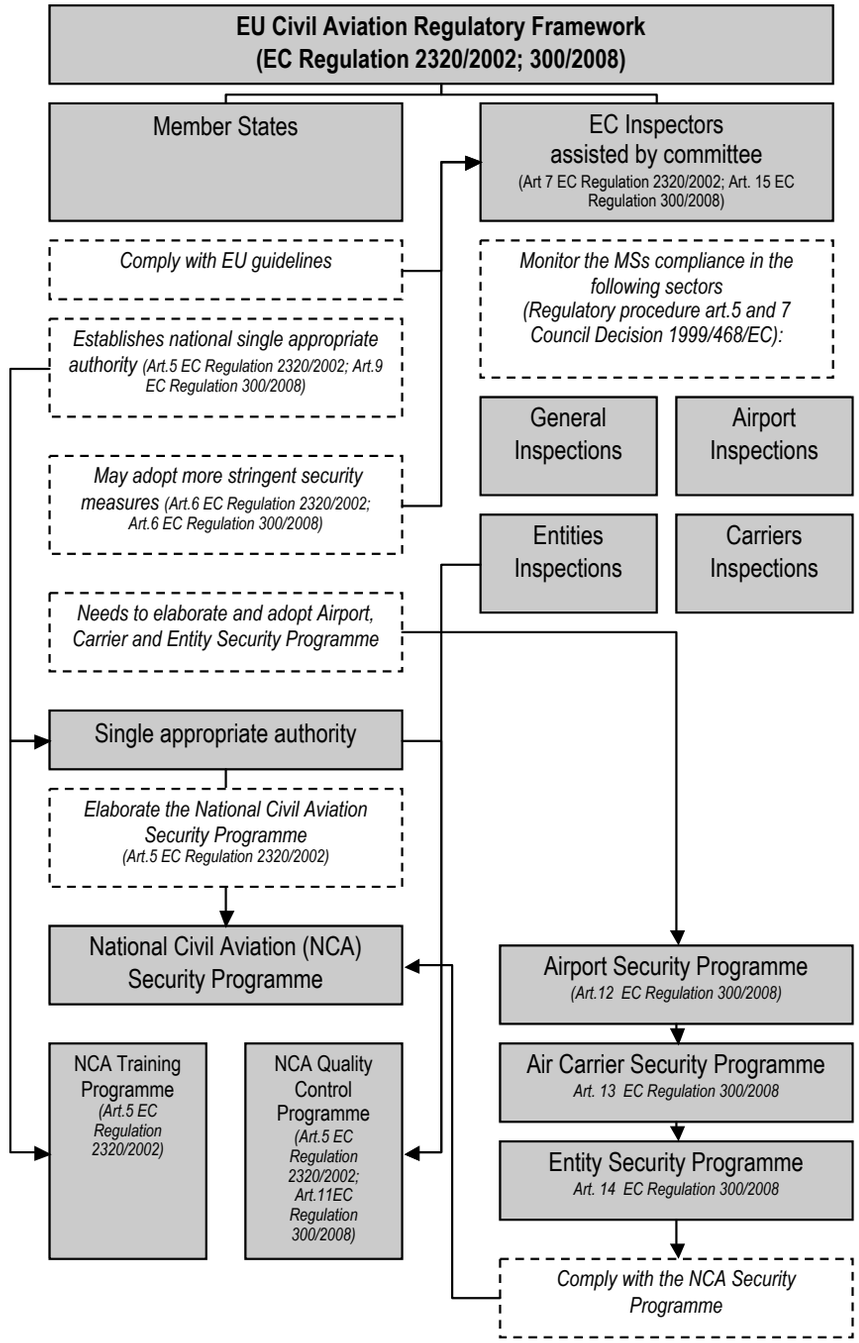


Graph 2 - The European Civil Aviation Security Legal Framework: main landmarks
Source: Elaboration made by ISIG illustrating the main landmarks of the EU regulatory framework on civil aviation security.

blunt instruments, explosives and flammable substances, chemical and toxic substances, that are not permitted to be carried into the security restricted area and in the airplane. This regulation has entered into force after its publication on 19.08.2008.

The harmonisation of aviation security measures at European level has largely facilitated travel by ensuring all EU countries apply the same standards and practices. It serves also as a guarantee for minimum levels of security in all countries. On the other hand, Member States remain free to apply more stringent security measures provided that they are relevant, objective, non-discriminatory and proportional to the risk that is being addressed. This, in combination with a general increase in security threats, has led to the adoption of a large number of "ad hoc" security measures, both at national and EU level[32].

32) In June 2009 the Commission adopted a package of proposals on CBRN in accordance with the December 2007 Council Conclusions on addressing chemical, biological, radiological and nuclear risks and on bio-preparedness, which invited the Commission to continue its work in the CBRN field and agreed with its intention to propose relevant policy measures in 2009. The overall objectives of the CBRN package are to fight terrorism by complementing relevant measures taken at Member State level, to address gaps and to promote the sharing of information and exchange of best practices between Member States. It should also assist in identifying measures to reduce the terrorist threat in the chemical, biological and radiological/nuclear fields. The core of the package is the EU CBRN Action Plan. The 133 measures included in the EU Action Plan are the result of a long consultation process with experts from national authorities of all EU Member States, EU institutions and agencies, as well as from the private sector and the research community. In line with these recommendations, the Commission proposes a broad approach to CBRN security ranging from prevention and detection to the enhancing preparedness and response capacities. The approach is focused on: ensuring that unauthorised access to CBRN materials of concern is as difficult as possible (prevention), having the capability to detect CBRN materials (detection), being able to efficiently respond to incidents involving CBRN materials and recover from them as quickly as possible (preparedness and response). The measures included in the EU CBRN Action Plan will be implemented predominantly by already existing national, EU and international structures and using a broad variety of tools.



Graph 3 – European Regulative Framework
Source: Elaboration made by ISIG presenting the summary of the EU civil aviation security system.

4. Regulations and Practices Within and Beyond the EU Level: The Italian Civil Aviation Security System

The regulatory framework of the Italian civil aviation system, for the most part, is made by the acts having the force of law and the executive regulations[33].

✓ *4.1. The Aviation Security Legal Framework*

According to the ***Italian Navigation Codex***34 from 1942, the sources of law for the regulation of the sea, internal and air navigation were the Navigation Codex, the ordinary laws and the regulations. Since the text of the Italian Navigation Codex from 1942 was no longer adequate for today's scenario in the air transport and since the new regulations of the European Union came into force, the Codex was amended in 2004 (with the Law No 265 from 09.10.2004 converted in Law from the Decree-Law No 237 from 08.09.2004) applying the Community regulations in the sphere of the urgent intervention in the civil aviation sector. It was also amended in 2005 (the Aeronautical part) by the Decree-Law 96/2005 and addressed the crucial parts of the Italian civil aviation: the sources of law, airports and airport management, the administrative arrangements, the functions of the police, the airlines and airport services and the responsibilities of the stakeholders in the sector. A more comprehensive framework was introduced with regards to the airports and concessions of the total management. The Codex now provides the definition of the principal functions of the airport operator, that has to be properly certified by the single authority; also the responsibilities of the police and the surveillance. In 2006, the Part of the Aeronautical Navigation was again amended by the Decree Legislative 151/2006.

The Italian regulatory framework governing the security aspects of civil aviation is, moreover, composed of the provisions set out in the ***International Conventions*** concerning the question of the aviation security[35]. As stated before, the European Union legal framework in the field of the civil aviation security, especially the Regulation 2320/2002 and its amendments and also the other mentioned regulations, are the basis on which the Italian legal framework and the Italian Security Programme has been updated and harmonized to ensure full adherence with the ***Community law***.

The criminal law (or penal law) is an area of the legal order of one state with a main role to prosecute a person for an act that has been classified as a crime. It deals with crime and legal punishment of criminal offences. Therefore, some elements of the Italian criminal law are treating the questions related to the civil aviation security. In Italy the main complex of legal criminal

33) More on the sources of Italian Law see Appendix F

34) Approved with the Royal Decree (Regio Decreto – R.D.) No 327 from 30 March 1942. In the Italian legislation, the Royal Decree was a legislative act having the force of ordinary law adopted by the Council of Ministers and promulgated by the King during the Kingdom of Italy.

35) The International Conventions briefly explained in the first part of this paper with special attention to the Annex 17 to the Chicago Convention on "The security for the protection of the International Civil Aviation against acts of unlawful interference" and the ECAC Document 30, that contains the "recommendations" aimed at ensuring the implementation of the Annex 17 and ensuring a greater degree of safety in the civil aviation.

norms are constituted by the ***Criminal Codex***[36]. Within the Codex are regulated: 1) the attack for terrorist purposes or subversion[37]; 2) the act of terrorism with deadly weapons or explosives[38]; 3) the act of massacre[39]; 4) the act of shipwreck, drowning or aviation disaster[40]; 5) the attack on the airport security[41]; 6) the collapses of constructions or other malicious disasters[42]; 7) the manufacture or possession of explosive materials[43] and other acts against the public health and security. The terrorist activities and the conduct of terrorism are also regulated in a package of urgent measures adopted in 2005[44].

The Single Text of Laws for Public Security[45] represents a normative body that gives protective norms against human acts causing danger to the public safety and security. This Single Text constructs the public security system and gives guiding principles for the responsible public security authorities in order to protect the public order, the safety of the citizens and their properties' protection.

With the ***Law No. 694*** from 23.12.1974 it is regulated the carrying of weapons on aircraft. The passenger carrying with him weapons or munitions is obliged to inform the competent authorities before entering into the aircraft and provide the authorities with an export licence.

The evolution of the legal framework in the area of airport security was found in the late '90s and was a result of the need to regulate the activities of the airport security in the light of both technical and normative connotations of the private security sector and the adaptation of the provisions (especially Art. 5) of the ***Law No 217*** from 27.02.1992 (converting the Decree Legislative No 9 from 18.01.1992) setting out urgent measures to adapt the police forces and the national corps of firefighters and for the development of infrastructure, facilities and equipment of the police. This Decree Legislative has given the basis of one important transformation process and contextually muted the institutional framework. Article 5 (without affecting the powers and duties of public security and customs authorities, and the powers of police and local bodies of the air navigation authorities) has allowed a concession of the airport control services, for which completion is not required the exercise of public power or the police. It leaves to the Ministry of Transport and Navigation in cooperation with the Ministry of the Interior, the arrangements for custody, requirements for concession, functional characteristics of technical equipment and any other requirement necessary to ensure the smooth operation of airport ac-

36) Established with the R.D. (Royal Decree) No. 1398 from 19.10.1930 and entered into force on 01.07.1931. The latest amendments were introduced by the Decree Law No 8 from 08.02.2007, the Law No 241 from 31.07.2006, the Law No 85 of 24.02.2006, the Law No 102 from 21.02.2006, Decree legislative No 231 from 21.11.2007, the Law No 48 from 18.03.2008, the Decree law No 92 from 23.05.2008 and the Decree Legislative No 11 from 23.02.2009

37) Art. 280

38) Art. 280-bis

39) Art. 422

40) Art. 428

41) Art. 432

42) Art. 434

43) Art. 435

44) Decree Law No 144 from 27.07.2005

45) Testo Unico delle Leggi di Pubblica Sicurezza (TULPS), approved with a Royal Decree on 18.06.1931 and related regulations with the Royal Decree on 06.05.1940

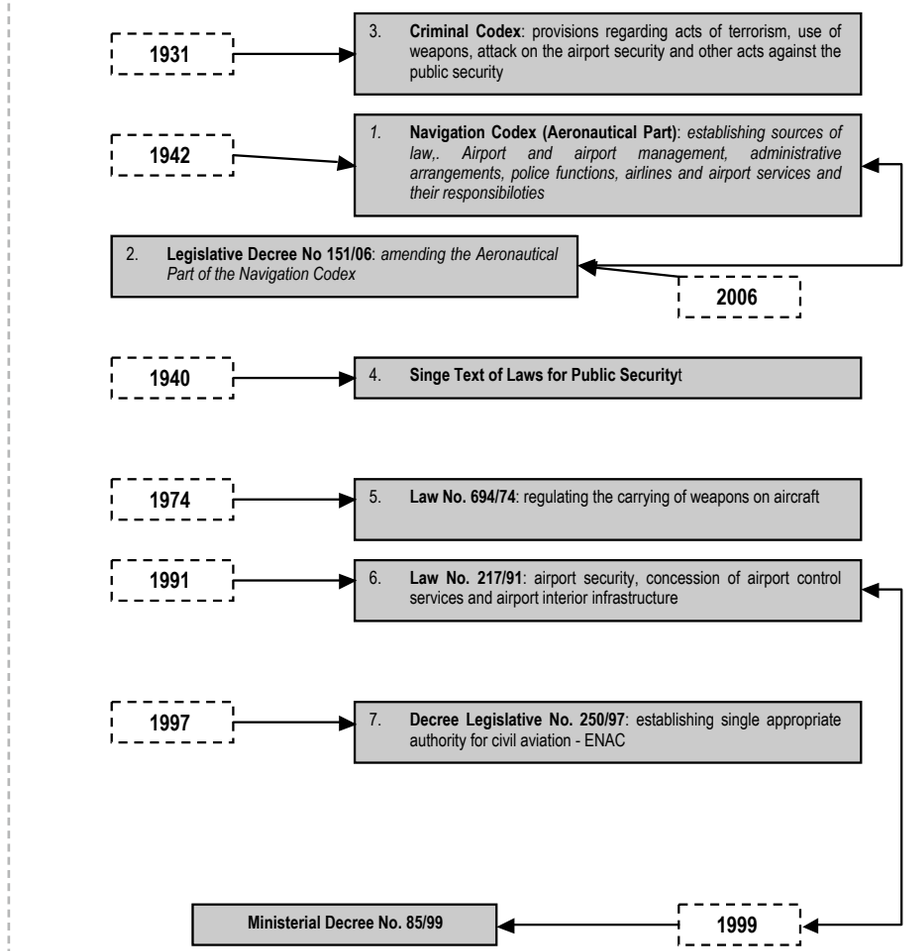
tivities, and the determination of remuneration for cover costs. From that period, the concession of the interior airport infrastructure (management and control services) has been given with special legal acts for maximum of 40 years. With the ***Ministerial Decree No 85*** (from 29.01.1999) were determined the control services under concession, the functional areas, the conditions and the modality of concession, requirements regarding technical equipment etc. In this Decree it was established that the services under concessions can be: the control over passengers in departure and transit, the radioscopic control of other types of control of the accompanied and hold baggage, goods and post.

The provisions of the ***Legislative Decree No 250*** of 25.07.1997, establish a single appropriate authority – National Authority for Civil Aviation (ENAC - Ente Nazionale di Aviazione Civile) responsible for regulating the general aspects of the flight security and safety providing technical set of regulations in the areas of its competence. The ***ENAC Regulations*** contain requirements on technical and operational matters so as to achieve safety standards adequate to the state of art and/or level of efficiency compatible with the national civil aviation system. Generally, in the regulations are decided the requirements and the rules for proper performance of the activities and procedural requirements that must be followed by the user (i.e. certification or other form of recognition) identifying the autonomy, the prerogatives and responsibilities that they are taking on. The ENAC regulations reflect the international standards set out in the Annexes of the Chicago Convention and the provisions laid down in the European Union Directives in the areas where these documents are applicable. In other cases they provide the necessary discipline of matters regulated on national level by laws and decrees. The issuance of the regulations is a complex procedure that normally includes an establishment of expert groups for development, regulatory and legal verification of the compatibility with the existing legal framework, consultation with institutions and concerned industrial associations, analysis of received remarks and opinions of the economic and legal authorities. The Regulations are adopted by a resolution from the Board of Directors of ENAC based on the results of the activities outlined above and submitted to the Minister of Infrastructure and Transport. The adoption of the regulations and amendments are published in the Official Gazette. The regulatory corpus of ENAC is currently composed from Technical Regulations, Administrative Accounting Regulations and Ad-hoc Regulations.

The ***Circulars of ENAC*** are documents that supplement the regulatory framework for the civil aviation and are developed to improve the understanding of the rules by all and to promote the transparency. The content of the circulars provide an interpretative material that addresses; 1) an optimal understanding of the requirements; criteria and procedures acceptable to demonstrate compliance with the standards; 2) procedural aspects of assistance to users for an efficient management of the procedures for approval, certification, licensing, etc. The Circulars may be related to specific topics or conditions that require a specific treatment or are directed to subjects, recipients of set criteria, because they benefit from harmonized standards of the applicable provisions. The Circulars are divided in series[46] that reflect the broad scope of the competence of ENAC. For regulating the security matter ENAC issues the SEC Series devoted to topics related to "security" issues and APT Series[47] concerning airports or any airport security operations including organisational structure in this field.

46) Series dedicated to: Navigation (NAV), Flight Operations (OPV), Airports (APT), Economic, Administrative and Legal matters (EAL), Security (SEC), Licenses (LIC), Air Traffic Management (ATM), General Series (GEN)

47) Airport Series



Graph 4 - The Italian Civil Aviation (Security) Legal Framework: main landmarks
Source: Elaboration made by ISIG presenting the summary of the EU civil aviation security system.

✓ *4.2. The Organizational Aspects of the Civil Aviation Security System*

On central (national) level, the Italian legal framework of the civil aviation security system gives the competences to act to different governmental bodies.

The *Ministry of Interior* has the primary role as the competent national authority responsible for public order and security, and the coordination of police force[s48]. There are five police forces in Italy: State (National) Police (Polizia di Stato), Army Police Force (Arma dei Carabinieri),

48) The present public security organization was introduced with the Law No. 121 of 1981

Financial Police (Guardia di Finanza), Penitentiary Police (Polizia Penitenziaria) and Forest Police (Corpo Forestale dello Stato). The enforcement of public order and security policies is entrusted to the Department of Public Security, headed by the Chief of Police – Director General of Public Security[49].

The *Ministry of Infrastructure and Transport* (according to Art. 42 of the Decree legislative No. 300 from 30.07.1999 and its amendments), is the competent public authority for civil aviation and air transport. For implementing its tasks, the Ministry is organized, at central level, in eighteen Directorate Generals incardinated in two Departments: a) Department for Infrastructure, general affairs and personnel; and b) Department for Transport, navigation, information systems and statistics. The Directorate General for airports and air transport acts under the Department for Transport, navigation, information systems and statistics. The DG regulates the civil aviation sector according to EU regulations and international agreements and among other tasks: addresses, supervises and has control over the institutions of the sector, supervises the aviation safety and airport operations and the quality of the air transport, programmes the airports' systems, evaluates investment plans and consultation regarding the infrastructure construction, analyses the civil aviation market, manages the competition and pricing dynamics, intervenes in the field of civil aviation in support of the mobility, performs tasks related to airspace management tariffs.

With the Ministerial Decree No 2-T from 15.01.1991 the Ministry of Transport introduced the *Interministerial Committee for Security*[50]. The composition and the functions of this Committee were modified with the Ministerial Decree No 107 – T from 02.10.2001 of the Ministry of Infrastructure and Transport transforming it into *Interministerial Committee for security of the air transport and airports*. (Comitato Interministeriale per la Sicurezza dei Trasporti Aerei e degli Aeroporti - C.I.S.A). The Committee is composed by a President (General Director of ENAC or its delegate), Technical Secretariat and Members[51]. The Committee has the responsibilities to: 1) elaborate and update the National Aviation Security Programme (Programma Nazionale di Sicurezza) in order to ensure, within the framework of the international cooperation, the safety of the passengers, crews, airport operators, the public and the airport infrastructure, and also the regularity and efficiency of the civil aviation in occurrence with the act of unlawful interference, 2) examine and study the international provisions related to the security and formulate proposals for their implementation, 3) study and propose concrete initiatives that are not covered by the international norms in order to increase the level of security, 4) study and coordinate the measures and initiatives to be proposed in the field of civil aviation security in order not to penalize, to the extent possible, the advantage of speed that is in transect to the air transport; 5) carry out

49) The Chief of Police is designated by the Minister of Interior and appointed by the President of the Italian Republic, subject to resolution of the Council of Ministers. He/She is assisted by a First Deputy Director-General, a Deputy Director-General responsible for the Co-ordination of Police Forces, and a Deputy Director-General in charge of the Central Criminal Police Directorate. The Department of Public Security coordinates police forces' operations, and manages and organizes the National Police. The Department of Public Security consists of Secretariat, 13 Central Directorates and 4 Offices. Some of them have an interagency status as they are staffed with personnel from the National Police, but also from the Financial Police and the Army Police Force.

50) Comitato Interministeriale per la Sicurezza – C.I.S.

51) The members are: the Presidency of the Council of Ministers, the Ministry of Foreign Affairs, the Ministry of Interior, the General Command of the Financial Police, the Ministry of Communications, the Ministry of Defense, the Customs Agency, the Ministry of Infrastructure and Transport, ENAC, ENAV SpA, the Italian Post, Assaereo, Assaeroporti, Ibar, Assocatering.

coordination activities with the relevant Committees for security of the other States in order to adopt, where possible, common measures for aviation security. For the coordination of activities at local level, this Committee has Offices at airports and Airport Security Committees (CSA).

The *National Authority for Civil Aviation (ENAC)*, according to law[52,] is a public institution with autonomy to regulate non-economic, organizational, administrative, investment, accounting and financial reporting. The Statute of ENAC has been approved by the Ministerial Decree in 1999 by at that time the Ministry of Transport and Navigation. This National Authority is under the supervision and control of the Ministry of Infrastructure and Transport. ENAC headquarters are located in Rome. The management of ENAC is composed by the President, the Board, the Board of Accounting Advisors and the Director General. ENAC is exercising the administrative functions already assigned to the Directorate General for airports and air transport (of the Ministry of Infrastructure and Transport) and in particular the following tasks: 1) preliminary inquiries leading to the entrustment to joint-stock companies of concessions for the total management of airports, 2) dealing with the free access to the market of handling services in national airports, 3) regulating procedures of airport services, 4) examination and assessment of land use projects and intervention programmes, as well as investments and airport development, 5) preliminary evaluation of acts regarding tariffs and airport charges, 6) evaluation of the conditions for warranting the application of state funded fares on certain city airports, 7) certification of personnel operating in the aeronautical/air navigation field, 8) enforcement of recommendations issued by the National Flight Safety Agency, 9) coordination with the National Authority for flight assistance and with the Air Force, 10) relations with organizations, companies and national / international organisations working in the field of the civil aviation and their representative bodies, 11) design and supervision of the quality parameters of the airport services and air transport. As mentioned, the air transport tasks within the institutional mandate of ENAC are various. Its core business is doubtless represented by safety control, in its double meaning of safety and security, according to internationally agreed terms of reference[53]. According to the Italian Navigation Codex[54] (Aeronautical Part) ENAC is the single regulatory authority in the civil aviation. As the single regulatory authority ENAC represents Italy in the major international civil aviation organizations such as ICAO, ECAC, EASA and Eurocontrol - European Organisation for the Safety of Air Navigation. In the air transport security sector ENAC places a major role as the single competent authority to define and coordinate the measures of air transport security and safety and to check the status of the application of these measures. In order to define the security measures and prepare the national security programme ENAC operates through the Interministerial Committee for security of the air transport and airports.

The Navigation Codex introduces also another entity in the Italian civil aviation that is responsible for the navigation services. *ENAV SpA*[55] is a National Entity for Flight Assistance and a public company controlled by the Ministry of Economy and Finance, supervised by the Ministry of Infrastructures and Transport and ENAC. It coordinates its work with the airport management

52) Decree Legislative No 250 from 25.07.1997

53) Safety is understood as the safe planning, construction, maintenance and exploitation of aircraft, as well as the skill assessment of air carriers and in-flight personnel. Security is meant as the land-side safeguard of passengers, on board aircraft, inside and outside the airports, aimed at the prevention of illicit acts.

54) Art. 687 Navigation Codex

55) Ente Nazionale per l'assistenza al volo

with the responsibility to discipline and control, at the airports in its competence, the resources and personnel and ensures the orderly movement of aircraft on the forecourts. It carefully, also, manages and maintains visual installations' support of its property. The organizational head office is in Rome and has operating headquarters throughout the country. ENAV is a component of the international ATM (Air Traffic Management), therefore participates in research and development in coordination with the international sector inspection bodies such as ICAO, EUROCONTROL and category (CANSO).

Another authority in the field of the civil aviation is the *National Agency for Flight Safety* (Agenzia Nazionale per la sicurezza del volo - ANSV). The Agency was established with the Decree Legislative No 66 from 25.02.1999, implementing the provisions of the EU Directive 94/56/EC of 21.11.1994. The same legislative decree also changed the Navigation Codex, in precisely the part relating to the conduct of aircraft accident investigations. This Agency (further in the text ANSV) is a public institution, characterized by broad autonomy, in a neutral position to guarantee the objectivity of their work, as required by Community Directive 94/56/EC[56]. To ensure the position of neutrality, the agency was placed under the supervision of the Presidency of the Council of Ministers. It is therefore the only civil aviation institution that is not subject to the supervision of the Ministry of Transport. This Agency has two main tasks: a) to conduct technical investigations of accidents and incidents involving aircraft of civil aviation, including the adoption, if necessary, the appropriate safety recommendations (the investigation of accidents and incidents involving State aircrafts fall outside of its jurisdiction) and b) to carry out a study and investigation in order to facilitate the improvement of flight safety. It is, therefore, an institution primarily with investigation connotation that has not, unlike other aviation institutions, tasks of regulation, control and management of the civil aviation system.

The multifarious activities that occur in an airport, determine the need to provide, for security reasons, an integrated system of prevention and intervention that is defined as "airport security system".[57] The airport security system is constituted by the activities of the police forces and other administrative authorities and public entities, from the airport management companies, air carriers to the private entities working in the airport security sector. On airport level, the competences of civil aviation management and security are given to the following administrative organs.

The territorial structure of ENAC is organized by three regional areas: North, Central and South, represented by the *ENAC airport offices*. The private actors engaged within the interior of airports that exercise the authoritative powers of jurisdiction, coordination and control of the airport operator are under supervision of ENAC. Without prejudice to the powers of the police, the public actors operating at airports are coordinating among themselves under the supervision of ENAC. It is guaranteed that the ENAC personnel is authorized to carry out inspection[58], to access to means, areas of airports and infrastructure as well as documentation relevant to the activities related to the air navigation. The functions related to the surveillance of the air transport are carried out by ENAC59. ENAC may prohibit flights on specific areas of the country

56) This directive, however, resumed extensively the principles contained in Annex 13 to the Chicago Convention.

57) L.Cola, N.Liotti. (2009). *Sicurezza Aeroportuale.* Sapignoli : p. 43

58) Art. 718 Italian Navigation Codex

59) Art. 792 Idem

for security reasons. When there are military reasons or due to security or public order, ENAC, at a request of a competent authority (the forces of the national police), bans flights over certain areas of the country[60].

The Airport Security Committee (Commitato di sicurezza aeroportuale – C.S.A.) is responsible for coordination and application of the security measures ordered by ENAC and proposed by the Interministerial Committee for Security of the Air transport and Airports. It considers and proposes any action that is taken at an airport, designed to prevent acts of unlawful interference against the civil aviation and develop the airport security programme. This committee (located at every airport) is usually composed of the Director of the airport as chairman coordinating the activities of the Committee itself and the Director of the Border Police, the Director of the Customs Office, the Commander of the Army Force Police, the Commander of the Financial Police, representative from the Airport Management Operator (Società di gestione), and representative of the Association of air carriers operating at the airport. The Committee may be also integrated, where appropriate, from the Director of the Health Authority, the Director of the Post Office, the Commander of the Fire Department, the Director of ENAV and eventually other experts from other organizations and entities. The Committee meets upon an initiative from the Director of the Airport, at least twice a year. In case of urgent matters, the members of the Committee can request extraordinary meetings. The minutes from the Committee's meeting are prepared in a special report to be sent to the Secretariat of the Interministerial Committee for Security.

The Law No 121 (from 01.04.1981) has been an indispensible normative act for regulating the role of *the Prefect (Prefetto) and the Chief of Police (Questore)* as competent authorities (on local airport and provincial level) in the situations where there is a danger for the public security. The Prefect, who represents the government on provincial level, is an authority responsible for general order and public security in the province (NUTS III) and oversees the implementation of the directives issued by the central organs of the Government. Hierarchically he/she is under the Ministry of Interior, however in some cases, under a Ministry competent for dealing the matter. He/She has the direction of operating the necessary emergency situations, in particular those of acts of terrorism connected with the air transport. In order to exercise its competences, it has to be informed, by the Chief of Police and the Director of the Border Police and further by the provincial Commanders of the Army Force Police and the Financial Police, regarding everything that is related to the public security and order. The Prefect may take urgent measures concerning public security, may dispose the law and enforcement authorities and ask if necessary, the exercise of other armed forces. The Chief of Police (Questore), as provincial authority ensuring the public security, has the directions, responsibilities and coordination, on technical-operational level. It is responsible for dealing with the emergency situation deriving from terrorist attacks connected to air transport and any kind of criminal act conducted in the airport area threatening to jeopardize the public security and order. In this sense, the Chief of Police needs to be informed by the Director of the Border Police concerning the issues relevant to the airport security. The technical management of security operations within the airport areas is entrusted to the Executive Office of the Local Border Police which may be assisted by any other office of the police considered necessary[61].

60) The Ministry of Infrastructure and Transport may also prohibit air navigation throughout the national territory, for exceptional reasons of public interest

61) L.Cola, N.Liotti. (2009). *Sicurezza Aeroportuale.* Sapignoli. : p. 49

The State Police, through the Office of the (Air) Border Police[62], *the Army Police Forces* (Carabinieri) and *the Financial Police* (Guardia di Finanza), with their exclusive tasks, are having the institutional competence to guarantee the public order and the public security at an airport. A special group of employees from the local offices of these organs, is daily engaged in the so called Airport Security Apparatus (Dispositivo di Sicurezza Aeroportuale)[63]. The Border Police has three different competences: *preventive*, *repressive* and *institutional*. Within the *preventive* competences (public security), *The Director of the Border Police Zone (Zona di Polizia di Frontiera)*, has the competences to address, coordinate and control all the activities of the local office of the Border Police. It coordinates the activities of the Airport Security Apparatus (Dispositivo di Sicurezza Aeroportuale) in consultation with the appropriate authorities in the Command Units of the Army Police Forces and the Corps of the Financial Police. It needs to be informed by the Director of the Border Police for any kind of criminal acts regarding the airport security. The Director of the Office of the Border Police is responsible for coordinating and managing the "Airport Security Apparatus" and adaptation of the security measures. The Director is a member of the Airport Security Committee. In case of problems in the airport security, it takes over immediately the direct management of the operations needed, and promptly informs the Director of the Border Police Zone and the provincial authority responsible for public security (Prefect and Chief of Police). Within the *repressive* competences (juridical police), the Border Police has the competence to take notice of offenses that are brought to prevent further consequences, looks for the actors, performs all the necessary steps to ensure the sources of evidence and reports to the Judicial Authority. Within the *institutional* competences (border police), it is responsible for the control of the immigration flows at the border, and for supervising and controlling the regularity of the airport security services established by the Ministerial Decree 85/99 and the National Security Programme. The primary competences of the *Army Police Forces (Carabinieri)* are: collaboration with the Border Police regarding the planned activities in the Airport Security Apparatus (prevention), having the same repression competences as the Border Police and acting as a police force with general competence and military order (institutional competences). The local *Financial Police* has also three types of competences: 1) preventive competences regarding the collaboration with the Border Police for the activities planned in the Airport Security Apparatus , 2) repressive competences same as the Border Police and the Army Police Forces and 3) institutional competences as Customs Police in coordination with the Customs Agency (Agenzia delle Dogane), performing checkings of the goods that enter and exit from the borders.

The Director of the Airport coordinates the procedures of the single airport components, so that they can integrate with the activity of the Police in order to guarantee the security of the air transport, through the "power of ordinance" conferred by the Navigation Codex. The Airport Directorate (Direzione Aeroportuale) needs to be informed about every fact that can determine the activation of one of the Levels of protection (Livelli di protezione) of the Airport System. Under those circumstances, he/she has the responsibility to activate and coordinate all technical and logistical support of activities deemed necessary for assistance. While performing the activities regarding security, the Director acts as a consultative body of the Airport Security Committee.

Under the control of ENAC, the *Airport Management Company (Società di gestione)* is another entity that among the many responsibilities, is entitled to administration, management of

62) Known as "Polaria"

63) A joint unit of police force, in charge of preventing events that jeopardize the safety at an airport.

the airport infrastructure, control and monitoring of the activities of the private operators present at the airport or airport system concerned. The right to carry out these activities, in respect of the technical standards of safety, is evidenced by a certification issued by ENAC.[64]

The possibility of transferring the activities performed at the airport regarding the public security to private concessionaires had been planned in 1992, in an urgent legislative measure to adjust the police forces and to rationalize the employment of staff. In 1999, the Ministerial Decree No.85 (29.01.1999) introduced the concept for concession of the control services (inspections), the discipline later completed with the adoption of specific measures to address the ministerial decrees and the determination of compensation for the services and requirements for suitability of the service providers. The procedures of concession are also further explained in the ENAC Circulars[65]. The services in the airport security check points that may be given under concession are: 1) control/screening of passengers on departure and arrival; 2) x-ray control or other types or screening of the passengers' luggage; 3) x-ray or another type of screening of the hold luggage, merchandise and bundles of the express mails. These services are carried out under the supervision of the State Police at the airport and under the supervision of the Director of the Airport. The providers of these services are usually the management airport companies that are carrying out the services directly or through their corporate organizations or entrusting these services to security companies. If the airport management companies are unable to provide the services, the security services are entrusted by ENAC, through competent procedures, to third entities, and they can attend to several airports. Subsequently there has been a rapid evolution of all activities related to security, prompted also by the international political scene and the aggravation of the terrorist threat. Between 2004 and 2005, ENAC completed the designation of the security services to management entities, while initiating a comprehensive inspection program based on the EC Regulation 1217/2003[66], to verify the quality of security at all airports open to commercial traffic.

Other actors such as: ENAV (Ente Nazionale di Assistenza al volo), A.O.C (Airlines Operators Committee), I.B.A.R. (International Board Airlines Representative), ASSAEREO (Associazione Nazionale Vettori e Operatori del trasporto Aereo), ASSAEROPORTI (Associazione dei Gestori aeroportuali), Ente Poste Spa (Post Company), Sanità Marittima ed Aerea (Health department for maritime and air transport), Regulated Agents[67] (Agenti Regolamentati), Volunteers from the Civil Protection Department (Protezone Civile) etc.

✓ *4.3. The Italian Civil Aviation Security Programmes*

4.3.1. National Security Programme

The Italian Civil Aviation Security Programme (further in the text ICASP) is elaborated and updated by the Interministerial Committee for security of air transport and airports, and it is a

64) Art 704 Italian Navigation Codex

65) ENAC Circulars Series Security SEC-02, 07.10.2004

66) This Regulation lays down the common specifications for national civil aviation security quality control programmes.

67) According to Art. 3 of the EC Regulation 300/2008, 'regulated agent' means an air carrier, agent, freight forwarder or any other entity who ensures security controls in respect of cargo or mail.

consequence of the provision established in the EU regulations (approved by the Interministerial Committee for security of air transport and airports on 02.10.2002). It is designed to ensure the safety of passengers, crews, operators, public and airport infrastructure, as well as the regularity and the efficiency of the civil aviation to prevent acts of unlawful interference. This programme represents a normative act with general character with the objective to provide the application of the security measures in entire Italian civil aviation security system. The programme is divided in five parts: 1) Introduction, 2) Air Carriers Security Programme, 3) Airports Security Programme, 4) Quality Control Programme and 5) Security Measures and Controls.

The Security Measures are subdivided into nine sections:

1) *Security checks of passengers and their hand baggage*: carried out by an airport security guard employed by the Airport Management Company or by personnel employed by private security companies. The Airport Security Apparatus is protecting the airport control stations[68] and the proper application of these security measures routinely checked by the State Police personnel;
2) *Security checks of hold baggage*: carried out by the staff of the Airport Management Company; [69]
3) *Security checks of cargo, mail, catering, supplies and materials on board*: carried out by the Regulatory Agents[70] or by the employees of the Airport Management Company;
4) *Security measures for potential exposure to risk and for susceptible flights*: under competence of the Ministry of Interior (Border Police); [71]
5) *Security checks of diplomats, special cases, crew members and airport staff*: these controls are still the most important legislative node since it has not been specified explicitly which authority is responsible for these controls; [72]

68) With the upcoming amendments of the Ministerial Decree 85/99, these responsibilities will be given to the Airport Management Authority.

69) Before the Ministerial Decree 85/99, the controls were carried out by the State Police.

70) The agents (Agenti Regolamentati) have the primary role in this procedure and for carrying out their tasks they are specially certified by ENAC.

71) The application of the security measures in case of susceptible flights is divided in three levels: basic, intermediate and high. The basic level corresponds to a situation where a "normal threat" is present, indicating a danger for the airplane or the airport with a possibility of an unlawful act of terrorist interference, a criminal group, people with mental disorder, suspicious air carrier or third subjects. The intermediate level corresponds to a situation of "intermediate threat" when one particular airport (or few), one particular airplane (or few) are at potential risk caused by an unlawful act of interference. To affront these situations, additional measures are needed to be determined by the Ministry of Interior. The high level corresponds to a situation where an "advanced threat" is present, when one (or few) airport or airplane is object to an unlawful act of interference. In this case, as well, the Ministry of Interior is adopting additional security measures according to the specific risk.

72) Different authorities can be found on various Italian airports (State Police, Financial Police, security guards). It has been predicted (in the amendments of the Ministerial Decree 85/99) the possibility of transferring the responsibility to the Airport Management Company. In this section (while waiting for the new section 10) the rules regarding the airport (identity) card are also agreed. The special cases in this section refer to a situation where there are "unruly" or "disruptive" passengers (terms previously explained) and situations when there is escort of expelled or extradited persons. In these cases the control is under the responsibility of the State Police. To facilitate the security procedure when there are aggressive behaviors by this kind of persons (passengers) the behavior is divided in three levels according to the type of aggressive activities (irritated passenger, passenger that uses threats or acts of disturbance and aggressive acts with use of physical violence).

6) *Security checks of aircraft*: carried out by the so-called "security agent" authorized by the Airport Directorate. This section explains and gives in details the measures taken by the security agent while performing a security check of the aircraft (in and out of service);
7) *Security checks of airport infrastructure*: this section gives basic security measures appropriate to prevent the unlawful or unauthorized access in areas, structures and offices considered and rendered sterile, prevent access of persons with intention or possible intention to do an unlawful act against civil aviation or at least to cause a serious disturbance in the normal air traffic at an airport;[73]
8) *Security measures for general aviation*: aim to prevent unauthorized access in aircrafts of general civil aviation by persons that can potentially do an unlawful act or cause serious disruption in the normal air traffic. By general civil aviation is meant: the air activities of different air transport of persons for example pilot schools, tourism, business activities etc.
9) *Guidelines for the determination of the critical parts of an airport*: established the definition on the critical areas of all Italian airports with more than 40 employees. This section is part of the appliance of the EU Regulation No 1138/2004[74] (establishing definition of critical parts of security restricted areas at an airport).

The measures in every single section of this programme are updated and integrated into the programme according to the EU guidelines and regulations.

4.3.2. Airports' Security Programme

The Airports' Security Programme illustrates the guidelines, to adopt, for coordination of all the subjects present at an airport. Among the most important parameters, it predicts the obligation for periodical simulation exercises, in order to improve the security obligations and tasks. This programme gives an obligation for every airport to clearly establish the following: the normative references of national and local character that discipline the various aspects of airport security, the authorities and other entities present at an airport and describing their competences, the authorities and other entities that constitute the Airport Security Committee, indicating the normative acts and members' qualifications, the intervals when the Committee's reunions are taking place, the physical and infrastructural characteristics of the airport, the security measures and controls, the measures that can guarantee the efficiency of the programme, the airport defence plans in case of acts of unlawful interference and CBRN attacks.

73) This section gives clear provision where the responsible authority to maintain the security measures at the airport to the Airport Management Company. Some areas of the airport, that are considered to be sensitive, can have additional security measures and controls by the Airport Security Apparatus, the Committee for Airport Security and ENAC.

74) Article 1(1): At airports where more than 40 staff members hold airport identification cards giving access to security restricted areas,the critical parts of security restricted areas shall be at least the following: (a) any part of an airport to which departing passengers, including their cabin baggage, after screening, have access; (b) any part of an airport through which, after screening, departing hold baggage may pass or in which it may be held, if the baggage has not been secured.

4.3.3. Leonardo da Vinci Security Plan

The Leonardo da Vinci Plan is a classified document which establishes the general criteria, methods and procedures of the police forces, providing also provisions on how to confront the emergencies and the acts of terrorism. As a document with national character, enthused by the ECAC Doc.30[75], it is issued by the Minister of Interior who, later on, sends it to the Prefects of all Italian provinces. The Prefects send the national document to all police offices at the airports for elaboration, following the criteria and directives of the document itself. Every airport has its own operative plan (Leonardo da Vinci). After the elaboration and editing process, the Prefect signs the document (making it an official document in the province) and transmits it to all competent authorities. The Leonardo da Vinci Plan establishes the prevention, control and repression activities (the emergency procedures), the basic trainings, the constitution of a "Committee for crisis" (for managing the emergency situations) and the Airport Security Apparatus (Dispositivo di Sicurezza Aeroportuale) which performs the primary activities in the airport security system.

4.3.4. Air Carrier Security Programme

The Air Carrier Security Programme (as part of the National Security Programme) establishes: security training of all the personnel, preparations for Air Carriers Security Programme, responsible authority for security on national level and representative in every airport in Italy. In particular, this part of the National Security Programme predicts that every entity (Italian or foreign), having the license for air transport operating on Italian airports, should have a security programme adequate to the provisions established in the National Security Programme and the Leonardo da Vinci Plan. The Programme, signed by the legal representative of the air carrier, needs to be sent to the ENAC Security Directorate for evaluation and acceptance. In case the air carrier security programme is not authorized, the air carrier cannot operate in Italy. It is stipulated in the security programme that the personnel responsible for operating needs to have a security training performed by instructors certified by ENAC. Above all, the programme must indicate the security procedures and measures taken in a single airport regarding: controls of passengers and hang luggage, violent, disabled, inadmissible, deported passengers and passengers in detention, acceptance of packages and hold luggage in areas different from the ones in airports, security measures for hold luggage, reconciliation, security for goods, post, catering, supplies and materials on board, transport of weapons and dangerous goods, sensitive flights, air crafts' security and situations in case of emergency. The air carries must also have quality control programmes containing actions and plans necessary to make certain that the security measures are proper and in accordance with the defined security standards.

4.3.5. Quality Control Programme

In Italy, the quality control of the national civil aviation security is performed by a qualified and trained personnel placed in the figure of "ENAC Inspector". This category of operators is elected by the Ministry of Interior and ENAC. It is constituted by police officials who operate in the national airport sphere and officials from the Airport Directorates analogously involved in the airport operative sector. The security quality controls are made through a test and audit from a National Unit for Inspection (Nucleo Ispettivo Nazionale)[76]. All members of this unit are elected on the basis

75) ECAC Policy Statement in the field of civil aviation facilitation

76) Foreseen in the Ministerial Decree 85/99 and its additional amendments

of the criteria set out in the EC Regulation 1217/2003[77] and certified by ENAC. On local level, the controls are performed by Airport Units for Inspection (Nuclei Ispettivi Aeroportuali) composed of personnel from the ENAC Airport Directorates and personnel from the office of the police.

4.3.6. Manual for Coordinated Procedures

The complexity of the airport activities, performed by all airport components in cases when there is a bomb alarm or emergency alarm determined by an incident, collapse of static structures, explosives, CBRN contaminations or other situations, requires a manual which will establish all the necessary measures to be taken in those situations. In Italy there exist Manuals for coordinated procedure on an airport level. These Manuals have the scope to coordinate the participation of the various actors (each in respect of its competences) in the process of application of the security measures and managing the emergency situations. The Manual predicts the management of every single situation by every single actor involved. In practise there are two identical manuals. One is open for all the actors involved and the other is confidential and is referring to specific responsibilities and actions taken by the police forces (Border Police). For security reasons, the first one is made with omitted clauses (hiding the specific responsibilities and actions of the police forces) and clauses describing the general actions taken by the police forces. This is made in order to facilitate the coordination of the various actors and their activities, and inform them about the situations where the police forces intervene.

✓ *4.4. The Criteria for Emergency Response*

According to the Italian Navigation Codex[78], when there are news of aircraft in distress or fall or other incident or accident, ENAC should immediately provide rescue measures and when it is not possible to procure the necessary measures ENAC must give a notice to other authorities that may intervene. When there is a sign of a detriment for the aviation security, when there are violations of the obligations set down by the police and when it is established that the competent authorities that operate the aircraft and the commander have not fulfilled their obligations set out by the rules regarding public interest in the field of sanitaria and customs, ENAC has the right to prohibit the departure of that specific aircraft[79]. When there is also detriment of the public interest regarding the security of airports, ENAC has the right to prohibit or limit the utilization of those specific airports. The airport management entity gives information to ENAC regarding the variations of the practicability and functionality of the airport facilities that may determine the adoption of the measures of prohibition or limitation of the airport utilization[80].

In a situation when an aircraft has been hijacked, the criteria for response are laid down in the international conventions81 and recommendations. In the Manuals for coordinated procedures are laid down, furthermore, the specific measures to be taken for an immediate response. Every airport, in its security programme, has a Plan for aviation emergency response (in case of technical problems with the aircraft). The criteria laid down in this plan are adjusted for specific

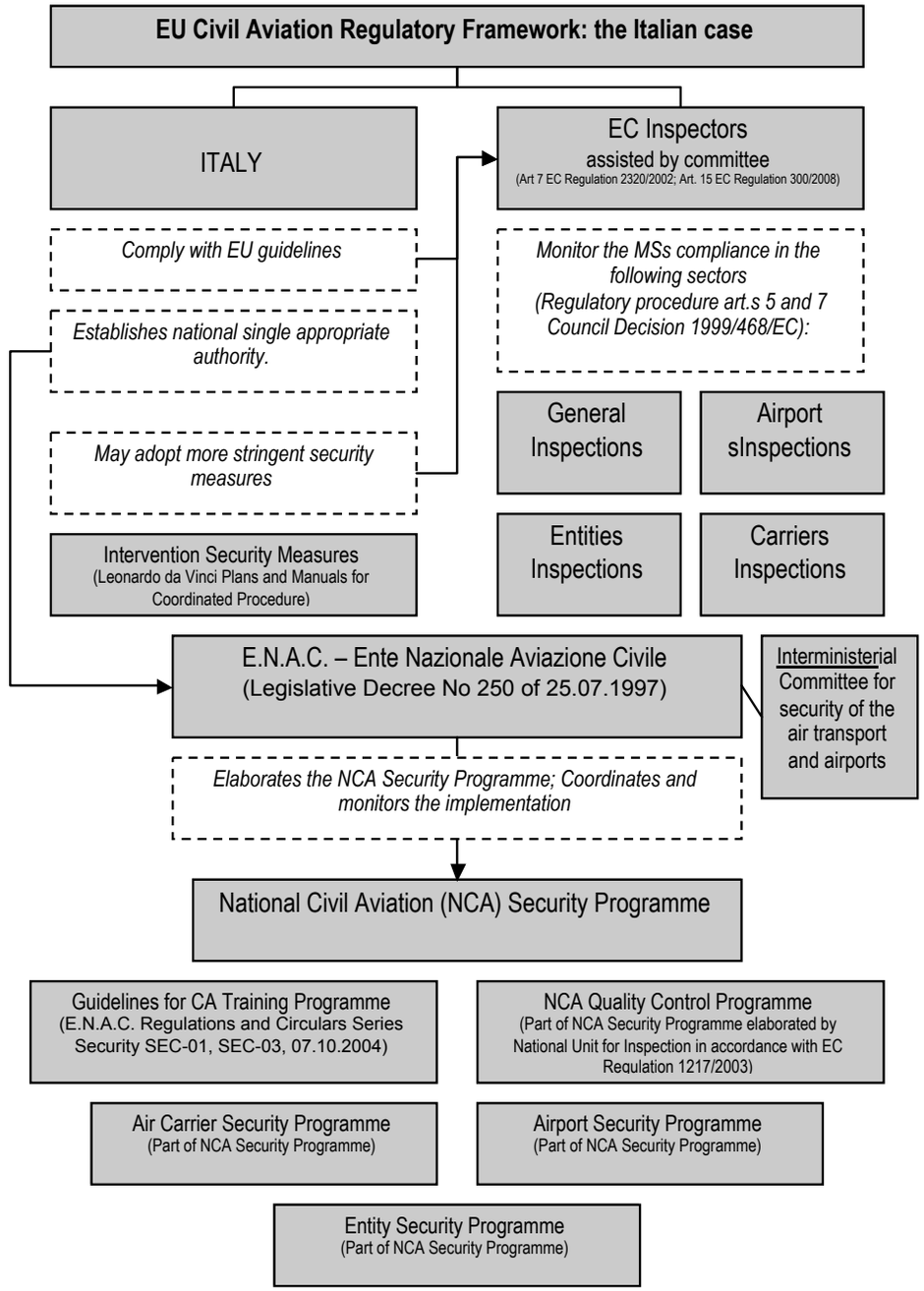
77) This regulation lays down the common specifications for national civil aviation security quality control programme.

78) Art 727

79) Art 802, Italian Navigation Codex

80) Art 806 Idem

81) Tokyo Convention, Aja Convention, Montreal Convention



Graph 5 – EU Civil Aviation Regulatory Framework – the Italian case
Source: Elaborated by ISIG illustrating a summary of the Italian civil aviation regulatory framework.

situations such as the one when there is a hijacked aircraft. In these cases it is taken into consideration the use of the so called "sky marshals"[82]. There are debates about which authorities can perform the tasks of the sky marshals. It has been thought of the special unit of the State Police called NOCS[83] or of the G.I.S. of the Army Police Forces[84].

In case of sabotage, understood as destruction or damage of the aircrafts, installations or airport services, the emergency response is determined by the presence of an explosive device. When it comes to the sabotage of an aircraft, it is presumable that the Captain of the aircraft communicates the Air Traffic Control (ATC). The ATC immediately communicates the Office of the Border Police. The Border Police together with the Airport Directorate evaluate the situation and determine suitable procedures for emergency response according to the Leonardo da Vinci Plan while the Airport Directorate activates all necessary emergency units. When there is a situation of sabotage at an airport, the Director of the Border Police Office gives a general alarm, giving on disposal the first security interventions and evacuations, and agree on, with the Airport Directorate, the eventual limitations of the operations.

In case of a terrorist attack, the Director of the Border Police Office evaluates the situation, declares the state of emergency and determines the procedures to be taken according to the Leonardo da Vinci Plan, while the Airport Directorate activates all the necessary units available. The principle hypothesis in this kind of situation can be summarized in: 1) an attack against parked aircraft, aircraft in movement (taking off or in landing); 2) a direct attack against the airport installation and infrastructure (control tower, radar installations, offices) and 3) attacks against passengers and personnel. The operative measures and procedures for response, relevant for these situations, are regulated in the Leonardo da Vinci Plan and modulated accordingly.

Another type of emergency situation exists in case there is a seizure over an aircraft (seizure of a parked aircraft or a terrorist attack finalized with a seizure over an aircraft). Also in this case, the modalities for operating and the relevant procedures are set out in the Leonardo da Vinci Plan (in a classified section).

When there is an aim to efficiently combat any eventual criminal action at an airport, it is necessary to prearrange specific action of prevention and individualize, contextually, the various actors responsible for the stabilisation of the respected competences. As said before, every airport has an Airport Security Apparatus which, according to precise rules, completes actions with preventive nature.

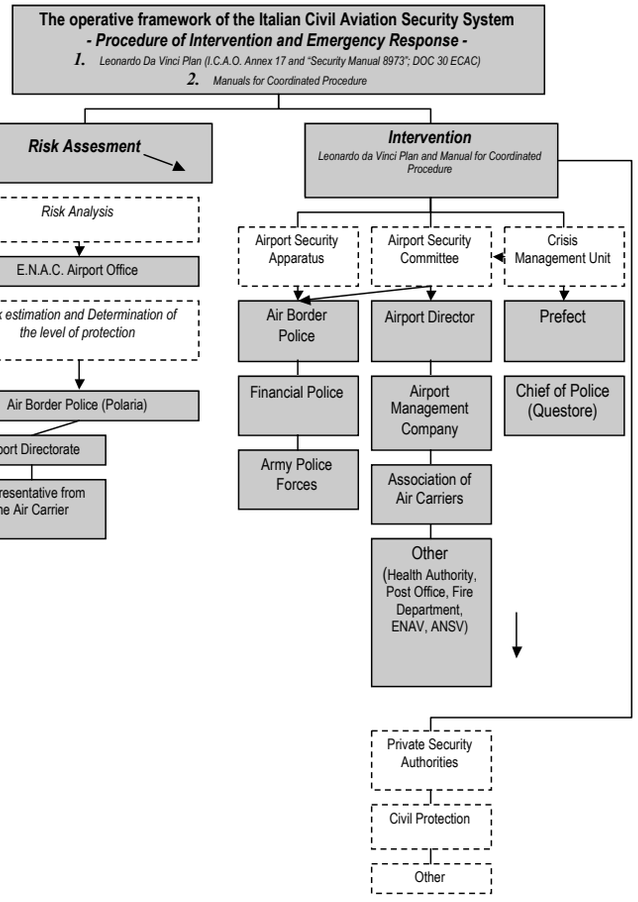
The procedure of intervention (repression), as said before, is carried out by the police forces. The Director of the Border Police Office, at an airport, evaluates the threat together with the Airport Directorate and an air carrier representative (in danger). The Director determines the "levels of protection"[85], formally declared afterwards by the Airport Directorate. The three levels of protection correspond to three different emergency responses (established in details depending on the valuation of the threat). The suitable procedures for response are set out in the Leonardo da Vinci Plan and the Manual for Coordinated Procedures.

82) Introduced in the EC Regulation 300/2008

83) NOCS stands for "Nucleo Operativo centrale di Sicurezza", a central unit for high risks security operations, formed in 1974.

84) G.I.S. stands for "Gruppo Intervento Speciale" of the Army Police Forces (Carabinieri)

85) Green, Yello and Red - established with International conventions



Graph 6 – The operative framework of the Italian civil Aviation Security System
Source: Elaborated by ISIG illustrating a summary of the Procedures of Intervention and Emergency Responses in the Italian Civil Aviation Security System

✓ *4.5. The Criteria for Civil Aviation Security Training*

ENAC as the National Civil Aviation Authority, as mentioned, is the competent authority for the civil aviation security, under the EC Regulation 300/2008, and in this context must, among other responsibilities, establish a National Security Training Program, which is part of National aviation security program under which all staff working in airports or in the civil aviation-related areas should be trained in the issues of the civil aviation.

The guidelines for this training programme are provided in the ENAC Regulation for certification of the security training (as part of the National Aviation Security Programme). This regulation constitutes the core of the training programme, providing a regulatory framework for individuals and organizations engaged. It disciplines the requirements for the certification of the organizations giving security trainings, instructors and security trainers. The appropriate

arrangements regarding the establishment of the technical-professional and structural security firms and professional requirements of the staff at the security checkpoints and any other professionals requiring certification; the establishment and the process of examination and retaining of the certification, are regulated by special ENAC Circulars. The courses must be provided by Schools for security training or Training Centres certified by ENAC possessing the requirements in the ENAC Regulation and ENAC Circulars. Single attendance certifications can be issued not only by schools for security training and training centres but also by enterprises that have limited security training certified by ENAV in possession of security instructors certified by ENAC.

The certification as "Organization for security training" is released by ENAC to specific "educational organizations" (organismi didattici) meeting the expected requirements. The common requirements for certification of the educational organizations are: 1) to have legal head office in the country; 2) adequate human and material resources; 3) teachers certified by ENAC; 4) educational programme and operational manual approved by ENAC. It is also required from them to have the ISO 9001 certificate. The certification released by ENAC has a duration of five years and it is renewable by request. ENAC has the authorization to perform inspections and audit the activities of the organizations performing security training.

The instructors, in order to retain the certification by ENAC, need to pass an exam in front of a Commission composed by representatives of ENAC and the Ministry of Interior Affairs. In order to be entitled for passing the exam, the candidates must possess the following requirements: 1) Italian citizenship or citizenship of one of the European Union Member States; 2) High school diploma or equivalent. The instructors must follow each year a recurrent training according to the modification made in the National Aviation Security Programme. The ENAC certification has a duration of two years and it is renewable upon request following the same procedure of the (previous) release. The certification for "instructor" can be issued to personnel: 1) belonging to a public administration (ENAC, Ministry of Interior and Ministry of infrastructure and transport); 2) belonging to a Society for Airport Management performing and controlling security measures; 3) belonging to an air transport company; 4) belonging to a security firm in the field of civil aviation. Special requirements are requested for each of the previous mentioned personnel[86]. The instructors can be certified for educating one or more of the following personnel categories: 1) airlines personnel, personnel on ground and in flight, including the security directors of the national carriers and their local points; 2) personnel attending to check the passengers and their hand and hold luggage, with or without the use of equipment, including the technical directors and the supervisors; 3) personnel assigned for inspections of goods, mail and catering with or without the use of equipment, including technical directors, supervisors, managers responsible for national security and local delegates; 4) personnel assigned to one or more services under Art. 3 of the Ministerial Decree 85/99[87]; 5) personnel of the airport management companies, handling

86) ENAC Circulars Series Security SEC-01, 07.10.2004

87) a) x-ray screening or other types of screening of equipment and goods, packages of express courier made in sublicensing areas; b) control of catering equipment and aircraft stores in the areas of production and / or development; c) supervision and recognition alongside baggage by the passenger in departure; d) procedures for interview and document checks before passengers' check-in; e) surveillance of parked aircraft and access to control systems on board; f) finding the identity of the passenger and shipping documents at the boarding gates; g) control of the passenger and hand luggage restrictions at the boarding gates; h) stock baggage, cargo, mail, and stores catering to or from aircraft; i) stock from the aircraft weapons as a result of passengers arriving and departure; l) supervision and custody of baggage, cargo and mail; m) preliminary inspection of the aircraft cabin; n) assistance of auxiliary police,

companies, cleaning and other personnel with access to restricted areas. [88]

The airport management companies, carriers and security companies, must provide training for the security personnel organizing specific courses, according to the programs set out by ENAC89. The general training programme deals with: 1) the international and national legislation regarding the civil aviation security; 2) international organizations (ICAO, ECAC); 3) the roles and responsibilities of the national organs in the field of the airport security (Interministerial Committee for Security, Airport Directorate, Border Police, Airport Security Committees); 4) the objectives and organization of national and airport security and the relations with the authorities concerned; 5) professional ethics; 6) different modes of behaviour towards various types of passengers subject to control; 7) access systems and circulation in the airport areas; 8) communication systems; 9) legislation regarding the airport identification cards and permits to access restricted areas; 10) techniques of behaviour and action to be taken in the presence of suspicious persons with unauthorized access as well as in cases of discovery of weapons, explosive devices, suspicious items, dangerous goods, baggage or packages left in the areas of airport weapons; 11) notions on the procedures concerning bomb threats at an airport or on board of an aircraft; 12) description of some cases of hijacking and attacks against civil aviation occurred in the past. Apart from the general training programme, for each of the responsible authorities there are special training programmes, for instance: a training programme for the technical director, a training programme for the personnel with supervision responsibilities, a training programme for the personnel possessing a qualification of a guard under oath that uses security equipment for control of the passengers and hand and hold baggage, a training programme for the personnel responsible for controlling the goods, a training programme for the personnel responsible for controlling the post, a training programme for the personnel responsible for controlling the catering and supplies on board, a training programme for the personnel assigned for security controls that require a possession of a special guard under oath qualification. According to the ENAC regulations the training courses should be organized in modules taking into consideration the specific tasks of the security officers under specific training programme. At the end of each module the personnel should pass a test in order to verify the degree of knowledge of the topics covered in the training modules. The examination consists of an interview and eventual written test with multiple choice responses (having 10 questions), an interview designed to ascertain the level of the knowledge of the English language, a practical test designed to verify the acquaintance with the security equipment (RX[90], PEDS[91], EDS[92], EDDS[93])

related to emergency procedures safety; o) any other check or activities arranged, subject to the direct understanding by the airport authorities for whose completion is not required to exercise in public authority or operational use of members of the police; p) other services under the national security program or required by express carriers and other airport operators.

88

89) ENAC Circulars Series Security SEC-03, 07.10.2004

90) Re-Xray Equipment

91) Primary Explosive Detection System: a system or combination of different technologies which has the ability to detect, and so to indicate by means of an alarm, explosive material contained in baggage, irrespective of the material from which the bag is made. (Annex of the EC Regulation 2320/2002)

92) Explosive Detection System: a system or combination of different technologies which has the ability to detect, and so to indicate by means of an alarm, explosive material contained in baggage, irrespective of the material from which the bag is made. (Annex of the EC Regulation 2320/2002)

93) Explosive Device Detection System: a system or combination of different technologies which has the ability to detect, and so to

in relation to the airport security duties that each employee will be asked to perform. After a successful examination, a certificate as "security officer" is issued and signed by the Director of the Airport District (Circoscrizione Aeroportuale). The certificate is subject to annual renewal that can be made after taking advanced courses offering upgraded knowledge of the matter in concern. The certificates can be revoked when the holder doesn't posses the requirements to perform the authorized tasks, when the holder cannot renew the certificate, for negligence in the performance of the assigned duties and when breaching the requirements imposed by the public security authorities or airport security authorities. The security personnel, apart from carrying their uniform, they have to carry also the issued certificate as "security officer" and, on a clearly visible place, their identification cards.

5. The Effective Compliance of the Italian Civil Aviation System with the EU Guidelines

The paper has unfolded the milestones of the EU and Italian contexts of civil aviation security. Relevant legislative tools and consequent organisational structures were analysed and set within the operative system of Italian civil aviation. The nature and scope of specific documents, such as the Italian National Security Programme – the main reference for the security of the national aviation system – and the so-called Leonardo da Vinci plan – the airport-specific security plan – made them classified texts and thus unavailable. However, a comprehensive description of such documents would have been beyond the scope of the paper the main focus of which was to depict the level of juxtaposition of the Italian s of the national aviation system with the EU guidelines. On the other hand, however, previous research on Critical Infrastructures Protection (Del Bianco, 2008) clearly showed that more often than not implementation praxis substantially differs from operational plans. This consideration has led researchers to carry out a number of interviews with qualified respondents to gather information on the main criticalities linked to the security of the civil aviation system. Given the broader scope of the paper, we limited our research to the potential criticalities at the airport level in general and on the emergency response in particular.

Before tackling these aspects it is useful to rapidly summarise the main characteristics of the framework of the Italian context of civil aviation security.

Fully complying with the EU guidelines, Italy has adopted a National Security Programme which coincides almost entirely with the dispositions set out in the relevant EU legislation. The Programme is designed and implemented by the Ministry of Transport through its competent authority ENAC. The Ministry of Transport together with the Ministry of Interior are the two key actors ensuring, at the national level, the compliance of the Italian civil aviation systems with the EU guidelines in terms of security. The airport managing authority together with and under the supervision of ENAC, is responsible for the implementation of all necessary security measures (especially linked to passengers and goods security checks). The repression of unlawful acts of interference, on the other hand, is dealt exclusively in the so-called Leonardo da Vinci plans, to

indicate by means of an alarm, an explosive device by detecting one or more components of such a device containing in baggage, irrespective of the material from which the bag is made. (Annex of the EC Regulation 2320/2002)

be considered as a complementary and supportive tool to the National Security Plan. They are classified and developed autonomously by the (border) police at the airport level and – once approved by the Ministry – implemented under the exclusive direction of the police in the event of an unlawful act of interference. Finally, these plans are to be considered as part of those additional measures a Member State can adopt to adapt the EU guidelines to the national context (EC Regulation 2320/2002 and EC Regulation 300/2008).

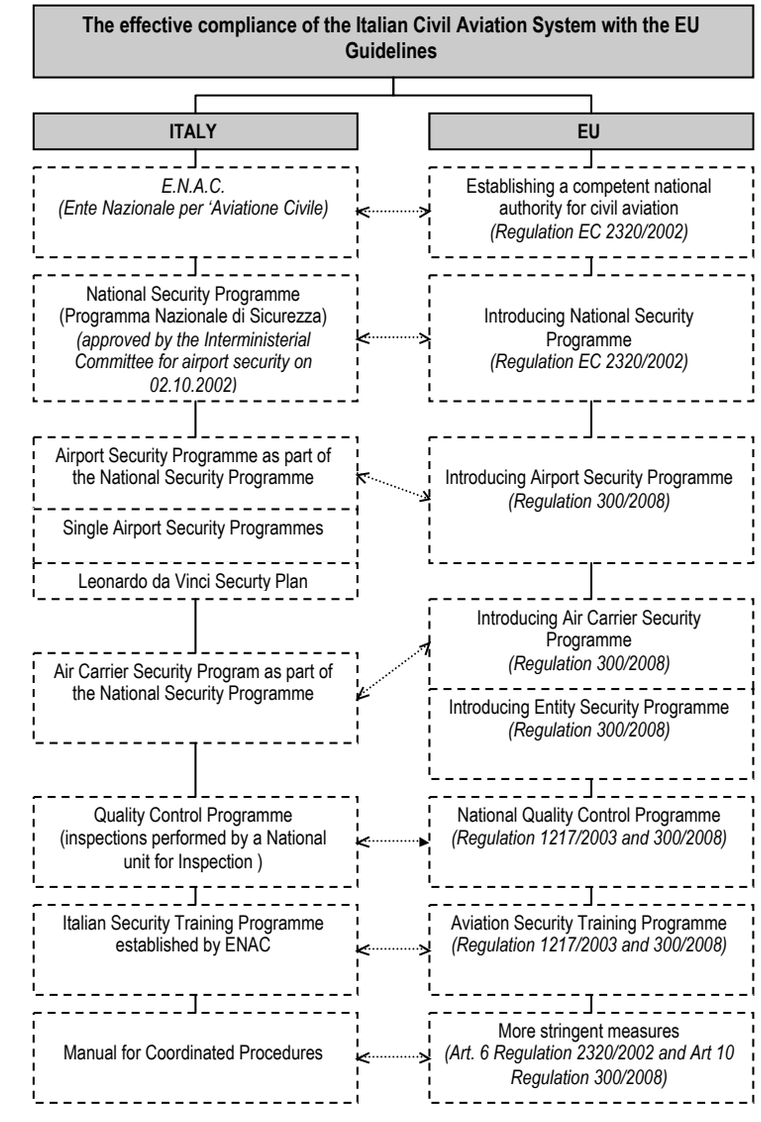
Given the context at hand and the insights gained from the interviews with expert informers, two main levels of criticalities can be identified: *airport financial autonomy in the prevention phase*, *coordination and communication in the repression phase*.

With regards to the first level, the stress derives from the typology of sources of income from which airport managing authorities have to cover security expenditures. Security taxes levied on passengers' tickets are the single most significant source of income. According to the draft regulation which is now under scrutiny of the competent bodies, airport managing authorities will see their competences over airports security increased in the near future. This implies a diminished direct effort of police forces in, for instance, the control of restricted areas or airport access points and an increased resort to private security companies. Within such perspective, smaller airports with less intense fluxes of passengers, will face disproportionably higher fixed costs for security measures. The lack of resources for smaller airports often push airport operators to carry out normal routines which do not necessarily comply with the security measures foreseen in the National Security Programme but are indispensable to guarantee the functioning of the airport. Both trends are interlinked and they could potentially and exponentially jeopardise the security of smaller airports.

The second level represents a type of criticality often highlighted in the analysis of emergency response systems. The coordination of all actors involved in any response to an emergency at the airport level is key to ensure the efficiency and effectiveness of the implemented strategy. Communication among actors is therefore crucial for both preparedness and action. However, the nature of the Leonardo da Vinci plan makes them classified documents which can be accessed only by the border police who directs the operation (and carries out the simulation exercise). In the event of an unlawful act of interference requiring a repressive intervention or in the occurrence of an emergency causing harm to a large number of civilians, actors are likely to be hyperactive preferring to autonomously offer "a helping hand" rather than complying with a given set of procedures. The existing protocols are likely to be overlooked thus causing unnecessary, overlapping activities and setting unbearable stress on the emergency response system. This is even more the case when actors do not have a precise "quick list" manual to which they can refer to but can solely rely on the orders received by the (border) police and on the praxis-led experience accumulated during the exercises. The positive outcome of such criticality lies in the successful elaboration of strategy resolving the trade-off between horizontal communication and the confidentiality of operative plans. The Venice international airport "Marco Polo" represents a so-called best practice with regards to this issue. The operative manual consequent to the Leonardo da Vinci plan elaborated by the (border) police foresees the drafting and circulation among all airport actors of a disclosed mirror operative manual. This contains only the chronological order of the communication system to be applied in the response of an emergency whilst all other activities are not disclosed and are left in *omissis*. This way all actors know when, from whom and what kind of communication they would receive in the event of an

emergency. The plan moreover foresees several meeting points at the airports where all external forces will assembly awaiting for specific orders from the (border) police.

Finally, such type of criticality appears to be culturally and socially determined. A comparative approach to other EU instances is strongly recommended to amend the EU guideline standards with specific recommendations on these issues.



Graph 7 - The effective compliance of the Italian Civil Aviation System with the EU Guideline
Source: Elaborated by ISIG illustrating the effective compliance of the Italian civil aviation system with the EU guidelines.

6. References

Articles and volumes:

- ✓ Abeyratne, R (2010), Aviation Security Law, Springer
- ✓ Del Bianco, D (2008). Critical Infrastructures and the protection at the EU and International level consul, *ProAdrias - Protecting the Adriatic Seaways*, Gorizia
- ✓ Fairhurst, J. (2007). Sources of Community Law. In *Law of the European Union 6th Edition* (p. 54-63). Pearson Longman.
- ✓ ICAO News Release PIO 02/2002
- ✓ L.Cola, N.Liotti. (2009). *Sicurezza Aeroportuale.* Sapignoli
- ✓ McWhinney E (1987) Aerial piracy and International terrorism, the illegal diversion of aicraft and International law, 2nd revised edn. Martinus Nijhoff, Dordrecht

Legal Documents:

- Annex 17 - Security. (1974, March 22). Convention on International Civil Aviation.
- Codice della Navigazione, Parte Seconda della Navigazione Aerea (latest revision Decree Legislative No 96 from 09.05.2005, Official Gazzette n.131 from 08/06/2005)
- Codice Penale R.D. (Royal Decree) No. 1398 19.10.1930 (latest amendment Decree Legislative No 11 from 23.02.2009)
- Convention for the suppression of unlawful acts against the safetu of civil aviation . (1971, September 23). Montreal.
- Convention for the suppression of unlawful seizure of aircraft. (1970, December 16). Hague.
- Convention for the Unification of Certain Rules Relating to International Carriage by Air. (1929, October 12). Warsaw.
- Convention on International Civil Aviation. (1944, December 7). Chicago.
- Convention on offences and certain other acts committed on board aircraft. (1963, September 14). Tokyo.
- Convention Relating to the Regulation of Aerial Navigation. (1919, October 13). Paris.
- Consolidated Versions of the Treaty on European Union and of the Treaty establishing the European Community (2006, December, 29), Official Journal C 321E
- Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security (Text with EEA relevance), Official Journal of the European Union L 089 (2003, April, 5)
- Commission Regulation (EC) No 1217/2003 of 4 July 2003 laying down common specifications for national civil aviation security quality control programmes (Text with EEA relevance), Official Journal L 169 (2003, July, 8) P. 004-0048
- Commission Regulation No 820/2008 of 8 August 2008 laying down measures for the implementation of the common basic standards on aviation security (Text with EEA relevance), Official Journal of the European Union L 221 (2008, August, 19)
- Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to

Regulation (EC) No 300/2008 of the European parliament and of the Council, Official Journal of the European Union L91 (2009, April, 3)

- Commission staff working document accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – *an EU CRBN Action Plan Impact Assesment* {COM(2009) 273 final} {SEC(2009) 791}, Brussels, (2009, June, 24)
- Costituzione della Repubblica Italiana, Ufficio delle informazioni parlamentari dell'archivio e delle pubblicazioni del Senato (Senato della Reppublica) (2003)
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Official Journal of the European Union L 345 (2008, December, 23)
- Decreto 29 gennaio 1999, n. 85 (Official Gazette n. 077 02/04/1999)
- Decreto Legislativo 235 luglio 1997, n.250 "Istituzione dell'Ente nazionale per l'aviazione civile (E.N.A.C.)" (Official Gazette n.117 31/07/1997)
- D.M. 3 giugno 1999 Approvazione dello statuto dell'Ente nazionale per l'aviazione civile (Official Gazette n.289 10/12/1999)
- ECAC Policy Statement in the field of civil aviation facilitation ECAC.CEAC DOC No.30 (Part I) 9th Edition (2003, July)
- ENAC Circolare SERIE SECURITY SEC-01 (2004, October, 7)
- ENAC Circolare SERIE SECURITY SEC-02 (2004, October, 7)
- ENAC Circolare SERIE SECURITY SEC-03 (2004, October, 7)
- ENAC Regolamento in materia di attestato di formazione in material di sicurezza (AFS), Edizione n. 1 approvato con delivera CdA n. 10/2009 (2009, March, 4)
- International Convention against the Taking of Hostages. (1979, December 17). New York.
- Regio Decreto 18 giugno 1931, n. 773 "Testo unico delle Leggi di Pubblica Sicurezza", Official Gazette n. 146 26/06/1931 (last amendments with Decreto Legge 25 giugno 2008, n.112 Official Gazette n. 195 21/08/2008)
- Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (Text with EEA relevance), Official Journal of the European Communities L 355 (2002, December, 30)
- Regulation (EC) No 216/2008 of the European parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (Text with EEA relevance), Official Journal of the European Union L 79 (2008, March, 19)
- Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance), Official Journal of the European Union L 97 (2008, April, 4)

Internet sources:

- *About ECAC*. (n.d.). Retrieved October 5, 2009, from European Civil Aviation Conference: http://www.ecac-ceac.org/index.php?content=presentation&idMenu=1*Aviation Security*. (n.d.). Retrieved October, 2009, from ICAO: http://www2.icao.int/en/avsec/pages/default.aspx/
- NiR. (n.d.), Retrieved October, 2009 from http://www.nir.it/index.htm
- Security. (n.d.) Retrieved October, 2009 from ENAC http://www.enac-italia.it/La_Regolazione_per_la_Sicurezza/Security/index.html
- Report on the Implementation of Resolution A33-4 concerning unruly/disruptive passengers. (n.d.), Retrieved July, 2010 from ICAO http://www.icao.int/ICDB/HTML/English/Representative%20Bodies/Council/Working%20Papers%20by%20Session/169/c.169.wp.12004.en/C.169.WP.12004.EN.HTM

7. Appendices

Appendix A: The International Civil Aviation legal framework – an outline

- ***1919 - The Convention of Paris*** established that each (contracting) State has complete and exclusive sovereignty over the air space above its territory and in time of peace to accord freedom of innocent passage above its territory to the aircraft of the other (contracting) States.
- ***1929*** - ***Warsaw Convention for the Unification of Certain Rules Relating to International Carriage by Air*** (signed on 12.10.1929) established the regulations regarding "the international carriage of persons, luggage or goods performed by aircraft for reward" (Art. 1).
- ***1937 - International Convention for the Prevention and Punishment of Terrorism.*** The Council of the League of Nations set up a Committee of experts on 10 December 1934 to prepare a draft convention for the prevention and punishment of terrorism. The draft was submitted to an international conference in Geneva in November of 1937 and was adopted. Subsequent to approval of this convention, it was unfortunately precluded from entering into force owing to the outbreak of World War II.
- ***1944 - Convention on International Civil Aviation (Chicago Convention)*** established as product of the ***International Civil Aviation Conference*** in Chicago, signed on 07.12.1944 by 52 States. Pending ratification of the Convention by 26 States, the Provisional International Civil Aviation Organization (PICAO) was established. It functioned from 06.06.1945 until 04.04.1947. By 05.03.1947 the 26th ratification was received. The Convention came into force on 04.04.1947 forming the ***International Civil Aviation Organization*** (ICAO) that became a specialized agency of the United Nations linked to Economic and Social Council (ECOSOC). Provisions for international aviation security were first incorporated into the Chicago Convention on 1974, and since then have been improved and updated 11 times. ICAO has also provided States with guidance material to assist the implementation of the security measures. This convention applies only to civil aircraft, to the exclusion of state aircraft.

- ***1963 – The Tokyo Convention.*** Convention on offences and certain other acts committed on board aircraft, signed in Tokyo on 14.09.1963 (in force from 4 December 1969) established provisions regarding offences against penal law and acts which, whether or not are offences, may or do jeopardise the safety of the aircraft, persons, property, goods, order and discipline on board.
- ***1970 - The Hague Convention,*** signed at the Hague on 16.12.1970, in defining the "unlawful seizure of aircraft" refers specifically to the cases of hijacking and provides that each single (contracting) State has the jurisdiction over the offence taking necessary measures to establish its jurisdiction over that offence and any other act of violence against passengers or crew committed by the alleged offender in connection with the offence – Art. 4 (1).
- ***1971 - The Montreal Convention*** (Convention for the suppression of unlawful acts against the safety of civil aviation), signed at Montreal, on 23.09.1971 recognized that every single State should take measures as may be necessary to establish its jurisdiction over the offences in the cases when: 1) the offence is committed in the territory of that State; 2) the offence is committed against or on board an aircraft registered in that State; 3) the aircraft on board which the offence is committed lands in its territory with the alleged offender still on board; 4) the offence is committed against or on board an aircraft leased without crew to a lessee who has his principal place of business or, if the lessee has no such place of business, his permanent residence, in that State - Art. 5 (1). The Protocol to this Convention (***the Montreal Protocol***) supplemented the suppression of unlawful acts of violence at airports serving international civil aviation. Signed at Montreal on 24.02.1988.
- ***1974 – Annex 17 to the Chicago Convention.*** One of the resolutions of the Extraordinary Session of the ICAO Assembly in June 1970, called for specifications in existing of new Annexes to the Chicago Convention to specifically deal with the problem of unlawful interference, in particular with unlawful seizure of aircraft. Following the work of the Air Navigation Commission, the Air Transport Committee, and the Committee on Unlawful Interference, Standards and Recommended Practices on Security were adopted by the Council on 22.03.1974 and designated as *Annex 17 – Security*. This Annex sets out the basis for the ICAO civil aviation security programme and seeks to safeguard civil aviation and its facilities against acts of unlawful interference. Of critical importance to the future of civil aviation, and to the international community at large, are the measures taken by ICAO to prevent and suppress all acts of unlawful interference against civil aviation throughout the world. Annex 17 is primarily concerned with administrative and co-ordination aspects, as well as with technical measures for the protection of the security of international air transport. It requires each Contracting State to establish its own civil aviation security programme with such additional security measures as may be proposed by other appropriate bodies. Annex 17 also seeks to co-ordinate the activities of those involved in security programmes. It is recognized that airline operators themselves have a primary responsibility for protecting their passengers, assets and revenues, and therefore States must ensure that the carriers develop and implement effective complementary security programmes compatible with those of the airports out of which they operate. The Annex is maintained under constant review to ensure that the specifications are current and effective. Because this document sets minimum standards for aviation security worldwide, it is subjected to careful

scrutiny before undergoing any changes, additions or deletions. Since its publication, Annex 17 has been amended several times in response to needs identified by States. ***The latest amendment of Annex 17 is expected to become applicable in 2011***, following formal consultation with Member States with regards to recently updated provisions. The Annex 17 is kept under review by the Aviation Security (AVSEC) Panel, a group of experts appointed by the Council includes representatives from Argentina, Australia, Belgium, Brazil, Canada, Ethiopia, France, Germany, Greece, India, Italy, Japan, Jordan, Mexico, Nigeria, the Russian Federation, Senegal, Spain, Switzerland, the United Kingdom and the United States, as well as international organizations such as the Airports Council International (ACI), the International Air Transport Association (IATA), the International Federation of Airlines Pilots Association (IFALPA) and the International Criminal Police Organization (ICPO-INTERPOL). Currently it is composed by 27 members nominated by States. Together with the ICAO Secretariat, the Panel actively develops ICAO security policy and responses to emerging threats as well as strategies aimed at preventing future acts of unlawful interference. The Panel has met 21 times since its formation, most recently from 22 – 26 March 2010. The Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (Doc 8973 – Restricted) assists Contracting States in implementing the Annex 17 by providing guidance on the application of the Standards and Recommended Practices (SARPs) found in the Annex. The seventh edition of Doc 8973 (2010) is comprised of the following five volumes: 1) Volume I – *National Organization and Administration* is intended for the appropriate authority and provides guidance with regard to the development and implementation of a national legal framework and the oversight responsibilities of a State as they pertain to aviation security. The guidance is related to legal aspects, international cooperation and additional security measures such as the establishment of a *National civil aviation security programme*, management of a *Qualitative control programme*, procedures for handling sensitive information, and the deployment of in-flight security officers and armed personnel: 2) Volume II – *Recruitment, Selection and Training* is intended for any entity responsible for recruiting and training personnel involved in aviation security implementation. It provides guidance with regard to the *national training policy* and *national civil aviation security training programme* including the recruitment, selection, training and certification of security staff, as well as the selection and training of non-security staff and training development; 3) Volume III - *Airport Security, Organization, Programme and Design Requirements* is intended for the airport operator and any entity responsible for the design of airport infrastructure. It provides guidance with regard to organizational requirements, the airport security programme and airport design; 4) Volume IV - *Preventive Security Measures* is intended for all entities responsible for the implementation of an aviation security system. Among other things, it describes security procedures for access control, passengers and cabin baggage, potentially disruptive passengers, hold baggage, cargo and mail, aircraft operators, general aviation and aerial work operations; and 5) Volume V - *Crisis Management and Response to Acts of Unlawful Interference* is intended for the appropriate authority, airport and aircraft operators, and any other entity responsible for crisis management and emergency response. This volume provides guidance with regard to threat and risk assessment, contingency plans, collection and transmission of information during an act of unlawful interference, and the

subsequent review, analysis and reporting of any act of unlawful interference.

- ***1977 - The Strasbourg Convention*** (The European Convention of the suppression of terrorism), signed at Strasbourg on 27.01.1977, treats as political: 1) the offences within the scope of the Hague Convention; 2) the offences with the scope of the Montreal Convention; 3) the serious offences involving an attack against the life, physical integrity or liberty of internationally protected persons, including diplomatic agents, offences involving kidnapping, taking hostages or serious unlawful detention; 4) the offences when a bomb, grenade, rocket, automatic firearm is used; 5) the attempts to commit any of the foregoing offences or participation as an accomplice of a person who commits or attempts to commit such an offence.
- ***1978 - The Bonn Declaration,*** a joint initiative between the Governments of Canada, France, the Federal Republic of Germany, Italy, Japan, the United Kingdom and Northern Ireland, and United States of America, for co-operative action to create an international regime for preventing and deterring acts of unlawful interference by imposition of stringent sanctions. The objective of this declaration was to intensify the joint efforts of States to combat international terrorism. In order to achieve this objective, the declaration has set out respective obligations on a third State in the event where a hijacked aircraft ended in the territory of such State. If the third State failed to meet the obligations the Declaration envisages that a definite sanction will be inflicted upon the State as a sort of punishment. The legal status of this declaration was a question mark since the exclusive jurisdiction of applying sanctions against State in the form of interruption of full or partial air services belongs to the UN Security Council.
- ***1979 - The New York Convention*** (International Convention against the taking of hostages) signed in New York on 17.12.1979 developed the international cooperation between States in devising and adopting effective measures for the prevention, prosecution and punishment of all acts of taking hostage as manifestations of international terrorism.
- ***1988 - Montreal Protocol.*** Signed at Montreal on 24 February 1988, this protocol supplements the Montreal Convention from 1971.
- ***1991 - Convention on the Marking of Plastic Explosives for the Purpose of Detection (MEX Convention).*** Following the resolution of the ICAO of the Council and the adoption of a United Nations General Assembly Resolution, an International Conference on Air Law was held under the auspices of the ICAO in Montreal from 12.02 – 01.03.1991, which unanimously adopted this convention. It was opened for signature on 01.03.1991 and on that day was signed on behalf of 41 States (ICAO Doc 9571). The Convention entered into force on 21 June 1998.
- ***2001 - Resolution A33-4.*** During its 33rd Session held in 2001, the ICAO Assembly adopted Resolution A33-4, urging all Contracting States to enact, so far as practical, the model legislation developed by the Study Group which is set out in the Appendix to the Resolution. This resolution represents a continuation and modernization of the legal aspects established in the Tokyo Convention from 1963. It urges for adoption of national legislation on certain offences committed on board civil aircraft (unruly/disruptive passengers).
- ***2002 - Circular 288:*** ICAO Guidance Material on the Legal Aspects of Unruly/ Disruptive Passengers dated June 2002 to facilitate the implementation of Resolution A33-4, ICAO Circular 288 "Guidance Material on the Legal Aspects of Unruly/ Disruptive Passengers".

Appendix B: Sources of European Union Law

There are seven principal sources of Community law:

1. The Treaties establishing the European Communities and the European Union;
2. Secondary legislation made under the Treaties;
3. 'Soft law' (i.e. non-legally enforceable instruments which may aid the interpretation and/or application of Community law);
4. Related Treaties made between Member States;
5. International Treaties negotiated by the Community under powers conferred on it by the Treaties;
6. Decisions of the European Court of Justice and the Court of First Instance;
7. General principles of law and fundamental rights upon which the constitutional law of Member States are based.

The article 249 EC Treaty94 sets out the different types of secondary legislative acts: "*In order to carry out their task and in accordance with the provisions of this Treaty, the European Parliament acting jointly with the Council, the Council and the Commission, shall make regulations, issue directives, take decisions, make recommendations or deliver opinions.*" The consequences of the legislative act depend upon its specific nature.

A *regulation* has a general application and it is binding in its entirety and directly applicable in Member States. The regulations shall be taken to have been incorporated into national legal system of each of Member States automatically, and come into force in accordance with the EC Treaty provisions. They are binding on anyone falling within their terms in all Member States. They require no further action by Member States, and can be applied by the courts of the Member States as soon as they become operative.

A *directive* differs from a regulation in that it applies only to those Member States to whom it is addressed, although normally a directive will be addressed to all 27 Member States. A directive sets out the result to be achieved, but leaves some choice to each Member State as to the form and the method of achieving the end result. A directive will quite often provide the Member State with a range of options it can choose from when implementing the measure. It is not directly applicable and it requires each Member State to incorporate the directive in order for it to become effective in the national legal system.

A *decision* is binding in its entirety on those to whom it is addressed. It must be notified to the person or Member State to whom it is addressed and it will take immediate effect upon such notification. If a decision is adopted using the legislative procedure (i.e. co-decision procedure), then it must be published in the Official Journal and it will take effect either on the date specified or, if there is no such date, on the twentieth day following its publication.

Non-legally enforceable instruments which may facilitate the interpretation and/or application of Community law are referred as *'soft law'*. Two particular forms of 'soft law' are the *recommendations* and the *opinions* and neither of them have a binding force. Although they

94) Consolidated Version of the Treaty on European Union and of the Treaty establishing the European Community (2006)

do not have a binding force, the use of these instruments may be useful to clarify matters in a formal way. They may achieve some legal effect as persuasive authority if they are subsequently referred to, and taken notice of, in a decision of the Court of Justice and the Court of First Instance. National courts are bound to take them into account when interpreting Community measures. The EC Treaty empowers the Commission to formulate recommendations and to deliver opinions on matters dealt with in the Treaty, not only where expressly provided for, but also whenever it considers it necessary (Fairhurst, 2007).

Appendix C: Commissions' Inspections determining the Member States' level of compliance with the legal provisions on aviation security

Under Regulation 2320/2002, the Commission is required to carry out inspections to determine Member States' level of compliance with the legal provisions on aviation security.

There are three types of inspections:
1) national appropriate authority;
2) airport; and
3) follow-up, to assess deficiency correction activities

These are carried out by the Commission's team of 11 aviation security inspectors, working with national inspectors nominated by Member States.

Each Member State is required to designate an appropriate authority to be responsible for coordinating and monitoring its national civil aviation security programme. The Commission inspected 9 appropriate authorities during 2008. These inspections involve an evaluation of the national civil aviation security programme, the national civil aviation security quality control programme and its implementation, the national training programme and airport and airline security programmes.

As for 200895, were demonstrated high standards in 5 and reasonable standards in 2 states; but the remaining 2 reports were unsatisfactory. National civil aviation security programmes generally covered the legal requirements well, despite a few omissions and outdated references. Provisions for small airports for which an exemption had been claimed under the terms of the Regulation were fairly frequently omitted from national civil aviation security programmes, along with some requirements for air cargo. Frequencies for monitoring activities and provision for security audits within the EU definition of the term96 were often missing from national quality control programmes. A number of national security training programmes failed to include adequate provisions for general awareness and recurrent training. Most deficiencies, however, were found in respect of the capacity to detect and correct failures swiftly. Common failing, even in sole of the best performing Member States, were lack of security audits, few tests and poor follow up. Much more seriously, but also more rarely, inspectors found airports not visited at all during long periods, brief and infrequent inspections or seriously delayed rectification action.

95) Fourth Report on the Implementation of Regulation (EC) No 2320/2002 establishing common rules in the field of civil aviation security, COM (2009) 518 final, Brussels, 08.10.2009

96) 'Auditor' means any person conducting national compliance monitoring activities on behalf of the appropriate authority.

During 2008, 10 initial inspections of airports were conducted, and the findings were by and large consistent with those from earlier inspections. Results in the four areas generally considered as the most crucial for maintaining the security of civil aviation (airport security, aircraft security, passengers and cabin baggage and hold baggage) indicated some improvement, even if this is not entirely empirically based. The weakest areas at the 10 airports inspected during 2008 related to access control and staff screening, overall, air carriers' standards of compliance were less robust than those of airports, although there was a great overall improvement between 2007 and 2008. The areas needing most additional effort were search and check of aircraft and aircraft protection.

Compliance with the provision covering passengers and cabin baggage was mostly high although serious deficiencies stemming from human factors were reported at some of the inspected airports. Compliance in the area of hold baggage screening was extremely high, with no deficiencies at all recorded against a good number of the provisions.

Appendix D: The security measures a propos the screening of passengers

The screening of passengers has been regulated with the EC Regulation 2320/2002 and successive amending regulations. In the Regulation 2320/2002 (and amending/repealing regulations) all departing passengers were to be controlled, to prevent prohibited articles from being introduced into the aircraft, by the following way: 1) searched by hand; 2) screened by walk-through-metal-detection (WTMD) equipment. The Regulation 272/2009 has introduced new methods of screening together with the hand search and WTMD equipment, having five methods for controlling the passengers before entering the aircraft 1) hand search: 2) WTMD equipment; 3) hand-held metal detection (HHMD) equipment; 4) explosive detection dogs and 5) explosive trace detection (ETD) equipment. However before the adoption of the new methods of screening, a debate[97] has been raised (as a consequence of the Motion for a Resolution submitted on the 20th October 2008) in concern of the use of the body scanners as from 2010, as one of the methods of screening the passengers and revising the security measures' implementations. Having regard the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the Charter of Fundamental Rights of the European Union, Article 6 of the EU Treaty, Article 80 (2) of the EC Treaty, and Regulation (EC) No 300/2008, the draft Commission's regulation supplementing the common basic standards on civil aviation security, which includes, among the permitted methods of screening of passenger, 'body scanners', the European Parliament adopted a resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection. In the parliament resolution it has been noted that the body scanners are machines producing scanned images of persons as if they were naked, equivalent to a virtual strop search, whereas may be one of the technical solutions required to keep a high level of security while a European framework is essential to guarantee the rights of passengers in the event of body scanners being used and to prevent every airport from applying different regulations. It has been also noted that this measure has a serious impact on the right of privacy, the right of data protection and the right of personal dignity, and therefore needs to be accompanied by strong and adequate safeguards. Since the justification of this measure has raised doubts, the European Parliament gave instructions to forward the

97) Taking place in Strasbourg on Tuesday, 21 October 2008 (see European Parliament document O-0107/2008 (B6-0478/2008) PV 21/10/2008 – 18)

resolution to the Council, the Commission and the governments and parliaments of the Member States in order to carry out an impact assessment relating to fundamental rights, scientific and medical assessment of the possible health impact and economic, commercial and cost-benefit impact assessment, consulting primarily the Fundamental Rights Agency and the European Data Protection Supervisor (EDPS).

In response to the attempt to blow up the US airplane on Christmas Day in Detroit, the European Union revisited to the old dilemma regarding the use of the body scanners as one of the methods of screening the passengers. At the beginning of 2010 the European Commission hosted aviation experts on body scanners, certain that the body scanners can play a very useful role as a complementary means of screening. At this point, the Members States are free to use body scanners, provided the security checks do not contradict national or EU legislation. Although the European Commission could theoretically propose European Union-wide legislation on body scanners, it preferred a more cautious approach. "The Commission has said it could reconsider the issue of body scanners when all concerns on privacy and human health have been addressed and the relevant technology is in place."[98]

The Netherlands and United Kingdom introduced the body scanners for US-bound flights. But few countries appeared to follow the example. Italy, Spain and Germany both ruled out the immediate use of the scanners that privacy campaigners claim can 'digitally undress' passengers and which others fear could expose people to higher levels of radiation and airport delays. France has not ruled out introducing body scanners, searching for other ways to detect traces of explosives. The Dutch government immediately began using full body scanners on flights to the United States in order to avoid such incidents as the one on Christmas Day. In Italy, full body scanners are planning to be installed at Rome's Leonardo da Vinci airport, Milan's Malpensa airport and possibly in Venice. Up till now, the EU has allowed member states to decide on whether to use body scanners at airport checkpoints.

Appendix E: Criteria for Civil Aviation Security Training

Initially, the appropriate authority of the Member State should develop and implement a National Aviation Security Training Programme to enable aircrew and ground personnel to implement aviation security requirements and to respond to acts of unlawful interference with aviation. This programme should include selection, qualification, training, certification and motivation of security staff.

The managers developing and conducting security training for security and air carrier and airport ground staff should possess necessary certification, knowledge and experience which should include as a minimum: 1) extensive experience in aviation security operations; 2) certification approved by national appropriate authority, or other equivalent approval; and 3) knowledge in the areas of security systems and access control, ground and in-flight security, pre-boarding screening, baggage and cargo security, aircraft security and searches, weapons and prohibited articles, overview of terrorism, and other areas and measures related to security that are considered appropriate to enhance security awareness. The managers and instructors, involved in and responsible for the security training of airport ground staff, should undergo an-

98) Statement given by the Commission spokeswoman, Barbara Helfferich, at the beginning of January, 2010.

nual recurrent training in aviation security and on latest security developments.

The Security staff should be trained to undertake the duties to which they will be assigned and should include the security areas of: 1) screening technology and techniques; 2.) screening check point operations; 3) search techniques of cabin and hold baggage; 4) security systems and access control; 5) pre-boarding screening; 6) baggage and cargo security; 7) aircraft security and searches; 8) weapons and restricted items; 9) overview of terrorism; and 10) other areas and measures related to security that are considered appropriate to enhance security awareness. The scope of training may be increased subject to aviation security needs and technology development. The initial training period for screening staff should not be shorter than the International Civil Aviation Organisation (ICAO) recommendation[99]. The security screening staff should be approved or certified by the national appropriate authority. The appropriate measures should be promoted to ensure that security staff is highly motivated so as to be effective in the performance of their duties.

For the other staff, for instance the flight crew and airport ground staff, the Security Training and Awareness training programme should be conducted on initial and recurrent basis for all airport and air carrier flight and airport ground staff. The training should contribute towards raised security awareness as well as improving the existing security systems. It should incorporate the following components: 1) security systems and access control; 2) ground and in-flight security; 3) pre-boarding screening; 4) baggage and cargo security; 5) aircraft security and searches; 6) weapons and prohibited articles; 7) overview of terrorism; and 8) other areas and measures relating to security that are considered appropriate to enhance security awareness. The security training course for all airport and air carrier ground staff with access to security restricted areas, should be designed for a duration of at least 3 hours in the classroom and a 1 hour field introduction.

In its Annex, the Regulation 300/2008 sets out only the general common basic standards related to the staff recruitment and training[100]. The persons implementing, or responsible for implementing, screening, access control or other security controls should be recruited, trained and, where appropriate, certified so as to ensure that they are suitable for employment and competent to undertake the duties to which they are assigned. Persons other than passengers requiring access to security restricted areas, should receive security training, before an airport identification card or crew identification card is issued. This should be conducted on initial and recurrent basis. The instructors engaged in the training of the persons mentioned should have the necessary qualifications. In the part dedicated to the in-flight security measures is only eminent that appropriate security measures such as training of flight crew and cabin staff should be taken to prevent acts of unlawful interference during a flight.

99) Standards and Recommended Practices for the licensing of flight crew members (pilots, flight engineers and flight navigator***s***), air traffic controllers, aeronautical station operators, maintenance technicians and flight dispatchers, are provided by Annex 1 to the Convention on International Civil Aviation. Related training manuals provide guidance to States for the scope and depth of training curricula which will ensure that the confidence in safe air navigation, as intended by the Convention and Annex 1, is maintained. These training manuals also provide guidance for the training of other aviation personnel such as aerodrome emergency crews, flight operations officers, radio operators and individuals involved in other related disciplines

100) Part 11, Annex to the Regulation 300/2008

The Regulation 820/2008, supplements some provisions regarding the staff recruitment and training. According to this regulation, the National Aviation Security Training Programme should include training requirements for handling unruly passengers[101]. Regarding the air carrier and airport security management this regulation sets out the fact that the appropriate authority should ensure that each Community airport and air carrier shall have suitable qualified security management. The appropriate authority should ensure that there is an adequate security management organisation. Senior managers responsible for the security compliance of air carriers or airports should posses the necessary level of qualification, knowledge and experience, including: 1) experience in aviation security operations, or 2) experience from other security related fields, such as law enforcement, military or other, 3) certification or equivalent approval by the appropriate authority and 4) knowledge in the following areas: security systems and access control, ground and in-flight security, weapons and prohibited articles, overview of terrorism.

Appendix F: Overview of the Sources of Italian Law

The main sources of the Italian law, ranked according to the criteria of hierarchy of sources, are: 1) the Constitution; 2) Constitutional laws; 3) Ordinary laws; 4) Acts having the force of a law: Decrees-Laws, Decrees Legislative, Regional laws; 5) Executive regulations; 6) Regulations of the local authorities and 7) Custom law. In addition to the primary sources of the Italian law, there are also the sources deriving from the accession of Italy into the European Union, the European Community and the various international treaties.

The *Ordinary laws* are enacted by the two Houses of the Parliament. They are also called "formal" laws to distinguish them from other sources called "material laws" (Decrees-Laws and Decrees Legislative are material laws). At the same level, there are also regional laws, covering matters other than the ones dealt with formal and material laws.

The *Decrees-Laws* are enacted by the Government "only in case of necessity and to cope with extraordinary and urgent situations"[102]. They have to be submitted to the Houses of Parliament the very same day of their publication on the Official Journal. They are ineffective *ex tunc* if not "converted" into an ordinary law by the Parliament within 60 days.

The *Decree Legislative* or otherwise called Delegated Law is enacted by the Government pursuant to a law of delegation of the Parliament[103]. The law of delegation establishes: one or more specific subject matter(s) that a decree can deal with, a final term for an enactment of the decree, the principles and guide-lines to be consisted in a decree.

101) The term "unruly passenger" was introduced with this regulation. Unruly passengers are persons who commit on board a civil aircraft, from the moment when the aircraft door is closed prior to take-off to the moment when it is reopened after landing, an act of: assault, intimidation, menace or wilful recklessness which endangers good order or the safety of property or persons, assault, intimidation, menace or interference with a crew member in performance of duties or which lessens ability to perform duties, wilful recklessness or damage to an aircraft, its equipment, or attendant structures and equipment such as to endanger good order and safety of the aircraft or its occupants, communication of information which is known to be false, thereby endangering the safety of an aircraft in flight, disobedience of lawful commands or instructions for safe, orderly or efficient operations.

102) Art. 77 of the Italian Constitution

103) Art. 76 Idem

The *Regional laws* have been given a greater importance with the reform of 2001. Before that, only Regions with special autonomy (and the Provinces of Trento and Bolzano) had an exclusive legislative power in certain areas. Other Regions had only a concurrent power in specific listed subjects and an integrative or delegated power where a law of the State established so. Now any Region can enact laws on subject(s) not reserved to the State. There are two types of law, related to: 1) a concurrent legislative power (the regional laws have to comply with the general principles established by the State with a specific law); 2) an exclusive legislative power (in all issues not reserved to the State or disciplined by a concurrent legislative power).

The *Executive Regulations* are resolved by the Government and enacted through a Decree of the President of the Republic. These Regulations generally are enacted to produce norms subordinated to the primary norms (ordinary laws. Decrees legislative and EU regulations) and they can never regulate matters covered by saving clauses, whether absolute or relative. Depending on the issuing body they can be distinguished in: 1) Regulations issued by the President of the Council of Ministers (D.P.C.M.); 2) Ministerial Regulations (D.M.); 3) Interministerial Regulations (D.P.C.M.) enacted by the Council of Ministers and referring issues afferent to many Ministries. The Executive Regulations are secondary sources and as such they cannot derogate the Constitution or the ordinary laws.

The European Community legislation becomes part of the Italian law on the basis of the Italian Constitution (Art. 11). Italy can transfer and limit its national sovereignty in favour of a legal order that ensures peace and justice among people. As a result of the accession of Italy to the European Community and the European Union, the Italian legal system is composed of the Italian and the Community law (especially by binding acts like regulations, directives and decisions). Each year the Parliament is required to adopt a Community Law in order to coordinate the national regulatory framework with the legal acts coming from the European Community. The coexistence between the Community law and the national Italian law is not always smooth. It may happen that there are contrasts and contradictions between them. Those who are applying or judge according to them must know which of the two and by what criteria are considered to be prevalent. On this point, the Italian Constitutional Court has intervened several times and ruled that there is a prevalence of the provisions of Community Law over the inconsistent provisions of National Law. The sources of Community law may derogate, in the matters within the exclusive competence of the Community itself, also the Constitutional norms, excepting always the high level principles of the Italian legal order.

The Community law that requires implementation in Italy must be presented by the Government to the both Houses of Parliament by the 31st January of each year along with a list of directives that require implementation. The Government has the duty to provide a report on the Italian participation in the Community normative process and on the principles and guidelines that characterise the Italian policy in respect of the Community legislation. With the Community law are amended or repealed also the national provisions that are contrary to the Community obligation and the Government is authorised to implement regulations. If the Italian sources of law interfere with the Community sources of law in the discipline of the same matter, the judges who are judging a dispute should not apply the Italian sources of law but have to apply the Community sources if they are legitimate.

A.A. Cohen: U.S. Homeland Security Policy Approaches to Defenses Against Airline Terrorism: Prevention of a CBRN Attack

1. Introduction

Imagine the following scenario: A commercial aircraft carrying some three hundred passengers of various nationalities from Hong Kong, China, to Helsinki, Finland, becomes the site of a bio-terror incident. While in Russian airspace, the plane's crew begins to report mounting health problems consistent with the dispersal of a bio-agent. By the time the flight touches down in Helsinki, authorities face a full blown CBRN event—one with the potential to expand beyond national borders and the ability of the government in Helsinki to contain it.

How should Finnish authorities respond? Beyond the immediate tasks of quarantining those immediately affected and decontaminating affected facilities/equipment, a comprehensive incident response plan is required. Such a blueprint would provide the Finnish government with guidance in three areas: preparedness, response and consequence management.

Currently, the Finnish response falls short of serving as such a comprehensive strategy. True, the country already boasts a comprehensive national civil defense infrastructure—a product of its close proximity to Russia and its need to anticipate threats from Soviet Union during the decades of the Cold War.[1] Yet, this infrastructure is still overwhelmingly oriented toward mitigating the overwhelming conventional force that would be employed by Moscow should hostilities erupt. According to experts, "Finland views its place on the threat radar as being very low, so the threat from outside (or inside) terrorists using non-conventional weapons is not seen as a major threat."[2] However, the world we live in is changing. The scenario outlined above, while quite feasible, would thus present a qualitatively new challenge to Finnish authorities — one requiring a modification of existing civil defense and homeland security protocols to more adequately address the danger of CBRN terrorism.

Here, the American experience can prove useful. In the aftermath of the September 11th attacks, a recognition of the resulting dangers prompted the U.S. government to launch a concerted effort to boost its planning and preparedness to the possibility of a CBRN (chemical, biological, radiation or nuclear) attack in the aftermath of the 9/11 attacks. More than eight years on, the United States boasts an elaborate and extensive process by which it can **prepare** for—and, if necessary, **respond to**—a catastrophic attack on the U.S. homeland involving biological weapons. US is also prepared to **manage the consequence** of such an event, as we will demonstrate below.

1) Pentti Partanen, "Going Underground," *CBRNe World*, Winter 2007, 62, http://cbrneworld.com/pdf/07_winter_Going%20Underground.pdf.

2) Ibid.

2. Defining the Problem

Such a response starts with analyzing the range and nature of hazardous materials that could be used by hostile forces to carry out a bioterror attack.

In the year 2000, the Centers for Disease Control and Prevention (CDC) in Atlanta laid the foundation for such a determination when they issued a list of potential deadly biological agents differentiated according to the dangers they posed and the levels of response they would require from the federal government and from state and local authorities. The highest threat level materials were defined as *Category A agents* which could be "easily disseminated or transmitted person-to-person (and) cause high mortality with potential for major public health impact". These agents, the CDC concluded, would "require special action for public health preparedness".[3]

By contrast, the CDC continued, *Category B* agents were far less dangerous, while still posing a significant threat to public health. They were defined as "moderately easy to disseminate (and) would be limited in their impact threatening only "moderate morbidity and low mortality".[4]

Category C agents were defined by the CDC as potential future threats caused by "emerging pathogens that could be engineered for mass dissemination in the future".[5] While not posing an immediate threat, the CDC recommended planning in advance to anticipate the emergence of such threats as they would need "specific enhancements of diagnostic capacity and disease surveillance" and might eventually pose a "potential for high morbidity and mortality and major health impact".[6]

The study, produced by the Clinton administration prior to 9/11, nonetheless anticipated that significant terrorist attacks against the U.S. mainland could be perpetrated specifically by al-Qaeda as well as "other extremist groups". It also drew a distinction between such non-state actors, which it defined as "independent terrorist organizations", and groups that were sponsored or supported "by rogue nations such as Iraq". The CDC also warned that the spectrum of threats would also cover "cult groups" (e.g., the Japanese religious cult Aum Shinrikyo) and "lone offenders", citing as an example 1994 Oklahoma City bomber Timothy McVeigh.

In the event of a bio-terrorism event, such as that outlined in the Aether scenario, the classification criteria outlined above will provide guidance as to the level of severity of the incident, and which measures should be employed as part of the governmental response to it.

3. Evolution of the American Response

It is useful for European CBRN planners to examine the American thinking and strategic planning on massive man-made disaster response. Following the 9/11 attacks, the U.S. government vastly expanded its funding, manpower, programs and procedures for responding to

3) Today, this categorization can be found at Centers for Disease Control and Prevention, "Emergency Preparedness and Response: Bioterrorism", n.d., http://www.bt.cdc.gov/agent/agentlist-category.asp.

4) Ibid.

5) Ibidem.

6) Centers for Disease Control and Prevention, "Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response", n.d., http://www.cdc.gov/mmwr/preview/mmwrhtml/rr4904a1.htm

chemical, biological, radiological and nuclear [CBRN] threats to the U.S. mainland. The initiative was a bipartisan effort, initially authorized by a Republican president and four Republican-controlled congresses (from late 2000 through November 2006), and subsequently sustained by two Democratic-controlled Congresses and current Democratic President Barack Obama.

The centerpiece was the establishment, in late 2002, of the U.S. Department of Homeland Security (DHS). Intended to serve as a "quarterback" coordinating and delegating authority for the activities of the 22 federal agencies, DHS represented the largest expansion of the federal government in nearly half-a-century. The fledgling Department certainly did not have a monopoly on issues of homeland security: it still had to coordinate the activities of its agencies with the Department of Defense, the Department of Energy, the Department of Justice (with particular reference to the Federal Bureau of Investigation, which comes under the authority of the attorney-general) and other government agencies. However, it quickly became seen as the central node for homeland security planning and preparedness across the federal bureaucracy.

Over the years, that position has garnered the Department no shortage of criticism. Government watchdogs and federal observers alike have highlighted the shortfalls in funding, unclear official priorities, and contradictory authorities. In many cases, these problems persist to the present day.[7] DHS also has had difficulty in winning the trust of the American people. It came in dead last of all 74 federal agencies in a national survey published in March 2007 by the Michigan-based Ponemon Institute, which sampled the views of more than 7,000 Americans.

However, these lingering problems must be weighed against the Department's successes in protecting the 300 million inhabitants of the single most open and potentially vulnerable major industrial nation in the world. As of this writing, more than eight years following the 9/11 attacks, not a single further significant terrorist attack against the United States has successfully been carried out.

This state of affairs owes a great deal to the integrated, networked structure put into place by the Bush administration in the days after 9/11. In creating DHS, the Bush administration abandoned the trend visible in modern business toward outsourcing and the lateral coordination of organizations. Instead, it chose to establish a huge, centralized structure on the model of the gargantuan "big government" systems in fashion at the time of the New Deal and in the decades that followed.

In the years since, the DHS and its dedicated disaster mitigation branch, the Federal Emergency Management Agency (FEMA), have focused their efforts in two broad areas.[8] The first deals with preparedness for future CBRN events. The second involves upgrades to coordination and capabilities in the wake of a potential CBRN disaster.

7) Spenser S. Hsu, "GAO Criticizes Homeland Security's Efforts to Fulfill Its Mission", *Washington Post*, September 6, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/05/AR2007090502570.html.

8) The mandate of FEMA is to implement and oversee a "comprehensive emergency management system to respond to and recover from natural disasters and terrorists attacks, including RDD and IND attacks". Government Accountability Office Natural Resources and Environment Office Director Gene Aloise, testimony before the House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, September 14, 2009, http://www.gao.gov/new.items/d09996t.pdf. .

✓ *3.1 Preparedness*

In order to prepare for a CBRN attack, the U.S government has implemented various training programs across all sectors that are likely to be involved or affected in an unconventional incident involving biological agents, such as that outlined in the Aether scenario. These include:

Governmental exercises. The Federal government conducts two types of exercises, the Federally Managed Exercise and the Alternate Year Exercise, which can be supplemented by additional exercises conducted by localities. The Federally Managed Exercise is intended to evaluate the "readiness" of a community. This exercise tests the entire emergency response effort, and evaluates the interaction of all relevant components. It involves mobilization of emergency service and response agencies, activation of communications centers and command posts, and field play. An Alternate Year Exercise is used by a community to train participants, evaluate emergency operations plans, evaluate procedures for new equipment or resources, validate corrections to outstanding findings, and address other issues.

Medical preparedness. One cannot underestimate the importance of medical preparations when facing a biological attack. The Hospital Preparedness Program (HPP) enhances the ability of hospitals and health care systems to prepare for and respond to bioterrorism and other public health emergencies. Current program priority areas include interoperable communication systems, bed tracking, personnel management, facility management planning and hospital evacuation planning.

There has been immense progress over the past five years to direct HPP funds specifically to target the needs of biological terrorism. There has been improved bed and personnel surge capacity, decontamination capabilities, isolation capacity, stockpiling of pharmaceutical supplies, training, education, drills and exercises. Additionally, the Pandemic and All Hazards Preparedness Act of 2006 transferred the National Bioterrorism Hospital Preparedness Program (NBHPP) to the Department of Homeland Security, where it is now overseen by the Assistant Secretary for Preparedness and Response (ASPR) at DHS. The focus of the program, while covering bioterrorism, is more broad-based response.[9]

Biodefense. Furthermore, in 2004, the Project BioShield Act was signed into law. One of the goals of Project BioShield is to "expedite the procurement of existing countermeasures and the conduct of research and development on new countermeasures".[10] In order to make promising treatments available quickly in emergency situations, the Act authorizes the Secretary of Health and Human Services to release for use measures as yet unproven and unlicensed by the Food and Drug Administration, such as vaccines which have not yet undergone full clinical trials. It also ensures that the government can buy improved vaccines or drugs to be included in the Strategic National Stockpile. These measures, though perhaps a bit controversial, give the U.S. government the freedom to take the drastic measures needed if a biological attack moves beyond conventional medical protocol.[11]

9) U.S. Department of Health and Human Services, "Hospital Preparedness Program", n.d., http://www.hhs.gov/aspr/opeo/hpp/.

10) See Henry L. Stimson Center, "Project Bioshield", May 30, 2007, http://www.stimson.org/MAB/?SN=CT200705111255.

11) U.S. Government Accountability Office, *Briefing: Project BioShield Act: HHS Has Supported Development, Procurement, and Emergency Use of Medical Countermeasures to Address Health Threats*, July 24, 2009, www.gao.gov/new.items/d09878r.pdf.

Coordinated communications. Communications move through various channels from Federal to local government and vice versa, and from first responders to politicians. However, having a coherent, systematic way to channel these communications is easier said than done. Programs such as SAFECOM, developed by the Department of Homeland Security, provide research, development, testing and evaluation, guidance tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies. The Office of Emergency Communications at DHS supports the SAFECOM program as a necessary tool to develop and maintain efficient and effective communications during an emergency.[12]

Environmental preparedness. Water, the source of life itself, can serve as a critical tool to safeguard against the effects of biological agents. If contaminated, it can also be one of the best ways to amplify the effects of a biological attack. To prevent this, the Water Sector Incident Command System (ICS) and National Incident Management System (NIMS) have developed training materials along with the EPA Water Security Division to help drinking water and waste water utilities to better understand ICS and integrate with other first responders within the ICS structure, and implement NIMS concepts that will help utilities provide mutual assistance to each other.[13]

The EPA has taken a part in this process by creating a program entitled *The Interim Response Protocol Toolbox*. This series of modules provides valuable emergency response skills and information for not just water utilities, but also laboratories, emergency responders state drinking water programs, technical assistance providers, and health and law enforcement officials.[14]

Pentagon involvement. In the past, the Defense Department (DoD) has specifically taken an active role for planning for a CBRN response. DOD forces, specifically the Joint Forces Headquarters Guardians and the Military District of Washington, could be called upon to execute a multitude of missions, ranging from civil disturbance assistance to all-hazard CM. The District of Columbia National Guard, for example, has established a Task Force-CBRN headquarters and developed a rapid detection team. It was established to provide command and control, communications, and intelligence information in support of the mission, showing the cooperation between federal and local authorities. The Command Operations, Communications, and Medical components of the surrounding states staffed TF-CBRN. There were also four mobile rapid detection teams, located throughout the National Mall, each comprising of three civilian and interagency personnel from different sectors. Lastly, there were also two Rapid Support Teams, made up of technical decontamination teams, the Analytical Laboratory Suite, and a command and control element.[15]

✓ *3.2 Response*

Mirroring the preparedness planning outlined above, the U.S. government has established an elaborate framework to respond to CBRN incidents. The foundation for this gameplan

12) Department of Homeland Security, "SAFECOM", n.d., http://www.safecomprogram.gov/SAFECOM/.

13) Environmental Protection Agency, "Nation Incident Management system", n.d., http://cfpub.epa.gov/safewater/watersecurity/home.cfm.

14) Ibid.

15*) Major Jeremy J. DiGioia and Captain Jonathan Ebbert, "CBRNE Response Measures for the 2009 Presidential Inauguration", Army Chemical Review, Summer 2009, www.wood.army.mil/.../CBRNE-Inauguration-Summer2009.pdf*

was outlined in January 2007, with the Bush administration's passage of Homeland Security Presidential Directive (HSPD) 18. That edict outlined the responsibility of the Secretary of Health and Human Services in spearheading Federal Government efforts to research, develop, evaluate, and acquire public health emergency medical countermeasures to prevent or mitigate the health effects of CBRN threats facing the U.S. civilian population. HHS leads the interagency process and strategic planning and manages programs supporting medical countermeasures development and acquisition for domestic preparedness.[16]

The Secretary is responsible for establishing an interagency committee to provide advice in setting medical countermeasure requirements and coordinating HHS research, development, and procurement activities. The committee will include representatives designated by the Secretaries of Defense and Homeland Security and the heads of other appropriate executive departments and agencies. This committee will serve as the primary conduit for communication among entities involved in medical countermeasure development.

The chair of the committee keeps the joint Homeland Security Council/National Security Council Biodefense Policy Coordination Committee apprised of HHS efforts to integrate investment strategies and the Federal Government's progress in the development and acquisition of medical countermeasures.[17] Also, all relevant HHS programs and functions to support this strategic planning are aligned.[18]

The crux of this role is to ensure that the development of near-term medical countermeasures and the ability to address future attacks is coordinated and focused into one agency, which can then use other agencies to implement these preparations.

Though the U.S. government has broad responsibility to respond to a CBRN attack, many aspects of response and recovery fall outside federal jurisdiction. The HHS Secretary therefore oversees engagement with the private sector in developing medical countermeasures to combat WMD, and provide clear and timely communication of HHS priorities and objectives. This includes creating an advisory committee composed of leading experts from academia and the biotech and pharmaceutical industries to provide insight on barriers to progress and help identify promising innovations and solutions to problems such as life-cycle management of medical countermeasures, creating a truly, collaborative response.[19]

The directive also outlines the specific duties of the Secretary of Defense in the event of a CBRN incident. While sharing similar responsibilities as HHS, they are related specifically to the Armed Forces and entail directing strategic planning for and oversight of programs to support medical countermeasures development and acquisition for Armed Forces personnel.[20]

16) White House, Office of the President, *Homeland Security Presidential Directive/HSPD-18*, January 31, 2007, http://www.fas.org/irp/offdocs/nspd/hspd-18.html.

17) Ibid.

18) Ibidem.

19) Ibidem.

20) White House, Office of the President, *Homeland Security Presidential Directive/HSPD-18*, January 31, 2007, http://www.fas.org/irp/offdocs/nspd/hspd-18.html.

The Secretaries of Health and Human Services and Defense together ensure that the efforts of the Department of Defense (DoD) and HHS are coordinated to "promote synergy, minimize redundancy, and, to the extent feasible, use common requirements for medical countermeasure development".[21]

The Secretary of Homeland Security develops a strategic, integrated all-CBRN risk assessment that integrates the findings of the intelligence and law enforcement communities with input from the scientific, medical, and public health communities[22], while continuing to issue Material Threat Determinations for those CBRN agents that pose a material threat to national security.[23]

Apart from DHS, DoD and HHS, other agencies are an integral part of the preparation process, as outlined by DHS:

- The U.S. Department of Agriculture personnel conduct cargo and product inspections to prevent the entry of pests and diseases. Within that agency, the Food Safety Inspection Service inspects farms and other production and processing sites to assure food safety. USDA also works with the Centers for Disease Control (CDC) and the U.S. Food and Drug Administration (USDA).[24]
- The U.S. Army Medical Research Institute of Infectious Diseases conducts research on potential bioterrorist agents and provides guidance on medical management issues.[25]
- The Agency for Healthcare Research and Quality (AHRQ) funds various projects to improve preparedness, including training. [26]
- The Centers for Disease Control are instrumental in creating and implementing programs to prepare of biological attacks as it is an agency that connects the Federal government to the U.S. general public. The CDC's goal for its bioterrorism programs is the enhanced public health preparedness against attacks. Focus areas include: surveillance, Epidemiology, rapid laboratory diagnosis, emergency response, and information systems. The CDC provides funding to state and local health departments, coordinates the Health Alert Network, and coordinates the Laboratory Response Network. It also participates in several food borne disease surveillance systems that involve collaboration between CDC, FDA, and USDA. Recently, the CDC also coordinated the smallpox vaccination program through state and local health departments.[27]
- The FDA monitors the occurrence of food borne illnesses through several surveillance systems that involve collaboration between CDC, FDA, and USDA.[28]

21 Ibid.

22 Ibidem.

23 Ibidem.

24 Department of Homeland Security, "Bioterrorism Planning, Preparedness, and Response, Preparedness of Other Federal Agencies", n.d., http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/planning/bt-prep-planning.html

25 Ibid.

26 Ibidem.

27 Ibidem.

28 Department of Homeland Security, "Bioterrorism Planning, Preparedness, and Response, Preparedness of Other Federal Agencies", n.d., http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/planning/bt-prep-planning.html

- The Health Resources and Services Administration (HRSA) has primarily been responsible for promoting hospital preparedness for mass casualty events, including those caused by bioterrorism.[29]
- The National Institutes of Health (NIH) has funded research in the area of diagnostics, clinical therapies, vaccines, and basic science through the National Institute of Allergy and infectious Diseases (NIAID).[30]
- The Office of the Assistant Secretary for Public Health Emergency Preparedness coordinates public health preparedness for terrorism acts, including bioterrorism. This office includes the Office of Emergency Response, which houses the Secretary's Command Center.[31]
- The Department of Justice (DOJ) and the FBI are responsible for coordination federal domestic preparedness against WMDs. The Counterterrorism Division includes the National Domestic Preparedness Office.[32]
- The Environmental Protection Agency (EPA) has a critical role in the preparation and response to a CBRN attack. It has the authority and responsibility to prepare and respond to emergencies involving oil, hazardous substances, and certain radioactive materials. It has required communities to develop emergency plans for release of hazardous substances through Local Emergency Planning Committees. It also trains first-responders to handle terrorist events. In the event on an attack that involves environmental contamination, the EPA is responsible for assisting with environmental monitoring, decontamination efforts, and long-term site cleanup. [33]
- Finally, the Department of Veterans Affairs provides backup to the DOC and DHHS as needed for medical disasters. It also provides support to DHHS/DHS for maintaining the Strategic National Stockpile.[34]

This web of bureaucratic involvement is complex and at times bewildering. It reflects multiple stakeholders with overlapping mandates and often-competing authorities. Whether such a structure will be effective and responsive in the event of a real world WMD incident remains to be seen.

4. Managing Bioterror in the United States

In the U.S. as well as in Europe, when a crisis occurs, the immediate actions fall under the responsibility of first responders. First responders include police, firefighters, local emergency personnel, and hazardous material technicians. These individuals must identify the agent used, so as to rapidly decontaminate victims and apply appropriate medical treatments. If the incident overwhelms state and local response capabilities, they may call on federal agencies to provide assistance.

29) Ibid.

30) Ibidem.

31) Ibidem.

32) Department of Homeland Security, "Bioterrorism Planning, Preparedness, and Response, Preparedness of Other Federal Agencies", n.d., http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/planning/bt-prep-planning.html.

33) Ibid.

34)Ibidem.

This assistance includes special teams that can respond to terrorist incidents involving chemical or biological agents or weapons, providing a "hands-on response" through technical advice to state and local authorities. Federal laboratories stand ready to perform tests to analyze and test samples of chemical and biological agents in order to identify and commence treatment.[35]

The step-by-step process of response is most clearly shown in The National Response Preparedness Program, which covers both protocols under the Stafford Act[36] and outside it.

Under the Stafford Act, the Department of Homeland Security Homeland Security Operations Center (DHS HSOC) continually monitors potential disasters and emergencies. If there is an advance warning, DHS may deploy – and may request other Federal agencies to deploy – liaison officers and personnel to a State Emergency Operations Center (EOC) to assess the emerging situation. An RRCC may be activated, fully or partially. Facilities, such as mobilization centers, are established to accommodate personnel, equipment, and supplies.[37]

Immediately after an incident, local jurisdictions respond using available resources and notify State response elements. As information emerges, they also assess the situation and the need for State assistance. The State reviews the situation, mobilizes State resources, and informs the DHS/EPR/FEMA Regional Office of actions taken.

Once this level is reached, the Governor activates the State emergency operations plan, proclaiming or declaring a state of emergency, and requests a State/DHS joint Preliminary Damage Assessment (PDA) to determine if sufficient damage has occurred to justify a request from a Presidential declaration of a major disaster or emergency which has budgetary and federal resource allocations consequences. Based upon the results of the PDA, the Governor may request a Presidential declaration and define the kind of Federal assistance needed. At this point, an initial assessment is also conducted of losses avoided based on previous mitigation efforts.[38]

After the major disaster or emergency declaration, a Rapid Response Coordination Center staffed by regional personnel, coordinates initial regional and field activities such as deployment of an ERT-A. The ERT-A assesses the impact of the event; gauges immediate State needs, and makes preliminary arrangements to set up operational field facilities. Depending on the scope and impact of the event, the NRCC, comprised of Emergency Support Function (ESF) representatives and DHS/ERP/FEMA support staff, carries out initial activation and mission assignment operations and supports the RRCC from DHS/EPR/FEMA. A Federal Coordinating officer

35) United States General Accounting Office, *COMBATING TERRORISM Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination*, November 2000, http://www.gao.gov/new.items/d0114.pdf.

36) *Robert T. Stafford Disaster Relief and Emergency Preparedness Assistance Act,* FEMA 592, June 2007, http://www.fema.gov/pdf/about/stafford_act.pdf.

37) Department of Homeland Security, "National Response Plan", December 2004, www.iir.com/GLOBAL/FusionCenter/NRPbaseplan.pdf.

38) Ibid.

(FCO), appointed by the Secretary of Homeland Security on behalf of the President, coordinates Federal support activities. The FCO works with the State Coordinating Officer (SCO) to identify requirements. A Principal Federal Official (PFO) also may be designated as the Secretary's representative to coordinate overall Federal interagency indecent management efforts. The ERT works with the affected State and conducts field operations from the Joint Field Office.[39]

ESF primary agencies assess the situation and identify requirements and help States respond effectively. Federal agencies provide resources under DHS/EPR/FEMA mission assignment or their own authority. The Interagency Incident Management Group convenes when needed to provide strategic-level coordination and frame courses of action regarding various operational and policy issues. The HSOC supports the IIMG and coordinates with the JFO.

In order to coordinate with the general public, a toll-free telephone number that individuals can call to apply for disaster assistance for common questions is activated. One or more DRCs may be opened where individuals can obtain information about disaster assistance, advice, and counsel. Individual applicants are processed at the DHS/EPR/FEMA National Processing Center. Inspectors verify losses and provide documentation used to determine the types of disaster assistance to be granted to individuals and families.[40]

As immediate response priorities are met, recovery activities begin. Federal and State agencies assisting with recovery and mitigation activities convene to discuss State needs. Public Assistance Applicant Briefings are conducted for local government officials and certain private nonprofit organizations to inform them of available assistance and how to apply. Applicants must first file a Request for Public Assistance. Eligible applications will be notified and will define each project on a Project Worksheet, which details the scope of damage and a cost-estimate for repair to a pre-disaster condition. The Project Worksheet is used as the basis for obligating funds to the State for eligible projects.[41]

Throughout response and recovery, the JFO examines ways to maximize mitigation measures in accordance with State administrative plans. Grounded in local risk, and with State priorities and mitigation plans in place, DHS/EPR/FEMA and State officials contact local officials to identify potential projects and suggest which one should be included in an early implementation strategy. The strategy focuses on viable opportunities to provide funds, technical assistance, and staff support to incorporate mitigation into the overall community recovery, to include the repair and replacement of damages or destroyed housing and infrastructure. As the need for full-time interagency coordination at the JFO ceases, the ERT plans for selective release of Federal resources, demobilization, and closeout. Federal agencies then work directly with their grantees from the monitor individual recovery programs, support, and technical services.[42]

39) Ibidem.

40) Ibidem.

41) Department of Homeland Security, "National Response Plan", December 2004, www.iir.com/GLOBAL/FusionCenter/NRPbaseplan.pdf.

42) Ibid.

5. Aether in the United States: Bioterror Response

It is actually more likely that a bioterror attack could occur in the United States than in Europe, given the vehemence of the proclaimed terrorist commitment to assault the American homeland. If it happens, the National Response Plan specifically outlines procedures for biological threats such as those outlined in the Aether scenario. In such an incident, HHS and its federal partner organizations would evaluate the situation and outline a national plan providing recommendations to appropriate public health and medical authorities regarding the need for quarantine, shelter-in-place or isolation to prevent the spread of disease.

It is DHS doctrine to take an all-hazards approach to response. Thus, its response arm, FEMA, is the primary agency in these response situations. The Honorable David Heyman, the Department of Homeland Security's Assistant Secretary for Policy, describes the biggest building blocks of the Nation's biodefense strategy as:

1. To detect-to-treat DHS operates the Bio Watch program for early recognition that a bioattack has taken place,
2. The development through HHS and DoD of medical countermeasures to protect people from the attack,
3. The partnership between DHS and National Center for Medical Intelligence (NCMI), and
4. Strengthening the public health community at the State and Local level to effectively treat the exposed population to mitigate illness and death.[43]

DHS likewise funds the nation's Bio Watch program. It stems from a critical part of Federal partnership that includes the HHS distribution of the strategic national stockpile to a location, and the dispensing of post-exposure prophylaxis by Federal, State and local officials to the affected population. DHS, HHS and DoD also partner to maximize investment utility on medical countermeasure development and acquisition for the most relevant vaccines and drugs, and jointly establish R&D priorities to respond to a full range of bio and chemical threat agents.[44]

The role of first responders and their relationship with the Federal government is also outlined in this statement. Heyman describes surge capacity as being vital to effective consequence management of large-scale CBRN events. The national architecture for responding to a CBRN incident assumes first and foremost a local response, with individuals and local communities managing and coping with the initial stages of an incident. When an incident occurs that exceeds or is anticipated to exceed local or State resources, a surge of additional resources and capabilities is required. These sources may come from nearby states or from the Federal Government. For major disasters, as governed by the Stafford Act, this surge can also be initiated through the request of a State Governor for regional and/or Federal support. It can also be initiated by Presidential declaration.

43) Assistant Secretary of Homeland Security for Policy David Heyman, Statement before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, July 28, 2009, http://armedservices.house.gov/pdfs/TUTC072809/Heyman_Testimony072809.pdf.

44) Assistant Secretary of Homeland Security for Policy David Heyman, Statement before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, July 28, 2009, http://armedservices.house.gov/pdfs/TUTC072809/Heyman_Testimony072809.pdf.

As it is anticipated that large-scale CBRN events are likely to overwhelm State and local capabilities, quickly requiring additional resources from the Federal Government is vital. Thus, DHS is actively working to further develop two key roles in CBRN response preparedness:

1. To assist state and local responder organizations in preparing to recognize and respond to the novel or unique aspects of CBRN attacks, and
2. To coordinate the Federal response.[45]

Assistance to state and local stakeholders is largely provided through grants to state and local governments from FEMA, state and local outreach efforts, exercises, and training.

In FY2009 DHS announced over $1 billion in homeland security grants to States and local governments to build and strengthen preparedness capabilities through planning, equipment and readiness for all hazards, including CBRN preparedness. As required by HSPD-8 and Post Katrina Emergency Management Reform Act, FEMA also provides assistance by establishing readiness metrics in the National Preparedness Goal to measure national progress in domestic all-hazards preparedness as well as an overall National Preparedness System for assessing the nation's preparedness capability to counteract CBRN threats. Additionally, FEMA develops preparedness guidance to support the enhancement of these capabilities.

FEMA also manages a Pre-Positioned Equipment Program that has caches of hazardous materials response equipments located at various sites across the country to support state and local first responders in the event of a CBRN attack or other disasters involving hazardous materials. DHS interacts daily with Federal counterparts to ensure maximum coordination on issues such as CBRN threats and intelligence, public health issues, infrastructure protection and security, counterterrorism and counter proliferation secure transportation and shipping, and disaster response coordination. DoD, and in particular NORTHCOM, play major roles in many of these areas.[46]

If a CBRN attack occurs, the Department of Homeland Security has set the following guidelines for how and what information is critical during an emergency response situation: situation assessments, general strategies and specific tactics, and safety information. Situation assessments provide reports of relevant incident information regarding public health and medical issues. It also provides information that may be useful in developing respective State IAPs. Resource assessments help managers or officials from other States gauge the severity of hazard impact. It also helps estimate the potential impact that may occur if people evacuate and how to anticipate the state of requests for mutual aid. Lastly, safety information describes a state or jurisdictional approach to health and medical issues affecting responders. This helps standardize safety protocols for responders across state boundaries.[47]

45) Assistant Secretary of Homeland Security for Policy David Heyman, Statement before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, July 28, 2009,http://armedservices.house.gov/pdfs/TUTC072809/Heyman_Testimony072809.pdf.

46) Assistant Secretary of Homeland Security for Policy David Heyman, Statement before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, July 28, 2009, http://armedservices.house.gov/pdfs/TUTC072809/Heyman_Testimony072809.pdf.

47) Department of Health and Human Services, "Forms of Interstate Assistance, Information Sharing", n.d., http://www.hhs.gov/disasters/discussion/planners/mscc/chapter6/6.2.html#6.2.1.

✓ *5.1 Communications Plan*

Meanwhile, information about the attack, and the mitigation efforts undertaken in response, is disseminated via a comprehensive communications plan. The Integrated Public Alert and Warning System (IPAWS) expands upon the traditional audio-only radio and television by providing one message over more media to more people during and after a disaster. Alerts were sent to 60,000 residential phones in ten minutes and transmitted in Spanish and Vietnamese translations (the most prominent non-English languages in the testing area). The program also provides individual alerts to people who signed up on the Internet, giving them the option to receive alerts through their cell phone. Additionally, to address the hard of hearing community, videos were posted on the internet and links to those videos were distributed to email and cell phones.[48] The U.S. Computer Emergency Readiness Team (US-CERT) is a 24-7 watch and warning center for the federal government's internet infrastructure.[49]

The Emergency Alert System (EAS) is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, and direct broadcast satellite providers to furnish the communications capability to the President to address the American public during a national emergency. The system may also be used by state and local authorities to deliver important emergency information. The President has the sole responsibility for determining when the EAS will be activated at the national level, and has delegated this authority to the director of FEMA. FEMA is responsible for implementation of the national-level activation of the EAS, tests, and exercises. The FCC's role included prescribing rules that establish technical standards for the EAS. FCC ensures that the EAS state and local plans developed by industry conform to FCC EAS rules and regulations.[50]

✓ *5.2 Critical Infrastructure Protection*

When preparing and responding for a CBRN attack, there are many actions and programs that are taken to protect critical infrastructure. Drinking water protection has been addressed under various directives and acts. Under the Bioterrorism Act, drinking water systems must certify completion of emergency response plans within six months of certifying that their vulnerability assessment is complete.[51]

Homeland Security Presidential Directive 5, "Management of Domestic Incidents," requires that states, territories, local jurisdictions and tribal entities adopt the National Incident Management System (NIMS). This program enables responders from a variety of jurisdictions and disciplines to work together effectively when responding to an emergency. The private sector, including water and wastewater treatment systems, also plays a vital role in NIMS. The implementation of the NIMS created a foundation for the nation's prevention and response strategy for its water.[52]

48) Federal Emergency Management Agency, "Integrated Public Alert Warning System", n.d., http://www.fema.gov/emergency/ipaws/.

49) U.S. Computer Emergency Readiness Team, http://www.us-cert.gov.

50) Federal Emergency Management Agency, "Emergency Alert System", n.d., http://www.fema.gov/media/fact_sheets/eas.shtm.

51) Environmental Protection Agency, "Nation Incident Management system", n.d., http://cfpub.epa.gov/safewater/watersecurity/home.cfm..

52) Ibid.

The FCC and FEMA have developed logistical coordination to provide assistance when state aid is not available. Under this protocol, FEMA can request that FCC personnel be deployed to the JFO to provide assistance to communications companies, including broadcasters. The FCC then coordinates actions with and between other private sector communications companies, and local businesses to determine who can provide the needed assistance.[53]

Homeland Security Presidential Directive 7 (HSPD-7) and the National Infrastructure Protection Plan (NIPP) provide the overall framework for a structural partnership between government and the private sector for the protection of critical infrastructure. This encourages the formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). SCCs foster and facilitate the coordination of sector-wide activities and initiatives designed to improve the security of the nation's critical infrastructure. They are self-organized, self-led and focused on homeland security and critical infrastructure protection. The GCC, meanwhile, brings together diverse federal, state, local and tribal interests to identify and develop collaborative strategies that advance critical infrastructure protection. GCCs serve as a counterpart to the SCC for each critical infrastructure and key resource sector. They provide interagency coordination around CIKR strategies and activities, policy and communication across government, and between government and the sector to support homeland security.[54]

The critical Infrastructure Partnership Advisory Council (CIPAC) provides the operational mechanism for carrying out the sector partnership structure The CIPAC provides the framework for owner and operator members of SCCs and members of GCCs to engage in intra-government and public-private cooperation, information sharing and engagement across all infrastructure protection activities. The CIPAC is a non-decisional body and includes sector members and government members. It has also been exempted from the requirements of the Federal Advisory Committee Act.[55]

In order to control the effects of a biological attack, certain quarantine measures are taken. The Federal Government derives its authority for isolation and quarantine from the Commerce Clause of the U.S. Constitution. Under the Public Health Service Act[56], the Secretary of Health and Human Services is authorized to take measures to prevent the entry and spread of communicable diseases from foreign countries into the United States and between States. Daily functions have been delegated to the Centers for Disease Control and Prevention (CDC), which is authorized to detain, medically examine, and release persons arriving into the United States – or traveling within the U.S. – suspected of carrying these communicable diseases.[57] When alerted about an ill passenger or crew by the pilot of a plane or captain of a ship, the CDC may detain passengers and crew as necessary to investigate whether the cause of the illness on board is a communicable disease.[58]

53) Federal Emergency Management Agency, "Disaster Support for Broadcasters", n.d., http://www.fcc.gov/pshs/broadcastersupport.html.

54) White House, Office of the President, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

55) Ibid.

56) 42 US Code 264.

57) 42 CFR 70 and 71.

58) Centers for Disease Control and Prevention, "Legal Authorities for Isolation and Quarantine", n.d., http://www.cdc.gov/ncidod/sars/legal.htm.

States have police power functions to protect the health, safety, and welfare of persons within their borders. To control the spread of disease within their borders, states have laws to enforce the use of isolation and quarantine. These laws vary from state to state and can be specific or broad. Tribes also have police authority to take actions that promote the health, safety, and welfare of their own tribal members. Tribal health authorities may enforce their own isolation and quarantine laws within tribal lands, if these laws exist.[59]

If a quarantinable disease is suspected or identified, CDC may issue a federal isolation or quarantine order. U.S. Customs and Border Protection and U.S. Coast Guard officers are authorized to help enforce federal quarantine orders.[60]

Despite this elaborate network of plans, procedures, and chains-of-command created over the past decade, the homeland security response of the United States is far from static. To the contrary, across the federal bureaucracy, constant thought is being given to methods by which CBRN interdiction, defense and mitigation can be accomplished more effectively.

A case in point is the Government Accountability Office's July 2009 "best practices" overview. The study, entitled *DISASTER RECOVERY: Experiences From Past Disasters Offer Insights For Effective Collaboration After Catastrophic Events*[61], outlines four collaborative practices that may help in responding to future catastrophic events, whether environmental or man-made:

(1) *Develop and communicate common goals to guide recovery*. Defining common recovery goals can enhance collaboration by helping stakeholders overcome differences in missions and cultures. After the Grand Forks/Red River flood, federally-funded consultants convened various stakeholders to develop recovery goals and priorities for the city of Grand Forks. The city used these goals as a basis to create a detailed recovery action plan that helped it to implement its recovery goals.

(2) *Leverage resources to facilitate recovery*. Collaborating groups bring different resources and capacities to the task at hand. After the Northridge earthquake, officials from the Federal Highway Administration and California's state transportation agency worked together to review highway rebuilding contracts, discuss changes, and then approve projects all in one location. This co-located, collaborative approach enabled the awarding of rebuilding contracts in 3 to 5 days - instead of the 26 to 40 weeks it could take using normal contracting procedures. This helped to restore damaged highways within a few months of the earthquake.

(3) *Use recovery plans to agree on roles and responsibilities*. Organizations can collectively agree on who will do what by identifying roles and responsibilities in recovery plans developed either before or after a disaster takes place. Learning

59) Ibid.

60) Ibidem.

61) U.S. Government Accountability Office, "DISASTER RECOVERY: Experiences From Past Disasters Offer Insights For Effective Collaboration After Catastrophic Events", Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 2009, http://www.gao.gov/new.items/d09811.pdf.

from its experiences from the Loma Prieta earthquake, San Francisco Bay Area officials created a plan that clearly identifies roles for all participants in order to facilitate regional recovery in the event of a future disaster.

(4) *Monitor, evaluate, and report on progress made toward recovery*. To improve the ability of the federal government to capture and disseminate recovery information, the Secretary of Homeland Security should direct the Administrator of FEMA to establish a mechanism for sharing information and best practices focused on disaster recovery, including practices that promote effective collaboration such as those discussed in this report.

6. Europe and America: Similarities and Differences

The American experience in homeland preparedness and civil defense differs from the European one in several key respects.

The first is authority. The U.S. response, while geographically diffuse, is centralized in nature and directed by a unitary authority and action plan. By contrast, a bioterror incident in the EU area, particularly were it to spread beyond the national boundaries of Finland, would activate multiple overlapping homeland security responses among various European Union members that could hamper prompt, effective action.

A rudimentary Europe-wide CBRN plan does exist, having been erected in the aftermath of the July 2005 suicide bombing attacks on London's public transport system. The JHA Council Declaration of July 13, 2005 called for the development of "arrangements to share information, ensure coordination and enable collective decision-making in an emergency, particularly for terrorist attacks on more than one Member State."[62] Subsequent EU emergency and crisis coordination arrangements (EU-CCA) outlined how the European institutions and states should interact in Brussels in a crisis. And the integrated EU arrangement for crisis management with cross border effects (EU-ICMA) provides practical, operational arrangements to implement EU-CCA and to aid cooperation between Member States.

These steps, however, fall short of the networked federal response developed by the United States, which integrates both military and civilian capabilities.

The second is leadership. The U.S. approach clearly designates the Department of Homeland Security, and to a lesser extent the Department of Health and Human Services, to serve as the coordinating mechanism behind a broad, interagency response, providing it with authority to coordinate both local and regional action plans dealing with CBRN events. The closest such authority in Europe is assumed by the Counter-Terrorism Coordinator, a post created by the European Council in the wake of the 2004 Madrid attacks.[63] That position is intended to "co-ordi-

62) European Union, *JHA Council Declaration on the EU Response to the London Bombings*, 13 July 2005, 11158/1/05 Rev.1, http://www.unhcr.org/refworld/docid/42fb11894.html.

63) European Commission, "Counter-Terrorism Coordinator", n.d., http://ec.europa.eu/justice_home/fsj/terrorism/institutions/fsj_terrorism_institutions_counter_terrorism_coordinator_en.htm.

nate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal".[64] It does not, however, possess the autonomous authority to coordinate counterterrorism and CBRN responses across the breadth of affected agencies possessed by relevant U.S. officials (namely, the Secretary of Homeland Security).

An array of other factors merit mention as well. These include linguistic barriers between European member nations (and even within them), which are not present in the American response and which may make it difficult if not impossible to communicate effectively and promptly among and with affected populations. Similarly, jurisdictional limitations are also a real concern; contrary to the U.S. experience, Europe does not represent a unitary government, but a collection of twenty-seven sovereign states. The individual civil defense plans established by each may well conflict with central EU planning for homeland security, and could even detract from a coordinated response across the Eurozone.

These issues hold salience for Finland. In the event that the scenario outlined above is not contained, and expands beyond the national borders of Finland, the American experience can provide a useful template for the protocols and procedures that could be successfully enacted by Finland specifically — and by the European Union more generally — in its efforts to prepare for, respond to, and cope with the aftermath of an incident of bioterrorism involving civil aviation.

64) European Commission, "Counter-Terrorism Coordinator", n.d., http://ec.europa.eu/justice_home/fsj/terrorism/institutions/fsj_terrorism_institutions_counter_terrorism_coordinator_en.htm.

Daniele Del Bianco, Marina Andeva & Emilio Cocco: Group Dynamics in the Airplane in the Aviation Rescue Situation

ABSTRACT: "When an airplane is flying, it is like a world of its own (…) aloof from everything else." It was with such a remark that a former flying pilot started to describe group dynamics on board of an aircraft in an emergency situation. The paper first identifies a specific descriptive model of group dynamics on board of an airplane by applying classical sociological theories to a number of case studies. Then, it focuses its attention on the psychological and social conditions and factors hindering or promoting effective management techniques of group dynamics and decision making in an emergency situation. Finally, the paper proposes a graphic framework to be applied during the simulation exercises as term of reference for its evaluation.

1. Analysing Risk On Board of an Airplane

In 1901, Wilbur Wright[1] stated: "If you are looking for perfect safety, you will do well to sit on a fence and watch the birds." But it is known that the fence will not collapse only by assessing its condition before it is sat upon, and even then the assessment may be wrong. The same can be applied not just for air safety but as well for security.

Risk is a normal part of daily life, and its assessment is a fundamental part of human behaviour. Risk has to be recognised, the alternatives weighed up and a balanced conclusion reached. In aviation, risk cannot be completely avoided but the penalties of taking unnecessary risks can be very high. Before a risk can be assessed it must first be recognised, but failure of recognition shows the seeds of a hazardous situation. Because human behaviour varies widely between individuals and situations, there is no simple formula for learning how to recognise degrees of risk. Essentially one can recognise two types of risk: objective – that is external risk, the assessment of which is not influenced by human beings; subjective – this is internal risk, which is coloured by the training and experience of the individual. Judgments can be affected by high stress levels which, in turn, may affect pilot and crew performances. There are four basic stressors: 1) physical – conditions associated with the immediate environment affecting physical well-being, such as temperature, noise, or vibration; 2) physiological – the physical conditions in relation to factors such as fatigue or hunger; 3) psychological – the influence of emotion, workload and the need to make decisions; 4) sociological – emotional stresses arising away from the flying environment, such as marital problems or job pressures. The positive capabilities in an individual's decision-making process are: creativity, innovation and adaptability. The negative human capabilities - potentially giving rise to errors - are: false mental model, incorrect motor programme[2] and lack of feedback. Time is a key element in the risk assessment process. When

1) The Wright brothers, Orville (August 19, 1871 – January 30, 1948) and Wilbur (April 16, 1867 – May 30, 1912), were two Americans who are generally credited with inventing and building the world's first successful airplane and making the first controlled, powered and sustained heavier-than-air human flight, on December 17, 1903.

2) According to Cambell (see R.D. Campbell and M. Bagshaw (2002) – 3 ed. Human Performance and Limitations in Aviation, Blackwell

time is perceived to be short, impulsive or inappropriate decisions are more likely to be made. Managing risk involves judgement and decision making, which is the result of appropriate thought processes (Cambell & Bagshaw, 2002). The effective management of group dynamics is a fundamental part of the risk management process on board of an airplane.

2. Introducing the Concept of Group Dynamics

✓ *2.1 Japan Airlines Flight 123*

On Monday 12 August 1985, the Japan Airlines Flight 1233 - a Japan Airlines domestic flight from Tokyo International Airport (Haneda) to Osaka International Airport (Itami) - suffered mechanical failures 12 minutes into the flight and 32 minutes later crashed into Mount Takamagahara, 100 kilometers from Tokyo. All 15 crew members and 505 out of 509 passengers died, resulting in a total of 520 deaths and 4 survivors.

As the aircraft reached cruising altitude, the rear pressure bulkhead failed. The resulting explosive decompression tore the vertical stabilizer from the aircraft and severed all four of the aircraft's hydraulic systems. The loss of cabin pressure at high altitude had also caused a lack of oxygen throughout the cabin, and emergency oxygen masks for passengers soon began to fail. Flight attendants, including one who was off-duty and flying as a passenger, administered oxygen to various passengers using hand-held tanks.

With total loss of hydraulic control and non-functional control surfaces, the aircraft began to oscillate up and down. The pilots managed a measure of control by using engine thrust. These improvisations proved helpful, but further measures to exert control, such as lowering the landing gear and flaps, interfered with control by throttle, and the plane's uncontrollability once again escalated.

Thirty-two minutes elapsed from the time of the bulkhead explosion to the time of the final crash, long enough for some passengers to write farewells to their families.

Japanese Airlines Flight 123	
Date	12 August 1985
Type	Structural failure, loss of hydraulic controls
Site	Mount Osutaka, Japan
Passengers	509
Crew	15
Fatalities	520
Survivors	4
Aircraft type	Boeing 747-SR46
Operator	Japan Airlines
Flight origin	Tokyo Int. Airport
Destination	Osaka Int. Airport

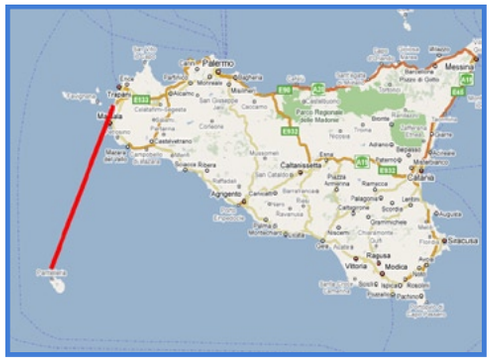
Science Ltd, Oxford) the four stages of information processing are: sensing, perception, decision making and motor action (response). The term 'incorrect motor programme' refers to an incorrect response programme determined by the motor skills of an individual.

3) Excerpts and data from http://en.wikipedia.org/wiki/Japan_Airlines_Flight_123

✓ *2.2. Private Air Flight DC3 Dakota*

In the mid 60s', private air flight DC3 Dakota4, on route from Pantelleria island to Trapani (Sicily, Italy), reported one engine failure 30 kms away from destination. It landed safely and in time at Trapani city airport. The private flight carried 26 Italian tourists, 2 pilots and 1 flight attendant. According to civil aviation regulations and protocols, when the engine failure was reported, the captain asked the flight attendant to invite passengers to wear their life jackets. Although very close to destination, since the airplane was flying over the sea, according to safety protocols, the captain and the cabin crew need to prepare passengers for splashdown.

As the then-captain recalls, few minutes after the flight attendant activated such procedure, screaming and shouting was heard in the cockpit. When the second-pilot entered the cabin to check what was happening, he could not restrain from laughing as he saw a distressed flight attendant helping passengers out from their life jackets which they had already inflated!



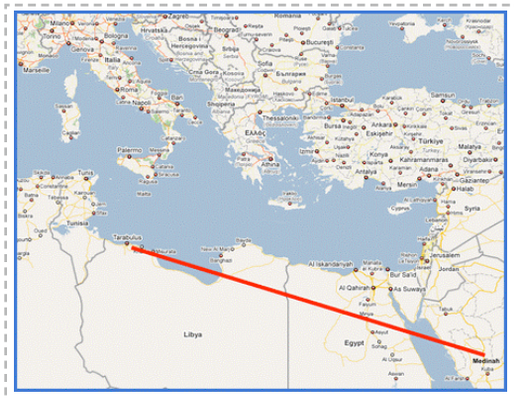
Private Air Flight DC3 Dakota	
Date	Mid 60's
Type	(One) engine failure
Site	30 kms from Trapani
Passengers	26
Crew	3
Fatalities	---
Survivors	26
Aircraft type	DC3 Dakota
Operator	Private
Flight origin	Pantelleria
Destination	Trapani

✓ *2.3. Private Air Flight DC6*

In the mid 80s', private air flight DC65, on route from Tarabulus (Lebanon) to Medinah (Saudi Arabia) reported cabin distress during the flight. It landed safely and in time at destination. The private flight carried 45 Muslim pilgrims, 2 pilots and 3 flight attendants. According to the then-captain report, approximately 30 minutes from departure, one flight attendant rushed to the cockpit urging the captain permission to use the fire extinguisher. Alarmed by the unusual request, the captain sent the second-pilot to the cabin to check the situation: a passenger had lit a small camping stove in the aisle to prepare his tea...

40 This case-study was analysed during an interview with a former civil aviation captain with a 50 years long experience in the field of aviation who is currently retired and acting as civil aviation security consultant for various Italian airports.

50 This case-study was analysed during an interview with a former civil aviation captain with a 50 years long experience in the field of aviation who is currently retired and acting as civil aviation security consultant for various Italian airports.



Private Air Flight DC3 Dakota	
Date	Mid 80's
Type	Cabin crew asks permission to use fire extinguisher
Site	---
Passengers	45
Crew	5
Fatalities	---
Survivors	45
Aircraft type	DC6
Operator	Private
Flight origin	Tarabulus
Destination	Medinah

✓ *2.4. Preliminary Considerations On Group Dynamics*

The three cases described above allow us to draw some preliminary considerations on group dynamics on board of an airplane in situations of distress. At first glance, the *cultural variable* appears to be a key factor for the analysis of group dynamics. Although such variable shall be considered together with other factors to avoid too easy stereotypes, "groupthink" and social conformity are mostly produced in a general way and both have similar patterns independently from cultural connotations (Janis 1971 : 84 – 90) The traditional Japanese values of discipline, respect for the authority and self-control clearly came into play in the first case. Informed by the captain about the situation and the impossibility to perform an emergency landing, passengers did not panic but followed cabin crew instructions and even wrote messages to their families, storing them in camera-film boxes so to preserve them from the imminent airplane crash. The second case presents a very different situation where the Italian individuality, lack of discipline and trust in formal institutions led to a state of chaos, which could have dramatically deteriorated an otherwise unproblematic situation. Finally, the third case is a good example of the difficulty to mediate between consolidated traditional community routines of primary groups and the modern organisational needs of secondary groups.

Secondly, all three cases seem to indicate that the emergence of a distressful situation is in itself the main factor turning the aggregate of passengers into a group. According to classical sociological theory, a group is defined as a dynamic whole composed of individuals perceiving each other as more or less interdependent on some specific aspects (Lewin 1965). In the cases at hand, a group was formed when 1) passengers act towards a common goal and its achievement is held beneficial to all of them; 2) passengers share similar knowledge about the situation; 3) there are not dramatic inter-individual differences about the capacity to achieve the goal; 4) passengers share the similar need to overcome their common isolation from the rest of the society (i.e. people not on board).

Thirdly, the analysis of the three cases showed that groups formed as reaction to an emergency situation on board of an aircraft are characterised by a low degree of internal organisation and are vertically structured. This means that groups are structured mostly in terms of dominance-submission and that inter-relations refer to the power dimension rather than to trust or affection.

Although with "group dynamics" we usually mean the whole of processes generating within a group, focusing on the groups of passengers as just identified, we rather refer to the ongoing interaction of powers within a group eventually leading to a given equilibrium. From this perspective, the analysis of group dynamics is focused on the "field" where each individual acts and where inner and outer elements and events are closely interacting and influencing each other (Lewin 1965). In other words, each passenger interacts with the group, influencing it and being influenced by it at the same time. Such interplay holds valid for any other group of which individuals are part in their daily life. The two-way (individual-group) influence, moreover, is not only directly dependent on the physical contacts among group members: there is a specific psychological dimension reciprocally linking individuals to the group even when they act outside it (this explains, for instance, the relevance of the cultural dimension in the cases described above).

From this perspective, classical group theory distinguishes three types of group dynamics developed on power relations and which can be used to describe group dynamics on board of an airplane: 1) Authoritarian leadership; 2) Democratic leadership; 3) Anarchic leadership. The figures below graphically represent the three types of group dynamics (Brown 1990: 69-107).

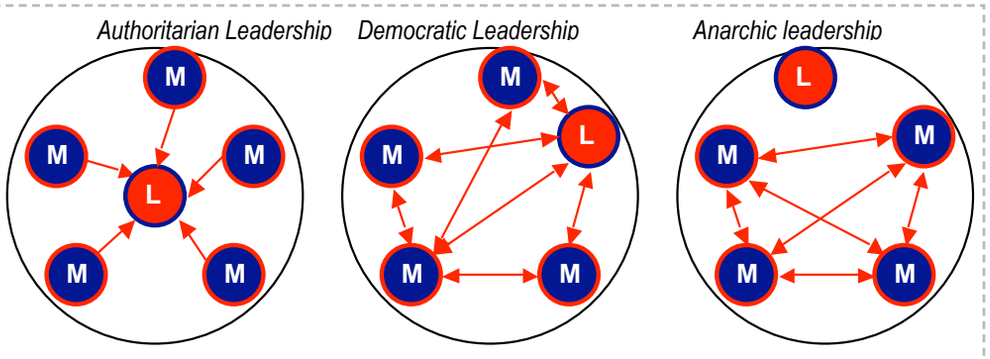


Figure 1 – Types of group dynamics
Source: Brown 1990 : 69 -107.

When an *authoritarian leadership* emerges, group members a-critically follow the leader giving up part of their creativity, capacity and independence. Such internal dynamic is usually unproductive and would lead a group to its implosion. However, in cases of emergency, high risk and danger the role of the leader is key due to the effectiveness of its decisional capacity.

A *democratic leadership*, on the other hand, stimulates groups decisions based on consensus building and participatory decisional processes. Group members cooperate with the leader towards the realisation of a common goal.

Finally, an *anarchic leadership* emerges when groups are short-term aggregation instances. Participation to the decisional process is *over*-democratic and the group leader is unable or unwilling to solve eventual conflicts, internal contrast or to give specific indications on how to face external threats (Lewin et al 1939). Notably, all three types of group dynamics focus on the

role of leadership as key aspect regulating interactions among group members and between the individual and the group.

Interpreting the three cases above in the light of the three types of group dynamics a fourth set of preliminary considerations can be drawn. Passenger groups share characteristics specific to all three types: they are extemporaneous as groups characterised by anarchic leadership; they are based on consensus and democratic legitimisation of specific rules (i.e. on-board safety conducts, etc); when emergencies occur they (are supposed to a-critically) follow the instruction of a charismatic leader (i.e. cabin crew, pilot, etc).

The following model graphically depicts groups dynamics on board of an airplane. Passengers (i.e. group members "M") are mainly concerned with their own flying experience. They interact only sporadically with other passengers (anarchic behaviour) and relate with the cabin crew (i.e. leader) in an orderly fashion: they legitimise the cabin crew and the standard aviation rules; if needed they dialogically interact with the cabin crew to accommodate their needs (democratic behaviour). In such a situation, extemporaneous groups may form because of social relations antecedent to boarding (i.e. large family groups, organised tourist tours, football supporters, etc). When emergencies occur, individuals tend to become group members horizontally joining the group of passengers at risk. The cabin crew (should) immediately claim(s) an undisputable leadership which manages the orderly organisation of the group and of its workings.

The leadership role of the cabin crew is key to structure social relations efficiently according to the overall goal (as envisaged by regulations, procedures and ultimately by the pilot). In the lack of a strong leadership, as suggested by classical sociological theory (Granovetter 1974), it would be rational for individuals to act independently disregarding any cooperative approach. The reason for this being that passengers do not share any social relations with any other passengers and thus cannot foresee how fellow passengers would behave. Cabin crew leadership is therefore necessary to provide a common approach and to oblige passengers to assume a cooperative behaviour. Moreover, when lives and goods are perceived as endangered, social pressure and conformism themselves may work as powerful factors orienting group dynamics.

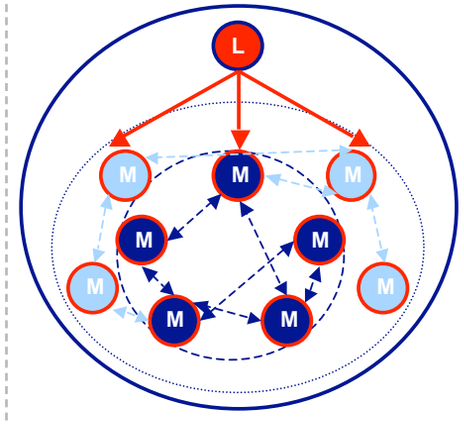


Figure 2 - Group dynamics on board of an airplane
Source: own elaboration

Despite their analytical value, modelling efforts fall short in representing the high degree of complexity of social reality. In the case at hand, it cannot be underestimated that a flying airplane is a most peculiar environment within which extremely heterogeneous social systems are formed; thus, extreme risk and rescue events develop complex scenarios.

The role of group dynamics is, therefore, crucial. It deeply influences the ability to take correct decisions; in other words, in the real world, to reach safety and to manage risks does not entirely depend on the compliance with

abstract rules and procedures. Other factors may act upon group dynamics and shape the social behaviours, such as status relations, individual personality of the involved participants and the cultural elaboration of the event, which may vary according to national, geographic, religious variables (Brown 1990: 111, Asch 1956). Before depicting effective management techniques of group dynamics and decision making in an emergency situation, it appears necessary to focus on the individual characteristics of passengers (i.e. cultural values and orientation, strong feeling of group membership/belonging prior to boarding, etc) key for understanding the overall complexity of group dynamics. These aspects are considered from a psychological perspective; namely, the impact of individual differences on people's experience of the travel process.

3. Experiencing Flying: Psychological Determinants of Passengers' Stress

Air transport is considered worldwide to be one of the preferred methods of travel. On the other hand, it is considered also to be a way of travel characterised by an impressive list of both minor and more serious potential health risks. Since stress is related to ill health via its effect on the body, it is important to recognize potential sources of psychological stress in relation to air travel. These can include: the fear of the physical sensations of being airborne, take-off and landing, and anxieties related to relatively minor hassles on the ground, due to airport delays, airport congestion, and security procedures. More recently, the unpredictable phenomenon of air terrorism, including hijack and bomb threats, coupled with widespread media reporting of events, has made air travel appear potentially more risky, with a marked public reaction (Swanson, McIntosh 2006). Immediately after September, 116 the number of air passengers fell dramatically in the world and especially in Europe, having an increase only a few years later[7]. Moreover, for the majority of travellers, the previously glamorous image of air travel has been replaced by perceptions of threatened disaster, airport delays and restrictions, poor on-flight conditions and potential ill-health as a consequence. All of these factors can influence passenger anxiety. The poor on-flight conditions appeared as a consequence of the need to lower the budget of the air travel and the launch of the low cost air companies with their immediate and successful expansion[8].

6) See Appendix A for data on civil aviation travel past and present trends.

7) In addition to increasing perceptions of risk of air terrorism, more media coverage has been given in recent year to the potential health risks of flying, including the potential for deep vein thrombosis (DVT), cardiac problems, infection risk (e.g. SARS), and passenger disruption (air rage). The world's famous and most viewed news channels and newspapers focused their news on the potential health risks and the need to inform the passengers of the consequences of flying. For example, the BBC, in 2001, highlighted the news about the UK's High Court writs issued against two major airlines over claims they failed to warn British passengers of the potential health risks from long distance air travel. The test cases against the airlines involved passengers who developed deep vein thrombosis (DVT) after long-haul flights. According to BBC at that time in Australia, 2,700 passengers were seeking damages from airlines after suffering blood clots. (http://news.bbc.co.uk/2/hi/uk_news/1625309.stm, retrieved on 6.04.2010). What's more, the airlines offices are claiming that there is no scientific proof of any connection between DVT and long flights. In addition to that, the World Health Organisation organised a two-day conference in Geneva to shed light on the potentially lethal risks posed by long-haul flights to thousands of passengers. (http://news.bbc.co.uk/2/hi/health/1214680.stm, retrieved on 6.04.2010).

8) As an example, the air company Ryanair offers the lowest prices on tickets not including snacks and meals on board, having the lowest and poorest quality of services but highlighting the number of flights on time and new opened connections. The same example is as well with the air company Easyjet, Wizzair, Germanwings, Transavia etc. Their services differ by the flight tickets' prices. The question to be asked is, do these airlines focus on the security on board and on the potential health risks for the passengers. An answer can be found in the many flight tickets offered to the passengers for just 0.00 euro without airport taxes.

From this perspective, it is necessary to distinguish various forms of stress which may determine the development of specific group dynamics. To this end, *transactional theory of stress and coping* is helpful to put emphasis on the importance of inter-relationships between sources of stress and individual factors (Folkman, Lazarus, Gruen & DeLongis, 1986).

The term "stress" is often used ambiguously by many people, the media, and in the research literature, to define both causes (i.e. sources of demand, hassle, or pressure) and outcomes (i.e. impact of these sources on the individual). The ability to distinguish between cause and outcome is important for those who treat stress and it is suggested that the term "stressor" be used to describe causal factors, and "stress" to describe the psychological outcome. It should be noted that stressors can be both physical and environmental or psychological – and objective or subjective. An individual enjoyment of travel depends upon a predisposition to cope well with a variety of physical and psychological stresses (Locke & Feinsod, 1982). This suggests that under the same stressor conditions, individuals will cope differently according to their own characteristics and resources. These can include coping resources such as skills and experience, support from others, or demographic characteristics such as age, gender, socio-economic circumstances or health, which might mediate or moderate travel outcomes.

Transactional theory suggests that the impact of different stressors on stress outcomes will vary according to the individual's appraisal of the seriousness of the threat, and their own ability to cope with it. Once an individual has made a primary appraisal of the problem, a secondary appraisal will assess whether current coping resources are sufficient, if not, the individual will experience psychological distress, or stress in some form.

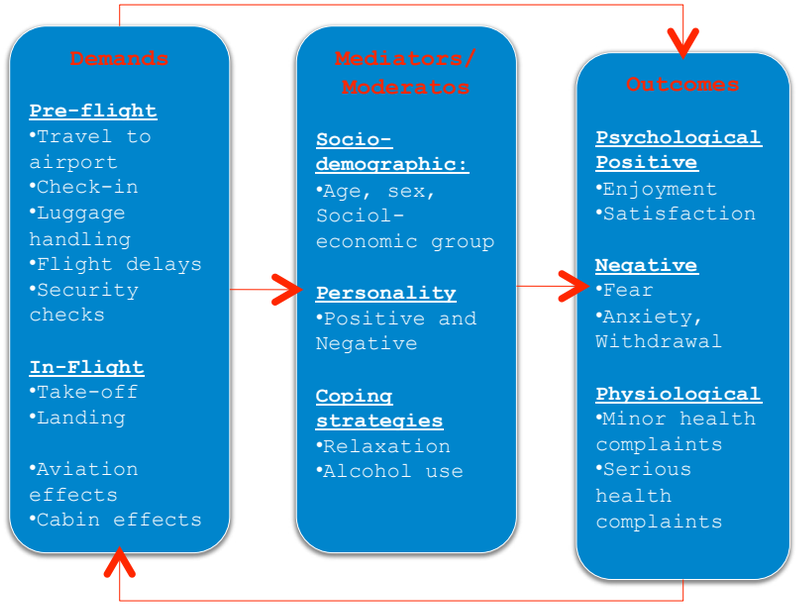


Figure 3 – Transactional theory model
Source: Bor, R. & Hubbard, T. (2006). Psychological Assessment and Reporting of Crew Mental Health, Aviation Mental Health, Ashgate Publishing

The focus is on three components of the transactional model: 1) potential objectively measurable sources of stress in the air travel process; 2) possible outcomes for passengers in terms of physical and mental wellbeing; 3) possible mediators or moderators of this relationship, including socio-demographic factors, individual psychological differences, and coping strategies.

One large scale UK study of intended travellers in the general public (McIntosh, Swanson, Power, Raeside & Dempster, 1998) revealed the extent to which different aspects of the air travel process caused respondents to feel anxious. Items are sequentially ordered from travel to airport, to baggage reclaim as shown in the Table 1.

Table 1 – Passengers anxiety factors

Item	***Never***	Sometimes, Often, Always
	No. (%)	No. (%)
Travel to airport	166 (70.3)	70 (29.6)
Check-in	165 (69.9)	71 (30.1)
Flight delays	115 (49.6)	117 (50.5)
Transfer	156 (67.2)	76 (32.8)
Waiting in lounge	172 (72.9)	64 (21.1)
Boarding flight	182 (77.1)	54 (12.9)
Take-off	137 (57.8)	100 (42.2)
During flight	149 (63.4)	86 (37.6)
Landing	133 (56.6)	102 (43.4)
Baggage reclaim	141 (60.0)	94 (40.0)
Customs	154 (65.3)	82 (34.8)

Source: Bor, R. & Hubbard, T. (2006). Psychological Assessment and Reporting of Crew Mental Health, Aviation Mental Health, Ashgate Publishing

Although this study was not able to establish which particular aspects or components of situations were stressful, a tentative analytical approach to the reported results seems to point out the following: 1) incontrollable (by passengers) changes in the flying patters (i.e. take-off, landing) provoke uneasiness among passengers; 2) when passengers not knowing each other need to interact (flight delays, baggage reclaims, etc) are more stressful situations then when interactions are more limited.

The transactional model provides a useful framework for interventions to alleviate such stress and anxiety by identifying stressors, and raising awareness of possible outcomes and potential mediators/moderators of stress. With appropriate warning, advice and precaution the traveller can adopt personal strategies to anticipate and minimise personal health risk. Good pre-travel health advice from health professionals may help travellers to anticipate problems and develop effective coping strategies. Additionally, the air travel industry could assist passengers to more accurately and realistically identify risk, and take appropriate precautions. Similarly pre-flight, in-flight and post-flight stressors could be identified and reduced by improved orga-

nization and communication by airlines.

Not all passengers react in the same way to stressors in the air travel process. Many factors will affect one overall experience of stress. Many anxious travellers, for instance, resort to alcohol consumption to combat stress and help them through the journey, but over indulgence by some may result in aggressive behaviour and air rage (Greist, 1981).

While some studies have evaluated differences in stress outcomes between male and female travellers, many fail to report gender differences. It is generally found that women tend to experience more stress, worry, anxiety and fear than men (Swanson, McIntosh 2006). This is in line with the greater prevalence of anxiety disorders in women in general.

Fears and phobias are more common in children that older people (Locke & Feinsod, 1982), and air phobia affects more children than adults. In addition, the potential for air accidents or terrorist events may have more impact on younger travellers (Gauld et Al., 2003). They may also have different perceptions of personal risk, due to a lack of knowledge or inability to put risks into a rational context.

Earlier retirement, increased wealth and potentially young life-span mean that many more elderly passengers now undertake air travel. Older people are more anxious about air travel than both children and working-age population groups. In addition, older travellers may justifiably exhibit greater anxiety about possible in-flight health problems, particularly in relation to cardiovascular illness and DVT, muscular-skeletal problems, and susceptibility to infection. However, this whole area is still under-researched in relation to stress, anxiety and air travel.

People who travel by air frequently, such as businessmen, may have reduced risk perception due to their personal experience of continued safe air travel.

Table 2 – Anxiety by passengers' individual characteristics

Passengers' characteristics	***stress, worry, anxiety and fear***
Gender	
Male	*expressing less*
Female	*expressing more*
Age	
Young	*common manifestation; affecting air phobias more; different perceptions of personal risk; more impact from accidents and terrorist attacks*
Old	*more anxious about possible in-flight health problems*

Source: Bor, R. & Hubbard, T. (2006). Psychological Assessment and Reporting of Crew Mental Health, Aviation Mental Health, Ashgate Publishing

Dispositional characteristics and current psychological state are likely to affect perceptions of the stressfulness of air travel, and individual outcomes and certain personality traits may be related to involvement in air rage incidents. Common traits and features include a difficulty in managing appropriate boundaries and impulsivity, and a tendency to act quickly without due consideration of possible consequences (Heller, 2003).

Discerning potential stressors is key to elaborate procedures and protocols aiming at reducing passengers stress. This, in turn, is key to reduce the degree of complexity of social reality on board of an airplane, thus, potentially facilitating the management of group dynamics within such context.

Once psychological, individual passenger-related factors are identified, it is necessary to focus on the social network dynamics, which can be activated when facing a stressful and disruptive event and –more precisely – to attempt to elaborate "a function of decision making" in a rescue situation on board of an airplane.

4. Towards a Function of Decision Making in a Rescue Situation On Board of an Airplane

The key role of cabin and cockpit crew members in managing a rescue situation on board of an airplane was elsewhere highlighted. Human beings have an enormous capacity for sensing information, the decision-making stage of the process consists of just one single channel, being time shared between the different inputs. While one piece of information is being processed, the other are held temporarily in the short-term memory store, from where they are retrieved at the appropriate time. The storage and retrieval operation can be affected by many factors and this gives a source of potential error.

The decision-making process has two major components. The rational part involves conscious thought and choice, whereas the intuitive part of the process utilises long-term memory stores. Decision making is a step-by-step scientific process which is sometimes referred to as the judgment concept. The stages in making a decision are: 1) diagnosis and definition of objective; 2) collection of information; 3) assessment of risk: development and evaluation of options; 4) decision of appropriate course of action; 5) implementation; 6) review and evaluation of consequences; 7) feedback.

Decision-making is the capability to properly choose responses in complex situations where several reactions are possible. It is a major component of situational awareness, airmanship and good flying judgement (Campbell, Bagshaw 2002). The effectiveness of decision making is limited by a number of factors. These include the individual's mental model of the particular situation, the application of heuristic methods of problem solving (proceeding by trial and error to discover the solution), assessment of probabilities and the ability to recognise personal limits of workload. All these are influenced by individual personality factors such as flexibility, creativity and social style (such as dominance[9]).

9) Dominance refers to the types of psychological characters humans can have, one can project dominance towards others and one can have weaknesses and be dominated.

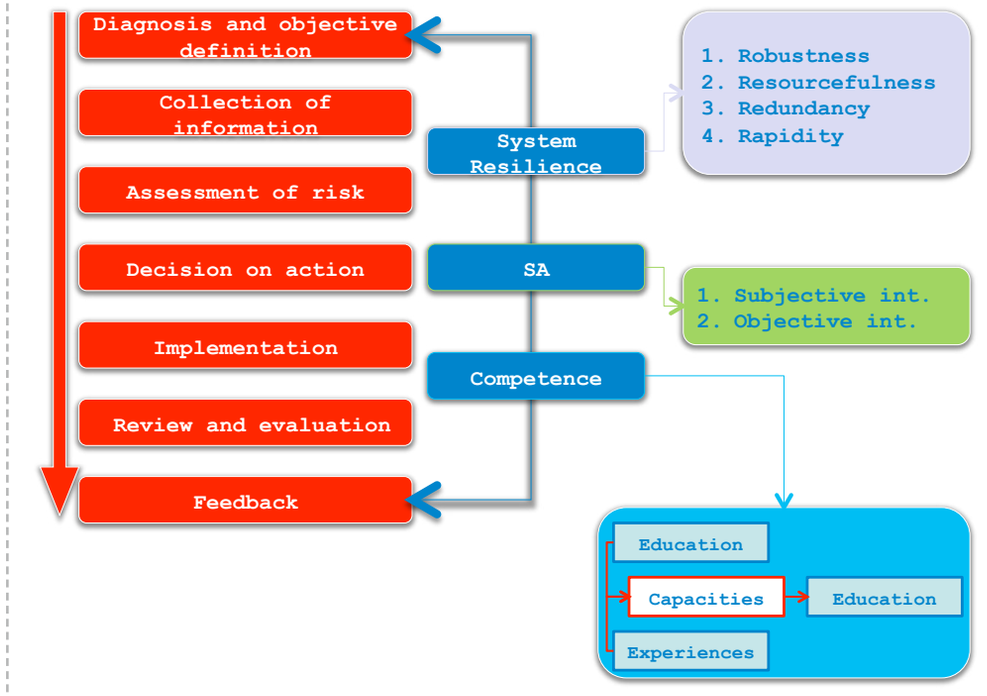


Figure 4 – The decision making process: its possible function in a rescue situation
Source: Elaboration made by ISIG

Figure 4 represents an attempt to depict the factors influencing the effectiveness of the decision making process (in red boxes). These factors are: 1) the system resilience, 2) situational awareness and 3) competence.

✓ *4.1. System Resilience*

Dynamics of learning and adaptation, which are central to the understanding of the complexities of system/environment relations in system theory, could be used to further interpret the degree of collaborative relations between sectors and decision makers in network based systems of governance. An important concept in this regard is the resilience of social systems that increase their complexity by minimizing possibility of failure.

Resilience is the "capacity to cope with unexpected dangers after they have become manifest, learning to bounce back" (Wildawsky, 1971) and a stronger resilience reduces the damages suffered by a social system, measured in terms of lives lost, material damages, negative impacts on communication flows and time to recovery, that is to say the restoration of social systems and institutions to their normal, pre-disaster level of functioning.

Extreme events that challenge the resilience of a social system often occur at the interface between natural, social and human (bio-psychological) systems and are generally interpreted as "disasters".

Box 1 – Measuring resilience

To identify and possibly measure resilience, system theory has identified four general properties that can be applied for all types of systems and the elements that compose those systems. These properties are:

1. Robustness: ability to withstand the forces generated by the hazard without loss or deterioration of normal functions
2. Resourcefulness: capacity to apply material, informational and human resources to repair disruptions when they occur
3. Redundancy: the extent to which systems or elements are able to satisfy their performance requirements in the event of loss or disruption that threaten functionality
4. Rapidity: the ability to contain loses and restore system functions in timely manner

The resilience of a social system does not refer to the ability to avoid "disasters" – which is, however, important to the evolution of the system – but to the capacity to understand and manage extreme events by understanding, anticipating, preparing for and responding to them. Therefore, fostering resilience of social systems – even at micro-level of interactions – sets the stage for new types of partnerships and collaboration among collective and individual social actors (Comfort 1990; Quarantelli, Dynes 1977)

Extreme events and the connected disaster scenario can work as an opportunity for the system to develop a new set of interactions where high levels of cooperation and collaboration among organizational and community actors can co-exist. (Even when there is no clear policy or guidelines available to the organizations or the community actors, or when the extreme dynamic situations do not make it easy to figure out responsibilities and procedures.) In such situations, trustworthiness and the ability to mobilize social capital can work as crucial factors to create consent and to suspend ongoing conflicts and disagreements. This way, networked approached among organizations and community actors are established to meet the urgent needs and to begin the recovery process. Effective responses and recovery operations require collaborations and trust between different actors at all levels and between the different sectors (public, private, non profit). Ongoing collaboration between different types of agents, even when it occurs outside defined guidelines or protocols, has the effect to raise trust and to increase the resilience of a social system.

Raising trust and increasing resilience during and after is, therefore, essential for the positive outcome of an extreme event: this is the underlying rationale of all emergency procedures. But what are the possible reasons why in some cases this happens and in others it does not? Namely, the ability to mobilise social capital and to promote cooperative behaviours is probably determined by other variables than the bare capability to inform or perform procedures. It may depend on cultural factors and informal skills (i.e. empathy or intuition of the decision makers). Moreover, it implies an understanding of the level of trust between passengers and the "formal institutions" represented by the airplane company, the cabin crew, etc. Therefore, the issue revolves around the possible emergence of cooperative forms of behaviours and the existence of

positive attitudes of actors towards the solution of a risk situation.

From this perspective, it is necessary to address the question of how do the individual (informal, private) and the collectivity (formal, organised) concretely interact in an extreme situation of risk (Kapucu 2005 : 35). The analysis of these interactions is extremely important to understand the limits of standardized procedures in contexts of somehow unpredictable collective behaviour. Procedures applied by the responsible institutions to manage a disaster and to cope with an extreme scenario may be challenged by the role of non-organized collectivity (i.e. groups of passengers, spontaneous associations) and other organizations, which are not explicitly dedicated to the management of disasters (i.e. members of formal organisations travelling on the plane, such as firemen, policemen, etc.).

Efficiency of responses depends on the ability to cooperate and collaborate. It is a skill that can be learned by organizations and this is what dynamic network theory and complex adaptive systems theory can contribute to explain. However, those theories sometimes fail to explain how building networks of effective action to tackle emergencies can be difficult in very dynamic situations of the "real world". As a matter of fact, institutional responses and official organizational plans of actions (i.e. security procedures and protocols) represent only one side of the collective behaviour in extreme disaster conditions. Additionally, it is important to focus on the social processes that fall within non standardized procedures and depend on the interactions between official emergency agencies (i.e. the crew) and other non-crisis oriented formal and informal organizations (Kapucu 2005: 36–38).

In the case of disasters, the border between organizational and social behaviour appears more blurred in complex and turbulent environments, organizations frequently develop formal or informal relationships in order to work together to pursue shared goals and reach mutual benefits. This model of governance is replacing in some cases the bureaucratic hierarchies, especially when the challenges are quite complex, like in the case of an extreme event. In terms of networks between organizations and between organizations and other subjects, one may observe a more horizontal style of management in which leadership is shared and decisions are more connected to the values of expertise than to roles and positions: the multi-faced nature of the complex problems connected with extreme events makes them extremely difficult to conceptualize and analyze, thus they become immune to simple solutions. That requires flexible and adaptive structures both based on organizational patterns and more spontaneous forms of behaviour. Thus, there is an issue of balance between differentiation and coordination among the actors to successfully adapt to the rising environmental complexity.

✓ *4.2. Situation Awareness*

It is assumed that an effective decision making depends on the ability to balance between differentiation and coordination among actors. As a result, the pursued balance may work as a crucial factor of successful adaptation, by increasing resilience and promoting cooperative behaviours (Dunn, Lewandowsky, Kirsner 2002: 719–723). In a dynamic environment such as a flight, an effective decision-making is highly dependent on the situation awareness (SA) – a constantly evolving picture of the state of the environment.

SA is formally defined as a person's perception of the elements in the environment within

a volume of time and space, the comprehension of their meaning and the projection of their status in the near future. Thus, SA encompasses not only an awareness of specific key elements in the situation but also a comprehension and integration of that information in the light of operational goals along with an ability to project future states of the system (Endsley, Kaber 1998: 43–48).

The operative comprehension and the ability to project future situations are particularly critical to the effective functioning in complex environments such as that of a flying airplane. Statistics of failures in decision-making are often cited causal factors in aviation accidents but a high percentage of the accidents is actually represented by errors in situation awareness. Namely, the cabin crew made the correct decision for their picture of the situation but that picture was not correct (Jones, Endsley 1996: 507–512; Endsley 1995: 32–64; Stanton, Chambers, Piggott 2001; 189–204).

The earliest discussion in situation awareness, as well as the early scientific works on SA and its measurements originated in the fighter aircraft domain, going back as far as the First World War. However, the use and the application of the term have rapidly spread to other domains (cars, railways, sports, enterprises, etc.) for the most prominent drive of this trend has been technology. As a matter of fact, the possibility to face an extreme situation and the subsequent need to enhance the operator situation awareness has become a major design goal for those developing operator interfaces, automation concepts and training programs in a wild variety of fields where decision-making could bring about risk scenarios. This is the case for many sectors both public and private where *robotization* and technological advancement set the stage for the challenges of a new class of technology in the mid 1980s and mostly in the 1990s. These sectors include aircraft, air traffic control, power plants, banks, sensitive public administration database and advanced manufacturing systems (Endsley, Garland 2000).

In the case of aviation, the emphasis shifted progressively to the creation of a new class of tools to help people to perform their tasks, largely those physical in nature, as situation awareness is eventually defined in terms of the goals and decisions tasks for an operator's job. Thus, considering the advancement of the computer age and the information technology, the tools provided to the operators in the aircraft are no longer simple but increasingly complex, focused on elaborate perceptual and cognitive tasks. The pilot, as well as the air traffic controller, has to perceive and comprehend a dazzling array of data which is often changing very rapidly. The operators have then to process and sort the needed information in a complex set of data, which in themselves do not provide the information: today's technological systems are capable of producing a huge amount of data about the situation on the airplane, but obviously cannot help in finding what is needed when it is needed. Therefore, to enhance the possibility of a correct situation awareness in a complex and dynamic environment such as a cockpit one should consider how well the technological devices, particularly the systems design, support the operator's ability to get the needed information under dynamic operational constraint.

Considering such concerns with reference to the general definition of SA, one should put the SA in a crucial position of the decision making process. Specifically, the SA would stay between the technological system based data production and the effective decision act. This for the following two reasons. First, the perception of environmental elements describing the situation is the basic step and some misperceptions in this phase would eventually lead to the formation of an incorrect picture of the situation. Either in the case of shortcomings in the electronic systems or of problems with cognitive processes, the misperceptions of needed information eventually may lead to wrong decision making.

Secondly, SA is a construct that goes beyond mere perception as it encompasses how people combine, interpret, store and retain information. Therefore, as pointed out by Flach (1995) "the construct of situation awareness demands that the problem of meaning be tackled head-on. Meaning must be considered both in the sense of subjective interpretation (awareness) and in the sense of objective significance or importance (situation)". In other words, an operator acting in the cockpit has to be able to derive operationally relevant meaning and significance from the data perceived.

Eventually, operators might show the ability to project from current events and dynamics to anticipate future events (and their implications). This ability is a mark of experience and skilled approach for it allows operators that rely on future projections for timely decision making. Thus, both the perception of time and the temporal dynamics associated with events play an important role in the formulation of SA, thus enabling projections of temporal sequences and consistent decision making.

Accordingly, situation awareness is represented as the main precursor to decision making because the operators can decide what to do about some extreme situation and carry out the necessary actions basing their choice on the representations they build up. Therefore, SA can be also depicted as the operator's internal model of the state of the environment. Consequently, SA represents a separate stage in the process of decision making (between the system and the decision) and is not combined in a single and integrated process with the act of deciding. The main reason is that it is entirely possible to have a perfect situation awareness and still make an incorrect decision, as the first does not determine the second one. Conversely, poor SA does not preclude some sound decisions based on intuition, luck or external intervention (other people operating in the cabin).

Situation awareness is derived from all the various sources of information available for the operators: visual, oral, tactile, olfactory or taste receptors. Thus the information provided through the system and its operator technological interface is not the only source of SA. In many domains, operators may be able to directly view and hear information from the environment itself.

✓ *4.3. Competence Building: Cockpit Crew's Assessment, Training and Selection as Factor*

There are a number of situations where the outcome of a flight incident or an accident could have developed quite differently, depending on the decisions and actions of the cabin crew. A number of regulations now specify what cabin crew should accomplish and have been added to the original requirements. The focus on duties on board has changed from serving to safeguarding the passengers by providing leadership in case of emergency – although the popular image has not caught up with this (Hackman 1986).

Significant differences in pre-training attitudes between airlines and between crew posi-

tions within each indicate that different organizations have developed their own cultures and norms despite operating in a regulated environment that stresses standardization. Although not depicted here, highly significant differences in attitudes and observed behaviour have also been found between aircraft fleets. Although diminished, the fact that differences persist after the initial awareness training is evidence that cultures and subcultures are difficult to change. From a theoretical perspective, it seems unlikely that individuals who hold divergent views regarding how individuals and crews should function can form optimally effective teams (Helmreich and Wilhelm, 1991).

Each airline has its own specific model when selecting flight attendants[10] focusing on a number of qualities and experiences which are held being the basis of the capacities and skills needed as a flight attendant. Most skills and capacities are, however, trainable; although the true test of proficiency is undertaken when these skills are assessed under actual or simulated emergency conditions. To identify who is therefore best suited in a selection process is rather complex: besides skills and capacities, there is also a personality dimension to include in the assessment. The task is therefore to determine to what extent the person's personality helps or hinders in utilizing their skills under pressure. Between the skills and effective competence is a personality filter which is either able to reduce the output of the skills or able to enhance them.

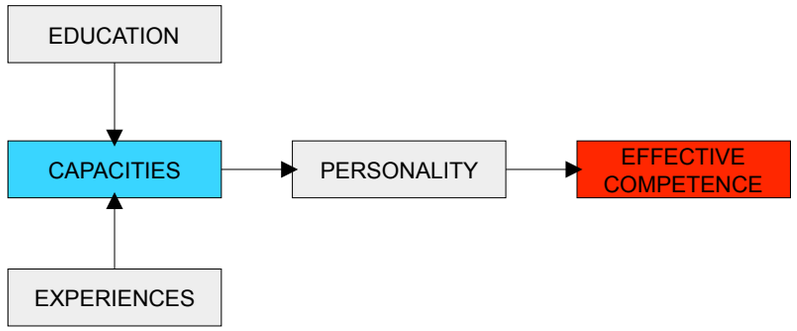


Figure 5 – Effective Competence Model
Source: Bor, R. & Hubbard, T. (2006). Psychological Assessment and Reporting of Crew Mental Health, Aviation Mental Health, Ashgate Publishing

A flight attendant with accurate basic skills and capacities, who does not possess the self-esteem to trust his/her correct observation, must be considered to be less effective or competent. A reliable process should strive to assess the effective competence of the applicants and not only their capacities and skills. This does not automatically imply that airlines should look for a certain personality, but rather dynamically evaluate the influence each candidate's personality traits have on their capacities and skills. There is a large range of factors and attributes airlines emphasise in their selection of flight attendants. Examples of typical requirement dimensions, covering education, experience, skills, personality characteristics and social competence, are:

10) Typical criteria include suitable age, height, weight, sight, hearing and other physical factors related to circumstances and limitations in the cabin environment. Educational background is typically focused on communication and language skills. An ability to swim is also necessary. Professional experience from the sector providing services (i.e. waiter/waitress) or nursing are often considered as an advantage.

value of education, value of experience, verbal ability, language skills, judgement, personal appearance and health, personal maturity, panic tolerance, self-esteem, independence, self-knowledge, empathy, responsibility, social flexibility, cooperative ability, and value of motivation.

While pilots[11] focus on flying the aircraft and communicating with other professionals when an incident occurs, flight attendants have to manage both themselves and the passengers. Both on flight deck and in the cabin, panic reactions would be disastrous. In a selection process, it is a serious challenge to make a valid prediction of each applicant's tendency to be seized by panic in a given situation. Panic situation is not a single-dimensional, clearly defined factor, so the assessor has to capture the whole dynamic complexity behind this phenomenon. Ego-strengths, emotional stability, absence of severe traumatic experiences, a flexible defence organization and a strong drive are factors that are considered as important for a higher panic tolerance. By collecting data from different sources (tests, interviews) and different themes (background, present life, here-and-now) and comparing them systematically, a valid assessment of the panic tolerance – and other variables – is possible to attain.

Despite the importance placed upon cabin crew's psychological wellbeing, a better understanding of the complex processes involved in the management of physical and psycho-social work related stress is clearly needed before one can begin the course of appreciating cabin crew mental health. Airline cabin crew are in many ways a unique occupational group in terms of their irregular work patterns, unique set of job demands and lifestyles. The working environment of the modern commercial aircraft and the conditions in which airline cabin crew operate have been largely ignored in the industrial relations literature, and organizational psychology. In a review of existing literature on the health, safety and working conditions of airline cabin crew, a number of health and safety risks, about which workers received little, if any, information was identified (Boyd & Bain, 1997). This includes exposure to poor air quality in cabins leading to increased level of airborne pollutants, recurring lethargy, headaches, and a range of influenza–type complaints. The literature on strategies of coping with threats to ill mental health suggest that any form of disruption to the psychological system is self limiting as the person will find a way to return to a stable state (Moos & Schaefer, 2004). Once confronted with physical or psychological threats, the individual is thought to engage in three processes that constitute the coping process. Firstly, at the initial stage of disequilibrium, the person initially appraises the seriousness and the significance of the threat (cognitive appraisal). In keeping with the existing literature, such threats could be classified as either physical/biological such as jet lag and fatigue (Caldwell, 1997; Price & Holley, 1990; Sharma & Schrivastava, 2004), psycho-social including low self control (Laura et al., 2004), or disrupted social/personal relationships (Bor et al., 2002; Lauria et al., 2004; Levy et al., 1984; Rigg & Cosgrove, 1994). Secondly, the individual utilizes adaptive tasks as part of the coping process, and these can be seen as either general tasks or those specific to the threat itself. Thirdly, the person engages in a series of coping skills that are accesses to deal with the crisis. These coping skills can be divided into three categories: 1. appraisal-focused coping involving attempts to understand the threat and represent a search for meaning; 2. problem-focused coping such as confronting the problem and reconstructing it as manageable, and; 3. emotion-focused coping involving management of emotions and maintaining equilibrium (Caldwell 1997).

11) For more about the important role of the pilots as the highest authority on board see Del Bianco, D. & Andeva, M. (2009). *Chapter: The Criteria for Emergency Response.* Compliance of the Italian civil aviation system within the European Union guidelines, AETHER Research Paper.

5. Managing Group Dynamics: The Carrier Perspective

The analysis of relevant theories, case-studies and relevant regulation conducted so far, pointed out: first the key role played by the cockpit and cabin crew in handling efficiently group dynamics in an emergency situation; second the fact that the aviation security training has the primary role in understanding the dynamics on an airplane in case of an emergency situation and when a terrorist attack is identified. As part of the research process, I.S.I.G. undertook a series of interviews with training authorities/institutes and private carriers around Europe in order to identify the role of the training specially in a situation where the communication between the cabin crew members and the passengers is having the main and significant role.

✓ *5.1. Selection and Training for the Management of Group Dynamics: The European Aviation Security Training Institute*

Investigating the selection and training of the cockpit and cabin crew contributes to better understand the relevance of communication during a flight, especially when dealing with an emergency situation (i.e. when there is a need of an immediate adequate reaction from the cockpit crew and cabin crew).

Psychologists may be called upon to formally assess the air crew for their suitability to fly and to submit a report of their findings to either the crew members employed or licensing authority. The psychological assessments and reporting in aviation play a major role in the aviation safety and security. These assessments are taken for three main reasons.

Firstly, at initial selection to determine whether the candidate has the necessary aptitude, personal resources, and skills to learn to fly. Secondly, at various points during their career advancement in order to assess whether the licensed pilot has the unique and specific temperament required to progress to more senior positions. Thirdly, and far less frequently, when there are concerns about a qualified and experienced pilot's mental state and the direct or indirect effect that this may have on his or her performance and ability to fly safely. Assessment may also be requested after an incident or accident (Bor, 2006). The quality of psychological reports on air crew has never been subject to a systematic study and therefore it is difficult to gain insight into the extent of their use and their usefulness. Psychologists themselves face significant challenges on their assessment of pilots.

There can be few other professionals that require such frequent and rigorous health checks as a condition of certification to work as must be endured by pilots. These are checks carried out as frequently as every six months for commercial pilots. The medical standards that have to be met by pilots are laid out by aviation authorities, and are broadly similar. These standards are considered the benchmark for determining pilots' medical fitness. The psychological requirements for medical certification state that pilots must not be suffering from any mental disorder, neurological conditions, or be dependent upon alcohol or recreational drugs. Medical and psychological assessment of pilots is by interview, physical examination and appropriate tests where indicated. The psychological examination of a pilot is normally requested by an authorized medical examiner, employer, licensing authority or legal counsel. The assessment is conducted in order to determine whether the individual currently suffers

from any of the excluding psychological problems.

There are three major forms of selection of pilots which aim at different purposes.

The first is selection for pilot training, usually referred to as *ab initio* selection. Its primary function is to establish the chance of success in completing the training program and to inform the candidate and the school in order to avoid high costs of failure. The emphasis is on psychological factors required for effective learning, adaptation to the school environment and the specific world of aviation, and the psychomotor and cognitive skills implied in flying. Selection for training usually happens once in a pilot's career.

The second form is *selection for employment* by an airline or another commercial or military operator. Here, all candidates have a license to fly a particular type of aircraft and at least some degree of operational experience. The function of this selection is to identify those who are expected to perform best according to standards set by the organization. These standards reach beyond handling the aircraft and typically include aspects such as following procedures, interacting with other crew members, and fulfilling leadership and representation roles. The emphasis is on responsible behaviour; that is, acting safely at all times, while balancing the sometimes conflicting interest of the company, the crew, the passengers, and the environment. This kind of selection may occur during a pilot's career a number of times; that is, every time he or she applies for a job with another operator.

The third form, *clinical selection*, is of a different nature. Its function is to identify signs of psychopathology among candidates as well as employed pilots, and to prevent behaviours that might endanger human life and corporate property. It is often part of a periodical medial check-up, such as required by Joint Aviation Requirements and Flight Crew Licensing in commercial aviation or similar military standards (Roe & Hermans, 2006).

From the interview taken with the European Aviation Security Training Institute (EASTI) in Brussels12, I.S.I.G. identified several crucial points in the training process. The training programme is overall designed so to comply with the latest updates on the aviation security issues in Europe, taking into consideration the EC Regulation 300/2008 of the European Union.

EASTI mainly focuses on training on response to hijacking, promoting exercises once every two years within an ICAO exercise scenario at the Brussels airport. The institute offers 12 different security courses divided into 2 categories: aviation security and basic training courses. In the period between the exercises the institute is performing ICAO workshops together with the training institutes around Europe. Apart from these security training workshops, the institute is performing workshops on crisis management, security awareness, in-flight security, airport security, crew security and unruly passengers situation with a sequence of three times per year.

12) EASTI is a joint venture between ICAO, ECAC, EC and their Member States. It is organised on a non commercial basis, whilst all income is reinvested in the development/updating of courses under the supervision of the Board. Courses are open to government officials and participants from the airport and airline Industry. Its instructors are leading experts on aviation security, generously made available by ICAO, ECAC and EU, their Member States and non-governmental international organisations including ACI-Europe, IATA, AEA, IFALPA, ERA, EEA, CLECAT, IACA and PostEurop.

5.1.1. Preparing a Simulation Exercise On Group Dynamics Management On Board of an Airplane in Case of Hijacking

During the security trainings focused on the situation of hijacking of airplanes, EASTI finds the focal point on the communication between the hijacker and the cabin crew members from one side and the cabin crew members and the passengers from other side. In the scenario where a hijacker is present there are four psychological stages to be analyzed: 1) the psychological presentation of the cabin crew; 2) the analysis of the psychological profile of the hijacker; 3) the communication between the cabin crew and the hijacker and 4) the communication between the (cabin) cockpit crew with the elite (negotiation) troops on ground.

As far as the psychological analysis of the cabin crew is concerned, the addressing point is the impact of the current situation on the cabin crew member. The first impact and impression apprising from the fact that the member is facing a perilous threat to his/her self and to the others in the cabin, is the crucial initial point of the action and reaction to the situation. The character presentation of one person has internal and external dimension. In this particular case the decisive point is to whether the internal dimension will prevail over the external dimension. There is no human being who doesn't feel or express fear and anxiety. The internal dimension is presented with fear and uncertainty of what will happen next and the external dimension is the projection of the internal dimension. As a consequence, in this kind of situation the most important aspect is how the cabin crew member expresses the external dimension of his/her fears: namely, expressing calmness, seriousness and full responsibility instead of panic attacks can give the circumstances a whole new approach.)

There is a whole discipline in the science of psychology dealing with psychological profiles like the profile of a hijacker. Having this fact in mind, the trainings in the institute analyses the possible profiles and the potential interaction of the cabin crew member and each profile separately.

Once the analysis of the external dimension of the cabin crew member and the psychological profile of the hijacker is performed, the next step is to identify the potential and best communication tools between these two characters on board. Here a great importance has been given to the science of communication and group dynamics factors.

The communication, in the last step, between the cockpit crew and the ground troops is mostly a technical issue that doesn't leave many improvisations and it is strictly described in specific protocols and rules.

EASTI has restructured the security procedures and trainings' methods and objective after a major incident at the Brussels airport during a scenario exercise as it was noted that the most significant step to overcome is the psychological stress during the circumstances of hijacking as well as the medical aspects of the situation. Having in mind that the four steps explained above are not an easy task to perform and especially to analyze and find the right action to perform, EASTI has individualized that these stages are the most fundamental points on which the highest attention should be given.

✓ *5.2. Dealing with Potential Threats On Board of an Airplane: An Air-Company Perspective. The Case of JAT Airways (Serbian National Air Company)*

I.S.I.G. conducted an interview with the Head of the JAT Airways office at the Friuli Venezia Giulia Airport, Gorizia (Italy). As an air company from a non-EU Member State, having regular lines between Italy and Serbia, JAT Airways provided the institute with examples of emergency situations as well as with past and present experiences dealing with unruly passengers and potential threats on board.

Box 3 – Jat Airways

The Society for Air Travel AEROPUT was founded in 1927, and later became Yugoslav Aerotransport [13]. In 1987 JAT was ranked 31st among the 112 international carrier members of IATA, and was ranked 10th in Europe among members of the AEA (Association for European Airlines). JAT has been a member of IATA since 1961 and of AEA since 1971. Currently, JAT Airways owns 16 planes for the transport of passengers and cargo on domestic and international lines: ten B 737-300, one B 737-400 and five ATR 72-200. The flight Academy in Vršac trains airplane staff for both JAT Airways's needs as well as for external users. The Training Centre provides training to aviation crew for various types of aircraft, control and continued training to other company employees (sales, technical crew and similar). On the other hand, the JAT Airways Aero-medical Centre – Occupational Medicine Office provides medical services to flight crew and other company employees.

Before exploring the relevant contents of the interview, it should be noted that all the offices of the air companies, for security reasons, moved from Trieste city center to the airport, having the only representation at the airport building. The reason for this transfer, as explained by the representative of JAT Airways, was the lack of security for the offices and employees in the city when dealing specially with nervous and suspicious passengers. As stated, at the airport the employees feel safer and more protected since the security at the airport is on a high level.

During the interview it was stated that security measures on board are ineffective if the chain of authorities' responsibilities is broken or does not function as it should. The international rules and protocols exist and they are fully respected, but when there is a simple and minor clash the consequences are enormous. Three actions were highlighted as most important factors for the security on board: 1) the first contact with the air company; 2) the security checks at the airports and 3) the security checks before departure.

When purchasing an air ticket, passengers have the first interaction with the air company. At this stage air companies employees may already identify the early signs of suspicious behaviour. Details that at first seem minor and unimportant, such as giving to the air company the wrong or incomplete contact telephone number, can be a signal of a passenger who can potentially cause danger once on-board. Several examples were raised during the interview referring to a number of episodes which took place at Trieste airport in the first months of 2010.

The interviewee stressed that this very first step of the flying process is an essential part of the overall security protocol. It is most important for the personnel of the air company selling

13) Yugoslav Aerotransport changed its name to JAT Airways in 2003.

the tickets or having any contacts with potential passengers, to receive the necessary training, as to acquire skills and abilities. These are necessary not only to respond to potential threats but also to analyse the situation and discover potential threats beforehand. These abilities and skills, as stated, should be part of the training process of the companies' personnel: lack of it could be identified as one of the main shortcomings of the training process.

Although JAT did not report to have experienced any major security threats in recent years, the respondent highlighted the high incidence of unruly passengers both on board and at the airport. It is often the case that passengers behaving suspiciously or problematically before departure are not admitted on board. This is often the case with passengers who should be extradited in the country of arrival. In these cases the company personnel contact the pilot asking for permission to admit on board passengers who constantly express violent behaviour and threats. The final decision rests, in fact, on the pilot judgment on whether to admit passengers freely or whether to ask for them to be accompanied by security authorities on board.

Preventing an unpleasant flight and the escalation of a potential threat situation is, therefore, the main objective of security protocols prior to boarding. Writing this process airport police plays a major role in performing – along with air company personnel – all security (i.e. formal and informal) checks.

Before departing, the cabin and cockpit crew have approximately fifteen minutes to perform the aircraft's check (i.e. security and safety) and briefing of the security procedures. These processes are performed also when the aircraft is landed and emptied. These security measures are crucial as to investigate possible threats (i.e. explosives, etc) on the aircraft, besides the passengers' checking procedures.

As far as group dynamics management on board is concerned, the following detailed process was explained by the interviewee. International protocols (which are kept confidential) are followed during the whole flight. Besides there are special protocols to deal with specific emergency situations. These protocols, which are standardized international protocols by ICAO, are kept strictly confidential and the interviewee could not explain their content or give specific references. However, it was explained that when having a specific emergency situation (i.e. dealing with an unruly passenger or potential terrorist) the cabin crew member's main role is to calm the situation down and to report immediately the state of affairs to the cockpit crew. The pilot undertakes the main responsibility in decision making. He/she is evaluating the situation, taking into consideration what was reported by the cabin crew and first-hand observation: the final decision is then taken and the air control and the security authorities on ground are contacted.

Although detailed protocols exist, as far as the role of cabin crew members is concerned, there is ample room for improvisation. In fact protocols are built upon the consequentiality of the security chain starting on the ground. However, if security failures passed unnoticed prior to boarding, protocols might not be sufficient to deal with the case at hand.

Finally, the respondent singled out the charisma and psychological assets of cabin crew members as the main factors for a successful resolution of a potential emergency situation on board. Moreover, another essential aspect is the capacity of the cabin crew to quickly perceive the complexity of the situation and the ability to report it accurately to the pilot. The respondent's opinion is that these aspects are not sufficiently covered by the training courses and manuals.

6. Insights For Scenario Building

The paper has described group dynamics on board of an airplane with a specific focus on emergency situation. Social and psychological factors were analysed so as to provide a detailed picture of group, passengers and cockpit and cabin crew conditions to be taken into consideration when managing group dynamics. We aim, here, at depicting the overall structure of the management of group dynamics in order to provide a reference framework for the analysis and evaluation of the management of group dynamics during the Aether project final live exercise.

The following figure illustrates the interaction of all relevant factors and conditions for the successful management of group dynamics.

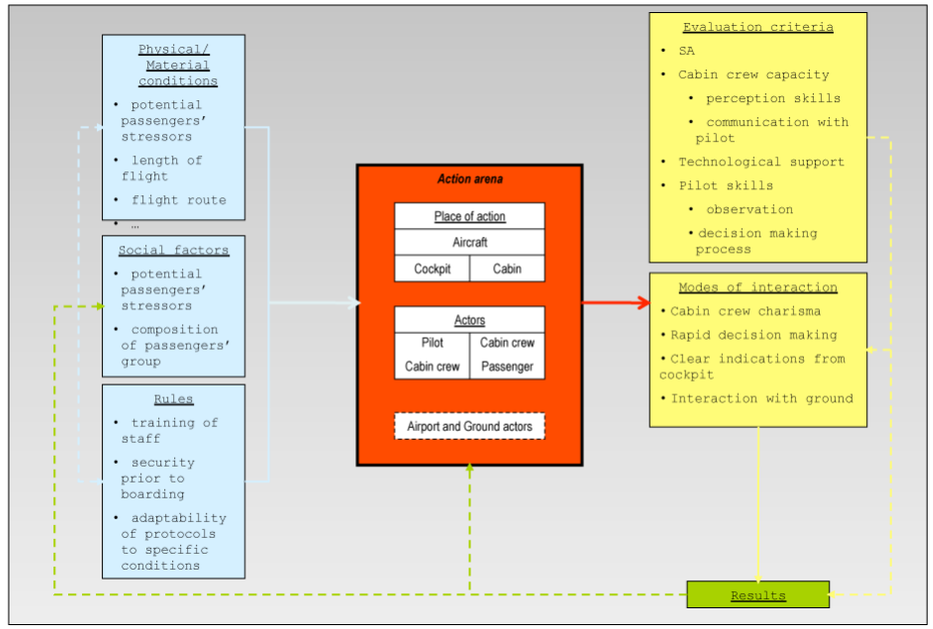


Figure 6 – Analytical framework for the analysis and evaluation of the management of group dynamics

An effective management of group dynamics in an emergency situation on board of an airplane starts on the ground. At this stage (light blue boxes) physical/material conditions and social factors should be taken into consideration by the competent personnel who need to appraise the situation and elaborate it by using available technology and personal skills. At this stage the compliance of all actors with standard international and airport-specific civil aviation rules and guidelines is key. The situation on board of an aircraft (red box) develops according to the interaction of: a) pilot; b) cabin crew; c) passengers; and eventually ground/airport actors. The analysis of the action arena should take into consideration the Evaluation criteria used by the relevant actors and their Modes of interaction. The yellow boxes highlight the key factors to be considered in the analysis. The resulting degree of success in the resolution of the distressful

situation on board of an aircraft should not be limited to its description. In fact, as represented by the figure, results can be interpreted as feedbacks which determine a consequent change in the system. Thus, this stage needs to be assessed using as indicators the specific interplay of each box with the others.

More specifically, as far as the analysis of group dynamics within the Aether scenario[14] is concerned, the elaborated management framework is implemented on the following scenario phases: "Early warning", "Alarm", "First measures" and "Emergency calls and media impact". The situation depicted in the scenario which the management framework assesses is graphically shown in the following graph.

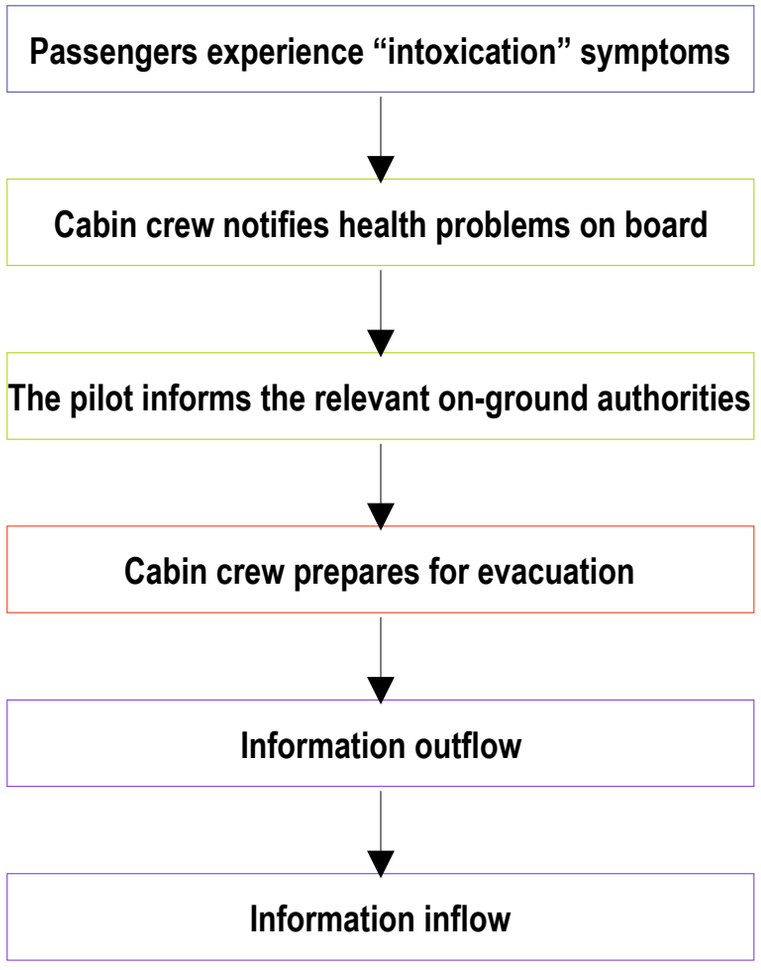


Figure 6 – Relevant scenario situation

14) The following analysis is based on the Aether draft scenario as elaborated on the 24th of April 2010.

As depicted above, the early warning signals (i.e. passengers feeling ill) represent the scenario at t0. In order to integrate the analysis of group dynamics on the Aether scenario a number of variables need to be addressed. They mainly refer to the following two so-called macro-variables: 1. Intoxication spread within the airplane; and 2. (passengers) Information flows once the airplane is landed. Within the two macro-variables several scenario alternatives can be singled out. The graph below depicts the interaction of scenario alternatives at each situation phase.

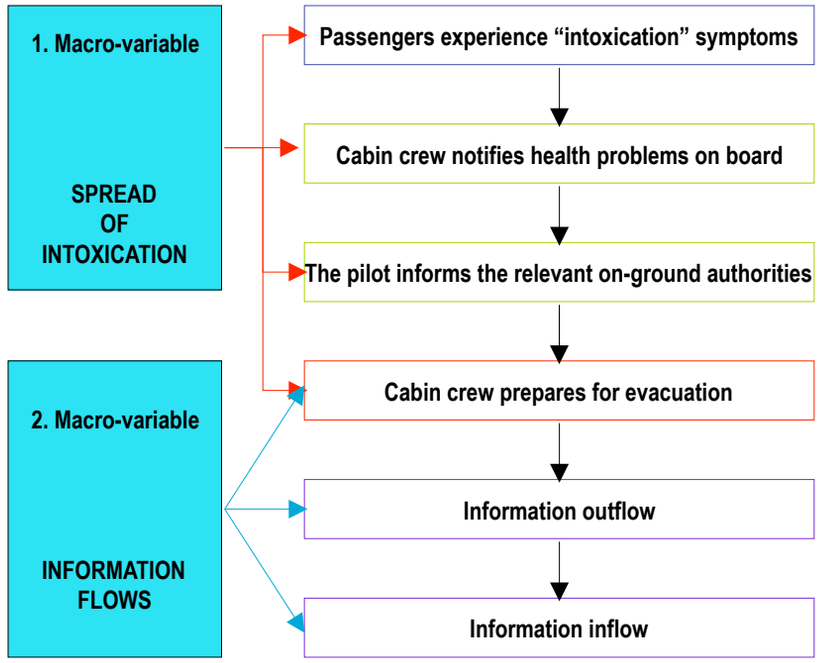


Figure 7 – Variable interaction with relevant scenario situation

According to the spread of intoxication (e.g. only a few passengers; the whole cabin; the whole cabin and cabin crew) a few alternatives can be elaborated:

1) cabin crew manages to isolate ill passengers and send out comforting messages to fellow passengers about a few cases of (for instance) food poisoning (i.e. Positive and Feasible Scenario);
2) cabin crew offers first aid to ill passengers and explains emergency evacuation procedure (Negative but Feasible Scenario);
3) everyone (cabin crew included) is suffering from the symptoms and no controlled action can be taken (Negative and Possible but not Feasible).

As explained elsewhere, the capacity to acquire information, to decode it and to manage information flows is a key aspect of SA and thus key for efficient decision making. Group dynamics in a rescue situation are strongly determined by the leadership capacity of the cabin crew. Its leadership appears to be positively related to its capacity as "gatekeeper" of information flows. Thus, scenario development alternatives should be elaborated according to the intensity and

direction of information flows from and to the cabin/passengers once the airplane is landed. Alternatives vary from 1) a situation where the pilot and cabin crew are the only actors informed about the whole situation – and thus able to exert their control and leadership; to 1+n) a situation where passengers have different degrees of knowledge and thus elaborate own goals and situation solution (Ref. p.7). The latter implies that the group is disintegrated and group dynamics leave place to individual initiatives.

Finally, as depicted in the following graph, one more variable is essential to be considered when the scenario is assessed: terrorist manifestation.

The manifestation of one or more terrorists on board is held as key in defying a feasible development scenario for group dynamics. Depending on when the terrorist(s) becomes overt; on whether he/she/they is/are armed or not; whether any request is made directly by the terrorist(s); whether passengers and crew are held as hostages; etc, group dynamics evolve differently.

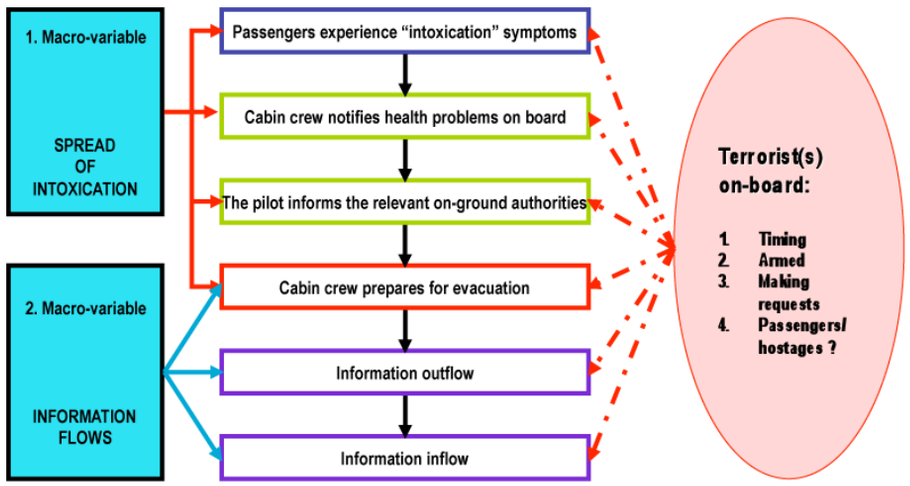


Figure 8 – Variable interaction with relevant scenario situation - Terrorist manifestation

Due to the complexity and multifaceted nature of interaction between psychological and physiological stressors such a situation would bring forward, it is suggested that the role of the terrorist is well defined before the exercise. By this we do not call for a strict interpretation of the role of the terrorist(s) but to reduce the alternatives of his/her/their action. It is suggested that the variables depicted in the red ellipse below are used to define the terrorist role in the scenario.

Once the scenario's final draft is ready, ISIG will test its main variables (without disclosing any specific/confidential detail) in a focus group with selected cabin crew. In order not to jeopardise the originality of the Aether scenario, ISIG proposes to structure the focus group methodology as follows: 1) participants are socialised to a similar t0 situation; 2) participants are then asked to elaborate, according to their competence and experience, a feasible scenario development; 3) participants will describe their management framework whilst developing the scenario; 4) participants will discuss the scenario development in terms of SWOT variables.

7. Conclusive Remarks

This section reports the results of a focus group conducted in Rome (22 September 2010) with a selected number of participants (5) which where all working as chiefs of the cabin crew for the Alitalia Airlines company[15]. The goal of the focus group has been to probe and check the literature review work and theoretical elaboration carried out by the ISIG research team on the subject of group dynamics in an airplane rescue situation. Particularly, the participants to the focus group were asked to discuss and comment on strategic issues such as: (a) the aspects of resilience and trust building in small interaction social systems like a cabin; (b) the role of spontaneous networking; (c) the relation between formal and informal grouping; and (d) the importance of situation awareness for the security of the crew and passengers. The focus group started with the discussion on the "Analytical framework for the analysis and evaluation of the management of group dynamics" (figure 6).

As conclusive remarks, to be discussed with reference to the wider results of the investigation, we provide here some comments on what the participants stressed and discussed with a stronger emphasis:

A) - The SA is considered to be the crucial aspect of all management issues of group dynamics. A good SA is built up with a dedicated training of the staff. Not just briefing or reading the manual but real exercises which are more and more rare for the budget constraints (in the 90s Alitalia reduced the training from 2 months to 1 week).

As a result, there is a negative impact on situations such as: communication with pilots, intra-communication within cabin crew, communication with passengers. The issue of communication is the most delicate in a danger, for the multinational composition of the group (passengers, crew, pilots) requires automatic responses that are possible only after a sound training.

B) - Protocols are more and more detailed but also more confusing. They change very quickly. This fact requires more adaptability of the crew, which is also exposed to harsher working conditions after the 90s because of the de-regulation processes. With fewer breaks and more flights, the participants consider the social relations on board less "culturally mediated" and more procedural.

I.e. the company does not represent the country and its custom. It is a neutral environment and the passengers perceive that. They feel the crew is less accustomed and less confident. The authority of the crew is somehow less strong and in the last 20 years there is a multiplication of deviant behaviours such as smoking in the cabin or lack of respect of basic rules.

C) - Low cost companies and the extension to a larger population of the flight habits, relaxed and de-constructed common approach to securities, compared to the time of more restricted access to flying when things were taken more seriously.

Now, among passengers, everybody thinks they are experienced and the pilots are more and more self-referentials. In this context, the management of group dynamics may be risky: normally, nothing happens, but in case of emergency, it is only the experience and the good training that may save the situation. It is not necessarily an issue of better or worse protocols.

15) Refer to appendix C

8. References

Articles and volumes:

- ✓ Barbour , R.S. and Kitzinger, J. (eds) (1999) Developing focus group research. Politics, Theory and Practice, London, Sage
- ✓ Bhugra, D. and De Silva P. (1998) Dimension of bisexuality: An exploratory study using focus groups of male and female bisexuals, in "Sexual and Marital Therapy", 13(2), pp. 145-157
- ✓ Bor, R. & Hubbard, T. (2006). Psychological Assessment and Reporting of Crew Mental Health, Aviation Mental Health, Ashgate Publishing
- ✓ Bor, R., Field, G., & Scragg, P. (2002). The mental health of pilots: an overview of recent research. Counselling Psychology Quarterly, 15, 3, 239 – 356
- ✓ Boyd, . & ain, P. (1997). Once I get you up there, where the air is rarefied: Health, safety and the working conditions of airline cabin crew. Oxford: Blackwell Publishers Ltd.
- ✓ Brown, Rupert. 1990. *Psicologia sociale dei gruppi*. Bologna: Il Mulino.
- ✓ Caldwell, J. (1997). Fatigue in the aviation environment: an overview of the cause and effect as well as recommended countermeasures. Aviation, Space and Environmental Medicine, 68, 932 – 938
- ✓ Campbell, R.D. and Bagshaw, M. (2002) – 3 ed. Human Performance and Limitations in Aviation, Blackwell Science Ltd, Oxford
- ✓ Del Bianco, D. & Andeva, M. (2009). *Chapter: The Criteria for Emergency Response.* Compliance of the Italian civil aviation system within the European Union guidelines, AETHER Research Paper.
- ✓ Dunn, C. John, Lewandosky, Stephan & Kirsner, Kim. (2002). Dynamics of Communication in Emergency Management. *Applied Cognitive Psychology*. 16 : 719 -737
- ✓ Endsley, Mica R. 1995. Towards a theory of situation awarness in dynamic systems. *Human factors and economic society*: 32-64
- ✓ Endsley, Mica R.; Garland D.J. (eds). 2000. *Situation Awareness Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates
- ✓ Flach, J. M. (1995) Situation Awareness – Proceed with Caution. Human Factors 37 (1) : 149-157
- ✓ Fleming J.A. (1998) Understanding residential learning: the power of detachment and continuity, in "Adult Education Quarterly", 48, pp. 260-271
- ✓ Folch, Lyon,E., Macorra, L. and Schearer, S.,B. (1981) Focus group and survey research on family planning in Mexico, in "Studies in Family Planning", 21, pp. 409-432
- ✓ Folkman, S., Lazarus, R.S., Gruen, R.,J., DeLongis, A. (1986). Appraisal, coping, health status, and psychological symptoms. Journal of Personality and Social Psychology, 50, 3, 571-579
- ✓ Gauld, J., Hirst, M., McIntosh, I.B., & Swanson, V. (2003). Attitudes to air travel after terrorist events. British Travel Health Association Journal, 3, 62-67.
- ✓ Greenbaum, T. (1998) The handbook for focus group research, 2nd ed., Newbury Park, Ca, Sage
- ✓ Greist, J. & Greist, G. (1981). Fearless flying. A passenger guide to modern travel. Chicago. Nelson Hall.
- ✓ Hackman, J.R. (1986). Organizational influences. In H.W. Orlady & H.C. Foushee (Eds.), Cockpit resource management training: Proceedings of the NASA/MAC Workshop (NASA Conference Publication No. 2455). Moffett Field, CA: NASA – Ames Research Center.

- ✓ Heller, J. (2003). Psychological and psychiatric difficulties among airline passengers. In R. Bor (ed) Passenger behaviour, (p.60.). Aldershot: Ashgate Publishing.
- ✓ Helmreich, Robert L. and Wilhelm, John A.(1991) 'Outcomes of Crew Resource Management Training', The International Journal of Aviation Psychology, 1: 4, 287 — 300
- ✓ Janis, Irving L. 1971. Groupthink. *Psychology Today Magazine*. 16 : 84-90
- ✓ Johnason, J. And Arneson, P. (1991) Women expressing anger to women in the workplace: perceptions of conflict resolution styles, in "Women's Studies in Communication", 14, 24-41
- ✓ Jones, Debra G.; Endsley, Mica R. 1996. Sources of Situation Awareness Errors in Aviation. *Aviation, Space and Environmental Medicine*. 67, 6: 507-511
- ✓ Kaber, David B.; Endsley, Mica R. (1998). Team Situation Awareness for Process Control Safety and Performance. Process Safety Progress. 17 (1) : 43-48
- ✓ Kidd, P.S. and Parshall, M.,B. (2000) Getting the focus and the group: enhancing analytical rigor in focus group research, in "Qualitative Health Research", 10(3), pp. 293-308
- ✓ Kitzinger J. (1994) The methodology of focus groups: the importance of interaction between research participants, in "Sociology of Health and Illness", 16, pp. 103-121
- ✓ Krueger, R.A. (1994) Focus group. A practical guide for applied research, 2nd ed., London, Sage
- ✓ Lauria, L., Ballard, T.J., Corradi, L., Mozzanti, C., Scaravelli, G., Sgorbissa, F., et al. (2004). Integrative qualitative methods into occupational health research: A study of women flight attendants. Occupational and Environmental Medicine, 61, 163 – 166
- ✓ Levy, D.E., Faulkner, G.L., & Dixon, R. (1984). Work and family interaction: The dual career family of the flight attendant. Journal of Social Relations, 11, 2, 67-88
- ✓ Lewin, K (1965). Teoria dinamica della personalità, Universitaria: Firenze
- ✓ Locke, S.A. & Feinsod, F.M. (1982). Psychological preparation for young travellers travelling abroad. Adolescence, 17, 815-819
- ✓ Maynard Tucker, G. (2000) Conducting focus groups in developing countries: Skill training for bilingual facilitatiors, in "Qualitative Health Researches", 10, pp. 396-411
- ✓ McGrath, Joseph. 1984. *Groups: Interaction and Performance*. Englewoood Cliffs: Prentice-Hall
- ✓ McIntosh, I.B., Swanson, V., Power K.G., Raeside, F., & Dempster, C. (1998). Anxiety and health problems related to air travel. Journal of Travel Medicine, 5, 198 – 204
- ✓ Merton, R.K. and Kendall, P.L. (1946) The focused interview, in "American Journal of Sociology", 51, pp. 541-557
- ✓ Moos, R.H. & Schafer, J.H. (2004). The crisis of physical illness. In J. Ogden (ed.), Health psychology: A textbook (3rd ed., pp.62-64. Buckingham: Open University Press.
- ✓ Morgan, D.,L. (1998a) The focus group guidebook in Morgan, D.L., Kreuger, R.A. and King J.A., (eds) (1998) Focus group kit, London, Sage
- ✓ Prezza, M. and Santinello, M.(2002) Conoscere la comunità. L'analisi degli ambienti di vita quotidiana, Bologna, Il Mulino
- ✓ Price, W. & Holley, D. (1990). Shift work and safety in aviation. Occupational Medicine, 5, 343 – 377
- ✓ Rigg, R. & Cosgrove, M. (1994). Aircrew wives and the intermittent husband syndrome. Aviation, Space and Environmental Medicine, 65, 654 - 660
- ✓ Roe, A.R., Hermans, P.H. (2006). Psychological Factors in Cockpit Crew Selection, Aviation Mental Health, Ashgate Publishing, 162
- ✓ Sharma, R.C. & Schrivastava, J.k. (2004). Jet lag and cabin crew: Questionnaire survey.

Journal of Aerospace Medicine 48, 1, 10-14.
✓ Stanton, N.A.; Chambers, P.R.G. & Piggott, J. 2001. Situation awareness and safety. *Safety Science*. 39 : 189-204
✓ Swanson, V. and McIntosh, L. B. "Psychological Stress and Air Travel: An Overview of Psychological Stress Affecting Airline Passengers", Aviation Mental Health, Ashgate 2006
✓ Tsang, P.S. & Vidulich, M. A. (ed) (2003). Principles and Practice of Aviation Psychology, Lawrence Erlbaum Associates, Mahwah, New Jersey, London, 1-3
✓ Vivien Swanson and Iain B. McIntosh "Psychological Stress and Air Travel: An Overview of Psychological Stress Affecting Airline Passengers", Aviation Mental Health, Ashgate 2006
✓ Wildavsky, Aaron. 1991. *Searching for Safety*. New Brunswick, NJ: Transaction Publisher

Legal Documents:

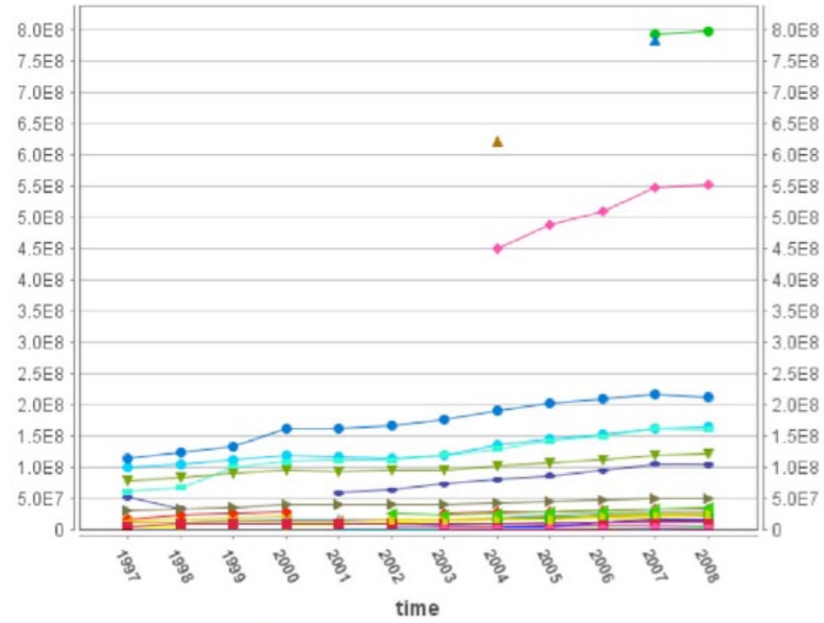
- Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council.
- Standards and Recommended Practices for the licensing of flight crew members, Annex 1 to the Convention on International Civil Aviation.
- Part 11, Annex to the Regulation 300/2008 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance), Official Journal of the European Union L 97 (2008, April, 4)
- Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security.

Internet sources:

- Excerpts and data from http://en.wikipedia.org/wiki/Japan_Airlines_Flight_123
- BBC News, Flight health risks under scrutiny, retrieved on 06.04.2010 from http://news.bbc.co.uk/2/hi/health/1214680.stm
- BBC News, Airlines face legal action over DVT, retrieved on 06.04.2010 from http://news.bbc.co.uk/2/hi/uk_news/1625309.stm

9. Appendices

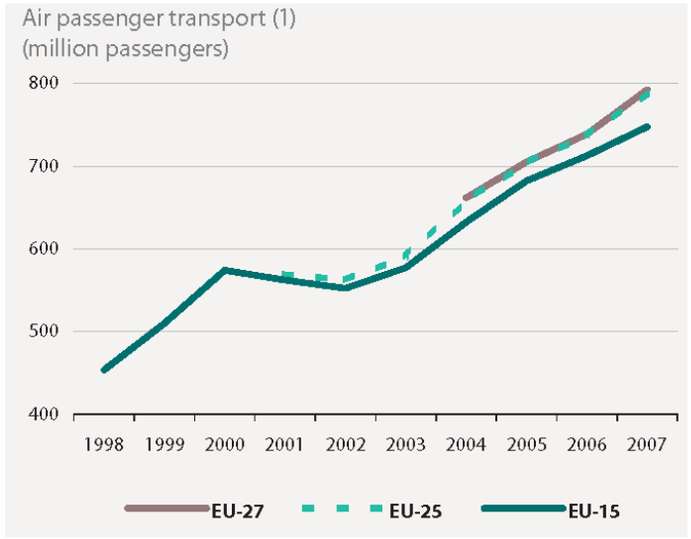
Appendix A: Passengers trends in Civil aviation



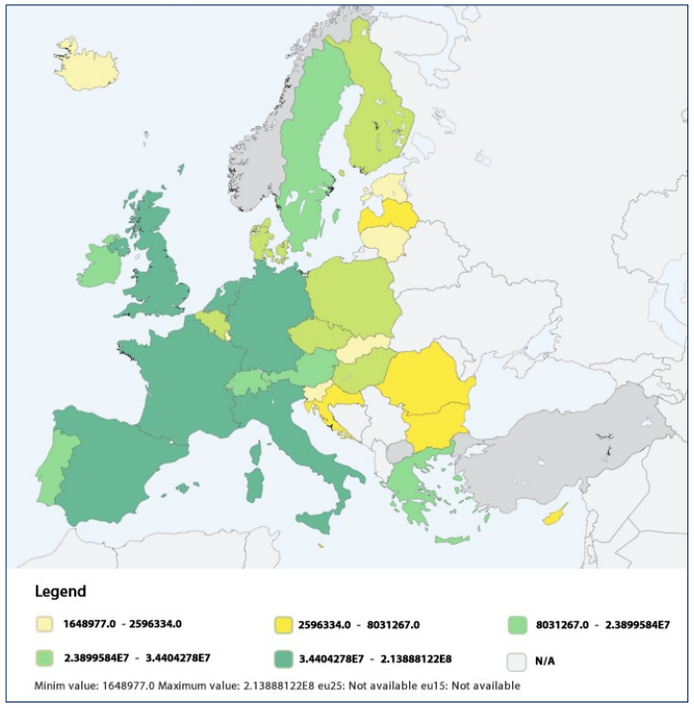
European Union (27 countries) European Union (25 countries) European Union (15 countries)
Euro area (EA11-2000, EA12-2006, EA13-2007,EA15-2008, EA16) Belgium Bulgaria
Czech Republic Denmark Germany (including ex-GDR from 1991) Estonia Ireland Greece
Spain France Italy Cyprus Latvia Lithuania Luxembourg (Grand-Duché) Hungary
Malta Netherlands Austria Poland Portugal Romania Slovenia Slovakia Finland
Sweden United Kingdom Croatia Iceland Norway Switzerland Unavailable data is ignored

Source of Data: Eurostat
Date of extraction: 06 apr 2010 11:45:07 CEST
Hyperlink to the graph: http://epp.eurostat.ec.europa.eu/tgm/graph.do?tab=graph&plugin=1&language=en&pcode=ttr00012
Disclaimer: This graph has been created automatically by Eurostat softw are according to external user specifications for w hich Eurostat is not responsible. Footnotes have not been included.
General Disclaimer of the EC: http://europa.eu/geninfo/legal_notices_en.htm
Short Description: The number of passengers transported by air has increased tremendously during the last decades. In the mid-seventies there w ere only slightly more than 200 million passengers transported by air in the EU-15. An estimation for 2000 gives a number of about 600 million. The effects of the tragic events of the 11 September 2001 are negative, estimates give that betw een 2000 and 2001, the total number of passengers carried decreased by 2 %.

Graph 1 - Air transport of Passengers in the EU



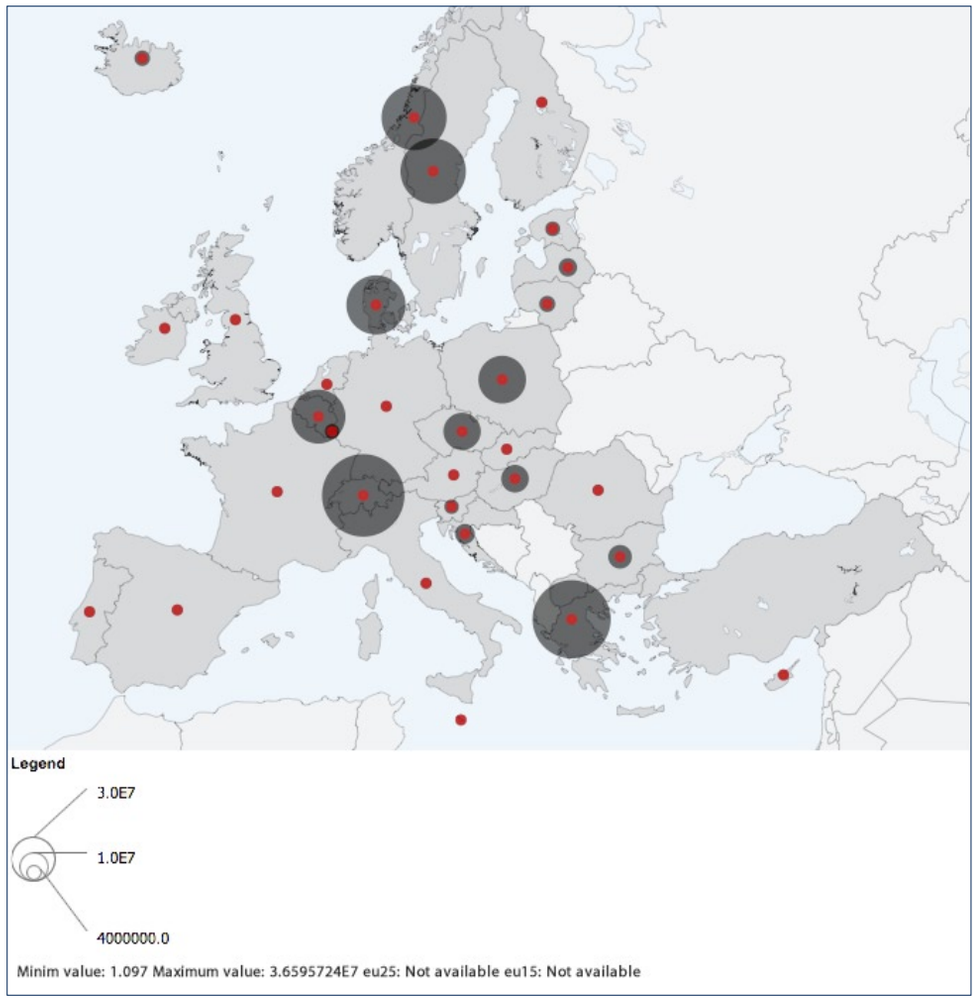
Graph 2 - Air passenger transport
Source: EUROSTAT guide to European transport statistics



Map 1: Air transport of passengers in 2008
Source: EUROSTAT

REPORTER	TOTAL PASSENGERS CARRIED (*) INCLUDING DOMESTIC FLIGHTS (THOUSAND)																								
PARTNER	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK
BE	60	113	276	452	1 363	32	394	765	3 445	1 111	2 334	51	49	49	0	291	79	231	469	330	715	140	92	2	225	400	1 627
BG	111	99	307	168	1 274	10	97	118	154	202	347	75	5	6	8	125	14	129	338	118	8	30	7	89	119	176	894
CZ	275	299	268	255	1 126	99	278	718	747	796	898	82	92	101	0	183	8	399	186	156	48	128	37	250	135	123	2 067
DK	450	170	254	1 951	2 115	144	228	664	1 977	1 227	893	67	168	231	73	189	45	1 040	386	392	198	25	20	20	751	1 783	2 347
DE	1 355	1 252	1 106	2 112	24 370	183	1 515	4 935	21 914	7 254	10 944	335	485	259	195	1 505	424	2 602	5 585	2 589	2 412	892	205	163	1 551	2 395	11 468
EE	32	10	99	145	184	20	18	48	57	23	36	0	42	53			1	77	21	21	5	0	0	1	174	173	182
IE	394	114	281	230	1 524	18	888	155	3 620	1 918	1 223	60	231	205	13	224	59	775	198	1 358	645	6	4	129	105	208	12 018
EL	776	118	728	665	5 050	48	154	6 685	508	1 610	2 381	1 204	48	55	60	314	22	1 550	931	488	6	274	94	156	348	735	5 451
ES	3 476	158	807	2 041	22 361	57	3 564	508	44 171	8 085	10 217		52	38	237	335	55	5 061	1 154	494	2 907	604	21	61	1 020	2 023	35 683
FR	1 057	201	772	1 186	7 367	22	1 897	1 495	8 090	27 192	7 748	124	35	26	147	510	139	2 327	924	757	2 113	473	126	99	458	1 152	11 726
IT	2 336	341	917	886	10 843	36	1 223	2 342	10 375	7 871	28 670	77	84	51	108	586	470	2 821	967	939	967	1 601	6	215	404	675	11 239
CY	52	76	83	70	342	0	57	1 187	3	130	78	0	5	5	8	60	19	105	154	53	0	72	1	6	42	228	2 983
LV	48	5	92	171	489	43	231	49	50	35	86	5	15	29	0	0	1	109	66	35	1	0	0	0	190	202	481
LT	49	6	100	231	260	53	203	55	40	27	65	4	29	0	0	0	4	86	37	52	0	0		0	91	53	338
LU	2	8	0	73	215	0	3	60	233	150	107	8	0	0	0	0	5	75	50	0	121	3	0	0	0	2	225
HU	290	121	171	191	1 453	0	178	298	304	527	575	60	0	0	0	0	18	416	81	129	46	294	22	0	191	268	915
MT	78	19	8	46	425	1	59	20	54	137	467	20	1	4	5	18	0	71	55	7	6	9	5	0	19	50	1 118
NL	204	126	406	1 043	2 612	76	776	1 530	5 000	2 491	2 859	105	109	84	76	412	72	56	544	356	987	301	19	52	444	953	8 368
AT	465	335	184	386	5 594	21	197	927	1 136	916	975	153	65	37	54	82	56	541	666	257	80	417	79	34	191	321	1 867
PL	329	110	156	391	2 611	21	1 174	453	494	756	949	54	35	52	0	155	7	360	259	1 087	55	59	11	1	160	457	3 865
PT	718	8	57	196	2 450	5	645	7	2 988	2 256	1 004	0	1	0	139	41	6	1 044	81	58	2 953	15	0	2	111	165	5 289
RO	121	32	128	21	847	0	6	276	564	436	1 494	72		0	0	220	5	297	370	63	12	544	1	8	21	1	325
SI	92	7	37	20	205	0	4	94	20	127	6	1		0	0	21	6	19	79	11	0	1	0	0	26	0	165
SK	2	75	231	20	159		128	151	62	130	197	5	0	0	0	0	0	52	34	0	2	9	0	175	0	16	485
FI	226	118	134	745	1 554	177	104	340	1 023	458	403	41	190	91	0	192	19	440	191	160	107	17	26	0	2 887	1 301	936
SE	398	165	123	1 655	2 389	178	206	723	1 978	1 170	668	232	202	53	2	230	50	954	320	480	164	1	0	17	1 315	6 893	2 267
UK	1 625	953	2 070	2 353	11 599	179	12 204	5 457	35 530	12 346	11 207	2 969	479	340	251	960	1 148	8 348	1 877	4 352	5 257	333	165	529	944	2 268	26 106

Table 1 – Total passengers carried including domestic flights (Source: EUROSTAT, Statistical Pocketbook, 2009, EU energy and transport in figures)
Notes: (*) Passengers carried are fewer than passengers on board, due to transit passengers staying on board the aircraft not being counted.



Map 2 - Air transport of passengers 2008 (Source: EUROSTAT)
Notes: Notes: Based on a comparison with: 2001

Short Description: The number of passengers transported by air has increased tremendously during the last decades. In the mid-seventies there were only slightly more than 200 million passengers transported by air in the EU-15. An estimation for 2000 gives a number of about 600 million. The effect of the tragic events of the September, 11 are negative, estimates give that between 2000 and 2001, the total number of passengers carried decreased by 2 %.

Passenger traffic	International		Domestic		Total	
Region	Growth	Market Share	Growth	Market Share	Growth	Market Share
Africa	-8.9	3	-13.4	1	-9.6	2
Asia/Pacific	-7.1	25	7.6	31	-1.2	27
Europe	-4	41	-10.5	8	-4.8	28
Middle East	10	11	10.3	1	10	7
North America	-5.5	16	-5.5	54	-5.5	31
Latin America / Caribbean	-2.9	4	1.9	5	-0.7	5
World	-3.9	100	-1.8	100	-3.1	100

Table 2 – Regional yearly passenger traffic growth and market shares in per cent (in terms of passenger kilometres performed – PKP for 2009)
Source: ICAOdata.com

Appendix B: International/European Legal Framework on Civil Aviation Security Training

The ICAO International Standards and Recommended Practices (signed in Montreal, 1986) give a specific focus on the training of the cabin crew members. In the Annex 6 dedicated to the operation of aircraft in international commercial air transport – aeroplanes, under the Chapter 13 (Security) it is specified that an operator should establish and maintain a training programme which enables crew members to act in the most appropriate manner to minimise the consequences of acts of unlawful interference. As far as the European Union legislation is concerned, in the Annexes of the EU regulations regarding the civil aviation basic security standards there are guidelines for training and accrediting of the security personnel. More specifically, in the Regulation 2320/2002, there is a part dedicated to the Staff Recruitment and Training[16]. Initially, the appropriate authority of the Member State should develop and implement a National Aviation Security Training Programme to enable aircrew and ground personnel to implement aviation security requirements and to respond to acts of unlawful interference with aviation. This programme should include selection, qualification, training, certification and motivation of security staff.

The flight crew and airport ground staff, the Security Training and Awareness training programme should be conducted on initial and recurrent basis for all airport and air carrier flight and airport ground staff. The training should contribute towards raised security awareness as well as improving the existing security systems. It should incorporate the following components: 1) security systems and access control; 2) ground and in-flight security; 3) pre-boarding screen-

16) Part 12, Annex to Regulation 2320/2002

ing; 4) baggage and cargo security; 5) aircraft security and searches; 6) weapons and prohibited articles; 7) overview of terrorism; and 8) other areas and measures relating to security that are considered appropriate to enhance security awareness. The security training course for all airport and air carrier ground staff with access to security restricted areas, should be designed for a duration of at least 3 hours in the classroom and a 1 hour field introduction[17].

The managers developing and conducting security training for security and air carrier and airport ground staff should possess necessary certification, knowledge and experience. The managers and instructors, involved in and responsible for the security training of airport ground staff, should undergo annual recurrent training in aviation security and on latest security developments.

The scope of training may be increased subject to aviation security needs and technology development. The initial training period for screening staff should not be shorter than the International Civil Aviation Organisation (ICAO) recommendation[18].

The security screening staff should be approved or certified by the national appropriate authority. The appropriate measures should be promoted to ensure that security staff is highly motivated so as to be effective in the performance of their duties.

In its Annex, the Regulation 300/2008 sets out only the general common basic standards related to the staff recruitment and training[19]. The persons implementing, or responsible for implementing, screening, access control or other security controls should be recruited, trained and, where appropriate, certified so as to ensure that they are suitable for employment and competent to undertake the duties to which they are assigned. Persons other than passengers requiring access to security restricted areas, should receive security training, before an airport identification card or crew identification card is issued. This should be conducted on initial and recurrent basis. The instructors engaged in the training of the persons mentioned should have the necessary qualifications. In the part dedicated to the in-flight security measures is only eminent that appropriate security measures such as training of flight crew and cabin staff should be taken to prevent acts of unlawful interference during a flight.

The Regulation 820/2008, supplements some provisions regarding the staff recruitment and training. According to this regulation, the National Aviation Security Training Programme should include training requirements for handling unruly passengers[20].

17) Annex to Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security.

18) Standards and Recommended Practices for the licensing of flight crew members (pilots, flight engineers and flight navigator***s***), air traffic controllers, aeronautical station operators, maintenance technicians and flight dispatchers, are provided by Annex 1 to the Convention on International Civil Aviation. Related training manuals provide guidance to States for the scope and depth of training curricula which will ensure that the confidence in safe air navigation, as intended by the Convention and Annex 1, is maintained. These training manuals also provide guidance for the training of other aviation personnel such as aerodrome emergency crews, flight operations officers, radio operators and individuals involved in other related disciplines

19) Part 11, Annex to the Regulation 300/2008

20) The term "unruly passenger" was introduced with this regulation. Unruly passengers are persons who commit on board a civil aircraft, from the moment when the aircraft door is closed prior to take-off to the moment when it is reopened after landing, an act

When having a recruitment, the persons implementing, or responsible for implementing, screening, access control or other security controls; the instructors; and persons who will be issued with an airport identification card or crew identification card have to receive theoretical, practical and/or on-the-job training[21].

The international and European legal framework guaranties the basic and common rules for security trainings, recommending specific training programmes to be developed in each state as well as in each air carrier.

Appendix C – Focus group on "Group dynamics in the airplane in the aviation rescue situation".

The focus group has been moderated by the ISIG researchers, which also collected, elaborated and interpreted the data. Accordingly, this appendix contains both a description of the theoretical presumptions and the explanation of the work done till the conclusive remarks, which hold a special value for the definition of a set of recommendations. The appendix is divided in two parts. The first subsection works as an introduction to the focus group technique of social research. Here the focus group is compared to other techniques of data collection and is eventually adapted to the specificities of the case study. Finally, the introductory section explains why such a tool is important for our case study.

The second subsection deals more in details with the collection and interpretation of the data in the focus group realized in Rome. Namely, in this part the most relevant information, reflections, comments, and generally speaking, valuable data emerge and pass through the interpretation process of the researchers. In other words, the researchers transcribe, select, elaborate the information obtained in the course of the collective discussion and search for sensible meanings without being influenced – or trying not to be influenced - by external factors such as the expectations of the donors or of the research partners.

1. Setting up and realizing a focus group on group dynamics in an airplane[22]

The focus group is a qualitative survey technique for data collection in the social science and it is based on the information emerging within a group discussion on a topic or an issue

of: assault, intimidation, menace or wilful recklessness which endangers good order or the safety of property or persons, assault, intimidation, menace or interference with a crew member in performance of duties or which lessens ability to perform duties, wilful recklessness or damage to an aircraft, its equipment, or attendant structures and equipment such as to endanger good order and safety of the aircraft or its occupants, communication of information which is known to be false, thereby endangering the safety of an aircraft in flight, disobedience of lawful commands or instructions for safe, orderly or efficient operations.

21) Annex to Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council.

22) The focus group has been implemented in one session that lasted from 10.00 a.m. till 14.30 of the 22nd of September 2010. The group has met in a private room reserved at the Italian Center for International Conciliation Studies in an historical building in the center of Rome. The choice made the participants relaxed and comfortable. The group conversation has been recorded by the moderator, Emilio Cocco.

that the researcher aims to investigate in depth.

Although there are many diverse typologies of focus groups empirically implemented, the scholarly literature defines three types of focus groups: the full group; the mini group; the telephone or internet group.

In our case, we opted for the realization of a mini group with chief cabin attendants. The reasons were both the difficulty to find available participants to convey in the same place at the same time, and the need to have deeper discussion on a topic full of technicalities and details, which are usually not disclosed to the wider public.

Thus, the group formation responded to few strict criteria such as the profession and the employer (Alitalia) as we chose to concentrate on a single company, the most important and almost monopolistic in the Italian scenario.

This way, we had the opportunity to drive the discussion along quite a long time span, from the Seventies till the present days, and to consider the changes that took place. For this reason, we differentiated the status and the age of the participants: two of them were already retired while the other three still working for the company. Consequently, the group was also differentiated in terms of age as we had both younger and older participants, although we selected only people with a long record and a sound experience.

Moreover, we made up the group with a gender balance: three women and two men. The prevalence of women reflects the dominance of female employees within the cabin crew and the more positive attitude of women to take part into focus group, as underlined by more than one study (Maynard Tucker: 2000).

All the participants were residents in the city of Rome but with different regional background: one from the north of Italy, one from the center, one from the south and two from the same city of Rome.

2. Interpretation of the data

The focus group aims to shed light on the facts from the perspective of the informants by combining the methods of the interview (making questions) and the ethnographic observation (studying the interactions). Therefore, the data produced during the focus group needs to be interpreted to provide some relevant information for research purposes (Krueger: 1998; Fleming: 1998: Kidd, Parshall: 2000).

The process of data analysis is divided in four different phases: 1) Raw data € 2) description €3) interpretation €4) conclusions.

The raw data are all the information produced by the verbal and not verbal communication, which are recorded and categorized by the researchers. The description of the data corresponds to a selection of the most relevant data and the reorganization of the information according to some leading ideas. In the phase the researchers may also report examples or relevant pieces of the discussion. Later, the interpretation phase is the moment when the data

are discussed with regards to their meaning for the research purposes. The conclusions include recommendations and/or reflections on the implications of the focus group for the research as a whole.

Here we report an analytical synthesis of the phases of the description and the interpretation of the data. These were mostly based on the notes of the moderator and on the analysis of the recorded discussion. Of course, the analysis takes into consideration data that refer to the social context and the environment besides the bare information: Also, the comments are evaluated considering their specificity, frequency and intensity, with regards to verbal and body language.

The discussion revolved around the diagram called "analytical framework for the analysis and evaluation of the management of group dynamics", which has been circulated in advance to the participants.

When asked to comment on the diagram, all the participants agreed that it was well done, comprehensible and clear enough. They also stressed that it looked very much like the documents they were provided by the company during the briefing and training sessions.

As the discussion developed, the participants focused their attention to some specific sections of the diagram and explained that those were the most sensitive points for the management of an emergency situation. Interesting enough, there was a general agreement on the points, whereas the interpretation given by the single participants has been slightly different though.

Particularly, the following points were spelled out:

1- the relevance of the flight route

2-the composition of passenger groups

3-the quality of training of the staff

4-the capacity to have a SA, with special regards to the ability to communicate with the pilots

The points above are all connected in the words of the participants but they all considered "the quality of the training of the staff" the most relevant one for safety.

Particularly, the shortening of the training period and the removal of technical personnel as trainers is pointed out as quite a dangerous practice, to be explained in terms of financial restructuring of the company and changing conditions of the business environment. In the words of the participants:

"We used to have a very solid training, both technical and commercial training, where the human relations were a central issue. But in the 90s we progressively lost the technical part of training and the same training period shrank from 2 months to 1 week."

"I used to work as a trainer too, at the end of my career, so I saw all the story. In the 70s we had 1 month of technical training and 1 month of commercial training, with final exams. If you failed twice you were out…. Moreover, we had simulations of emergencies with fire and water at the training center in Fiumicino (Rome), which was a model in Europe. At the end of the 90s all that story was cut."

"I think pilots and cabin crew are less trained nowadays. In the 70s and the 80s the requirements were higher and there was no way you could have non trained personnel on board. I do not want to say personnel is not trained at all today, but we are talking about cabin crew that went through simulations, study periods... real experts. I am sure people are less qualified now, at least from a cultural point of view."

It is clear from the above that the conditions on the airplane are considered less safe because of a poorer training that depends on economic factors, which are found in the deregulation processes that started in the 80s and brought to a radical change of the business environment in the 90s. As a result, according to the participants, the companies – and Alitalia specifically – tend to balance the lack of training with information redundancy.

"It is the same thing abroad, we probably have more knowledge but also fewer opportunities to apply them in exercises… everything is well regulated and we have lots of manuals, reports, rules to learn, probably too much. And they change very quickly because technology runs fast. At the end of the day my experience is that only with a good training you can properly react to emergency."

"The SA depends primarily on the training of the cabin crew; there is no way you can define it with protocols, does not matter how good these protocols are. We have now dozens of protocols; they give instructions about every possible case. But quite often they are confused and in contradiction, they change from state to state and from company to company – although basic measures are the same."

Consequently, the SA is poorer because of the training. However, another problem factor of weakness is the deterioration of the social relations and the communication in the cabin. This is a trend that participants explain both with regards to the economic restructuring and the emergence of the low cost company philosophy. As a result, they witness processes of progressive lack of communication between pilots and the cabin crew, changing patterns of relations between the cabin crew and the passengers, harshening of industrial relations in the company. The poorer training, combined with the processes of above eventually compromise the SA because it weakens not the general security level –which remains high – but the ability to promptly react to emergencies.

"The self-referentiality of the pilots is crystal clear! At the beginning of 2000 we had to start a special training of "crew integration" because it became difficult to interact with the pilot and to communicate efficiently."

"The communication between the cabin crew and the pilots is minimal nowadays. Basically, it is limited to long distance flights, while in Italy and in Europe we do not have any proper interaction with the pilots. You can imagine that if we have to face an emergency situation it would be good to know who we are dealing with!"

"In some emergency situation, the human touch and the intuition are more important than protocols. I personally found myself in danger more than one time. And I can tell you that the manuals are not enough. It has been the good relations between the crew members and the pilots that made things recover. In specific cases, like when you need an "oxygen-therapy", if you do not act quickly, you may find yourself stuck between silence and redundancy."

"It is probably the deterioration of the professional relations that may eventually endanger the flight. The low-cost company competition is detrimental to the health of the cabin crew, who has now worse contract, less time to recover, less social support… if you think of the big number of female cabin assistants, the lack of social support, like baby sitting service or free days to stay with the family, brings the level down. We also experienced a highest rate of suicide for stress."

An episode described by one of the participants explain quite well the problem of communication:

"About 6-7 years ago, at the Catania (Sicily) airport a charter plane for tourists had a bad takeoff for an error with refilling the fuel. They only filled one tank because of a misunderstanding while communicating in English. So, the pilot decides to go back and land; tells the cabin crew to prepare for an emergency landing, but the cabin crew starts showing how to wear the safety jackets for an emergency landing in the sea. All in English, because no one was Italian – the pilots from Iceland and the crew from Finland, or vice versa, I cannot remember correctly. At the end, 3 passengers had a heart attack and one later died. The Italian authority for Aviation takes the license back to the company (Air Sicilia). This shows how in an emergency situation, if you are not trained, you tend to forget basic things, like how to communicate with the language of the company, which in this case was Italian. And the EU says that at least one member of the cabin crew should speak the language. But if you want to save money, this is what you get."

Eventually, the participants pointed at the composition of the passenger group and the relevance of the flight route as important factors to consider in the management of emergency situations.

"In some cases, the passengers are very problematic and you should know it. Not all the flights are for businessmen or families. We had cases of real danger where the passengers did not recognize the authority of the crew and pretended to know more than us. The low cost companies created new types of frequent flyers with lower culture and a wilder approach to the flight itself. This is a problem for security and a less trained and less paid cabin crew does not help."

"Some flights are "sensitive" for the destination or the composition of passengers. For their religions or ethnicity. Most of them are spelled out in the protocols, some other are described in the briefing. But there are destinations and flights you would not deem "sensitive" but they actually are. Like the ones for Brasi that are very long. Pilots, passengers and the crew become stressed out for the time to recover from one flight to the other is diminishing. And we had many accidents. Only the experience helps you out."

A.A. Cohen: Toward a Public Information Strategy for Bioterrorism Response

Is Europe truly prepared for a bioterror incident? Are European states capable of reacting quickly, synergistically and effectively to counter a national, regional or continent-wide bioterror event? And what are the essential messages that need to be sent to key segments of the European Union's inhabitants in connection with these efforts? Answering those questions will become essential as Europe continues to work toward a truly agile, coordinated counterterrorism strategy.

Recent history can serve as a guide in this regard. The two largest terrorist events in Europe of the past decade – the March 2004 Madrid rail bombings and the July 2005 London subway bombings – elicited vastly different governmental responses. The former revealed serious shortcomings in state-to-state crisis coordination, and a lack of a clear, coordinated messaging effort on the part of the Spanish government. The latter drew a more robust, synchronized response from the affected government (England) and from other EU member states.

The differences were attributable to the advances being made at the time in law enforcement and other horizontal cooperation in the EU area. Growing coordination among member states spawned new frameworks for law enforcement and intelligence. These advances in information access and sharing, policy implementation, collective security action and media synchronicity were embodied in the European Union's 2006 Crisis Coordination Agreements.

A coordinated media strategy is an essential component of this response. Whether the crisis is local, regional or continental, the European response to a terrorist attack should include a distinct public information component aimed at simultaneously informing the public, calming public fears, and coordinating what is often a complex set of disaster responses. The following study seeks to assess and analyze the state of public information strategy in the European Union in the context of a bioterrorist attack of the type outlined in the Aether Scenario.

Scenario I examines the response to a biological attack using aviation that is promptly identified and properly contained by Finnish authorities. Under such conditions, local authorities will need to affect prompt containment of the incident, and subsequently the quarantine of infected and sick passengers. Thereafter, authorities will need to decontaminate both individuals and affected facilities. A systematic plan for patient care and outbreak containment will need to be formulated, along the lines outlined in the article by the Jalasvirta Group. Subsequently, authorities will need to investigate the source of the incident and its perpetrators, using the combined efforts of local, national and international law enforcement agencies. This scenario should entail a multi-tier public relations strategy focusing on three overarching messages: the transparency of the governmental response; the competence of responsible authorities in addressing the incident; and the successful containment and diffusion of the incident. These objectives should be communicated through methods such as press conferences, dedicated websites and telephone lines, as well as the proper use of social media outlets such as Youtube and Twitter.

Scenario II envisions a biological attack using aviation that is not contained, and expands to become a national crisis within the borders of Finland. Such a scenario presupposes that the affected aircraft and its passengers are not promptly and/or properly sequestered and decontaminated, and that as a result the biological agent is introduced into the broader Finnish population. The immediate burden of response in such a crisis scenario would fall to regional rescue services, while public information response would fall to the Finnish Defense Administration. As in Scenario 1, authorities will also be required to investigate the source of the biological attack via the combined efforts of local, national and international law enforcement agencies.

Scenario III envisions the expansion of the Aether scenario to the level of Continental pandemic. In such a scenario, both local and European response would need to focus on two priorities. The first is containment, in which EU member states work in tandem to establish the necessary medical protocols, health surveillance and reporting procedures, and treatment routines and facilities, in various urban centers if necessary, in order to mitigate – or at least slow – the spread of the biological agent. The second is the isolation and treatment of the infected, with significant procedures and protocols necessary to deal with high volumes of patients, and beyond that an extensive – and extended – mobilization of resources across the Continent to accommodate law enforcement, civil protection and medical services to provide both for emergency medical assistance as well as aftercare.

Effective response under the scenarios above will require significant changes to current European approaches to public information strategy. There is at present no central body responsible for a strategy in communications to the public in emergency situations. Rather, the European Union currently boasts multiple, overlapping agencies with a mandate for public information dissemination. A clear hierarchy or chain of command is necessary to ensure message cohesion and clarity, and guarantee that local authorities and responders are trained to respond and communicate properly, and more effectively use multiple forms of media beyond traditional broadcasting (i.e., Web 2.0, Twitter, etc.). At the same time, there needs to be greater consistency of messaging between individual European member states involved in a given crisis, and increased centralization of the public policy response to bioterrorism.

1. Introduction

On March 11, 2004, a series of coordinated bombings targeted the Cercanias commuter rail system in Spain's capital, Madrid, killing 191 people and wounding 1,800 more. These attacks originated from radical Islamists residing on the Continent and inspired – but not necessarily formally directed – by al-Qaeda. A new model of "homegrown" terrorism had emerged.[1] Today, more than six years later, it is easy to forget the initial shock and confusion that accompanied the Madrid attacks. But that disorder is well worth remembering, because it provides insights into how European states can and should conduct the informational response to terrorism on a mass scale.

Immediately following the attack, most TV stations reported the attack during their regular morning news programs, starting at around 08:00. The programming on *Antena 3* lasted until

1) "The Legacy Of The Madrid Bombings", BBC (London), February 15, 2007, http://news.bbc.co.uk/2/hi/europe/6357599.stm.

14:00. Madrid newspapers issued special midday editions and TV stations rearranged their regular schedules. The public stations *TVE* (national) and *Telemadrid* (regional) did not break for commercials at all during the day. All TV stations replaced their logos with black ribbons at 18:00.

Prime Minister Jose Aznar conferred with King Juan Carlos, then with leaders of the political parties in parliament and with the heads of government of Spain's autonomous communities. At 10:36, a "Crisis Cabinet" was convened, comprised of Aznar, Deputy Prime Ministers Rodrigo Rato and Javier Arenas, and Interior Minister Angel Acebes. The government issued a decree declaring three days of official mourning, and demonstrations were called for Friday evening in cities across the country, under the motto "With the victims, with the constitution and for the defeat of terrorism".

Almost from the start, however, the public information messaging associated with the governmental response was fraught with problems. Governmental officials immediately assumed that the radical Basque separatist group ETA, with its history of violence against the Spanish state, was the principal culprit. Prime Minister Jose Aznar publicly blamed the group in his statements before journalists and reporters, as did Interior Minister Angel Acebes. This initial supposition, however, proved to be false. Subsequent developments demonstrated conclusively that there was no involvement in the incident by the Basque group.[2]

The Spanish government's credibility was mortally wounded. By 17 March, just days after the incident, governments around Europe – initially supportive and sympathetic – were voicing concerns that the Spanish government had jeopardized their security by feeding them false information about ETA's involvement. The incident was a telling indicator of the potential dangers of inconsistencies in messaging between EU member states, and throughout the EU area, regarding threats and responses.

2. Toward a Response: London, 7/7

Only a year later, the United Kingdom experienced a similar attack. In July of 2005, multiple attacks targeted the London Tube subway system. On July 7, four suicide bombers struck in central London, killing 52 people and injuring more than 770. After the attacks, Metropolitan Police Commissioner Sir Ian Blair confirmed fears that it was a coordinated terror attack, but appealed for calm, asking people not to travel to London or make unnecessary calls to the emergency services. Shortly thereafter, Prime Minister Tony Blair spoke out about the incident, calling the attacks a coordinated series of "barbaric" terrorist attacks. Having flown back from the G8 Summit in Scotland, Blair emerged from a meeting in Downing Street and urged the public not to "be terrorized".

The main UK TV networks (BBC1 and ITV) dropped regular programming and carried news of the attacks within 30 minutes of the first reports of the incidents. The length of this media coverage in the UK was unprecedented: for example, it constituted the single longest broadcast in ITN's history. There was total blanket coverage on all UK news channels for several days. Radio stations toned down their programming, and supplemented it with extended news

2) "Al-Qaeda 'Claims Madrid Bombings'", BBC (London), March 14, 2004, http://news.bbc.co.uk/2/hi/europe/3509426.stm.

and information throughout the day. This coverage was aimed at Londoners struggling to get home or to work in the aftermath of the attacks.

Within hours of the explosions, several websites were established, including You Will Fail, which celebrated London Mayor Ken Livingstone's defiant words, and We Are Not Afraid, inviting all folk to express their resolution not to be "afraid, intimidated or cowed by the cowardly act of terrorism". While initially intended for Londoners, the site was soon receiving supportive messages worldwide. Throughout, official messaging on the part of the British government was clear and consistent. Rather than moving quickly to cast blame, UK officials focused instead on consoling the bereaved, expressing solidarity with the victims, and promoting feelings of unity and solidarity in the face of terrorism.

The EU sprang into action as well, issuing a Declaration condemning the London bombings and calling for a better way to share information and a consistency in law enforcement throughout the EU area. Part of the core message was that the 7/7 bombings represented an attack on EU values as a whole.

In contrast to the Madrid attacks, there was more evidence of a united, cohesive response from the EU. The European Council expressed its commitment to strengthening cross-border cooperation "in order to impede terrorists' planning, disrupt supporting networks, cut off any funding and bring terrorists to justice".[3] Equally significant, but less noticed, was the Council's focus on strategies for cooperation and communication between Member states. These included a range of initiatives, the Data Retention Directive, to the European Evidence Warrant, to greater exchange of information between law enforcement authorities. The Data Retention Directive was created to harmonize and facilitate communications on data between Member States regarding law enforcement. The European Evidence Warrant is another directive that was established to make the exchange of judicial proceedings easier between Member States. Through the EEW, Member states may take advantage of the telecommunications systems under the European Judicial Network. These efforts had clear goals in mind; as British Home Secretary Charles Clarke explained at the time, the objective was to address the factors that contribute to radicalization and recruitment, even as European states reduced the vulnerability of their citizens and infrastructure to future attacks.[4]

These Crisis Coordination Agreements, or CCAs, passed on 1 June 2006 by the Council Justice and Home Affairs, as they came to be known, encompass six key functions:

1) information access and sharing; support;
2) enabling consistency in actions taken;
3) enabling debate on contentious policy decisions;
4) enabling debate on collective external action; and
5) media coordination.[5]

The structure created in these agreements, is ad hoc and flexible. It covers joint efforts to

3) Press Release, "Council Declaration On The EU Response To The London Bombings", Extraordinary Council Meeting, European Union, July 13, 2005, http://www.europa-eu-un.org/articles/en/article_4906_en.htm.

4) "The Legacy Of The Madrid Bombings."

5) *EU Emergency And Crisis Co-Ordination Arrangements,* n.d., http://www.consilium.europa.eu/uedocs/cmsUpload/WEB15106.pdf

respond to a Europe-wide attack, and the creation of dedicated organs to do so (among them the post of Counter-Terrorism Coordinator, the Joint Situation Centre, the Commission Monitoring and Information Centre, and the Council's ESDP crisis management structures). Each of these organs helps facilitate a key counterterrorism function: to allow senior EU leaders and EU bodies to share information, to ensure coordination and to enable collective action during a cross-border emergency[6]

Still, significant challenges remain with contemporary European counterterrorism policy. Among the most pressing is trying to ensure that proper analysis of threats and responses is built into planning processes at the national and regional levels. After all, the processes involved (electoral, budgetary, procurement, etc.) do not evolve at the same pace as threats. It therefore is difficult to ensure that longer-term counterterrorism planning makes it onto the agenda of politicians who are concerned with the "here and now" – and even more difficult to ensure that it stays there. More often than not, counterterrorism policy is reactive, and keyed to a particular near-term crisis.[7] For example, after the Passage of the European Arrest Warrant, Mamoun Darkazanli, a Syrian-born German suspected of being an al-Qaeda operative, had been held in custody for extradition to Spain under the warrant procedure. On appeal, on 18 July 2005, the German Constitutional Court held that the law applying the warrant did not respect fundamental rights and procedural guarantees and so was contrary to the German Constitution. As a result the EU arrest warrant no longer applies in Germany and the suspect has been released. It will take a new law from the German Parliament to reinstate the arrest warrant.[8]

Another challenge is that of prioritization. European policymakers are constantly attempting to achieve greater results from a limited pool of resources, in the process choosing from among a multitude of competing demands. These officials need to be able to correctly analyze the information they receive, and build policy that accurately addresses that information. This is exceedingly difficult when trying to take into account the needs and opinions of twenty-seven Member states. Even if consensus is reached, experience has shown that it is often difficult to follow-through on implementation on these agreements and policies.[9]

A public policy response to a CBRN attack would involve many elements. The International Red Cross and Red Crescent Societies provide a good example of how disaster awareness plays a key role in developing a response. Given the organization's deep influence and global outreach, the Red Cross model provides useful parallels and ideas that can be internalized by European governments, including:

- Recognizing that disaster preparedness should be one of the primary activities of the International Federation and each National Society;
- Recognizing disaster preparedness as an effective link between emergency response, rehabilitation and development programs;
- Strengthening the organizational structures at international, national and local levels required for effective disaster preparedness;
- Improving coordination; and
- Striving to provide the financial, material and human resources required to carry out appropriate and sustainable disaster preparedness activities.[10]

6) Ibid.

7) Stephen Pullinger, "European Security In 2020: Threats, Challenges And Responses", *European Security Review* no. 37, March 2008, http://www.isis-europe.org/pdf/2008_artrel_149_esr37europeansecurity2020-mar08.pdf.

8) "European Arrest Warrant Ruled Unconstitutional In Germany", EurActive.com, July 19, 2005, http://www.euractiv.com/en/security/european-arrest-warrant-ruled-unconstitutional-germany/article-142674.

9) Pullinger, "European Security In 2020: Threats, Challenges And Responses."

To accomplish these goals, many countries – including the United States and Great Britain – have created "war rooms" to coordinate their disaster response and preparedness in the event of crisis. Hurricane Katrina provides a microcosm of how such a structure helps to effectively respond to a disaster. With the landfall of the Category 5 hurricane in August 2005, the Operations Center at the Department of Health and Human Services, run by the Secretary of that department, became the crucial communications node in the U.S. government's disaster response effort.[11] Once the magnitude of the damage was realized through satellite photos and on-the-ground communications, HHS staff began shifting more than 1,000 U.S. Public Health Service officers and tons of supplies into the affected region, making the response to Katrina the largest public health relief operation in U.S. history. (The subsequent breakdown of the Katrina response, tragic as it was, should not obscure the early successes of that "war room" in mobilizing the national response. Simply put, people – rather than processes – are what failed in that instance.)

A key part of this process is communication. The United States has historically taken a calculated approach to communicating with target audiences in the instance of a terrorist threat. Domestically, it is a priority for the U.S. government to clearly message to the American people why the United States is reacting in the way it is, especially in the context of military operations in Iraq and Afghanistan. Abroad as well, Washington takes pains to communicate to its allies and international partners why it is undertaking a particular course of foreign policy action.[12] The reasons are obvious; in order to persevere in the War on Terror, it is essential for the United States to receive the trust and operate with the cooperation of foreign nations.[13] America leverages its public policies to accomplish that.

3. The Media and Crisis Response

America is hardly unique in this regard. Clear, concise and timely communication is indispensable to Europe's success in the counterterrorism sphere as well. Whether the crisis is local, regional or continental, the European response to a terrorist attack should include a distinct public information component aimed at simultaneously informing the public, calming public fears, and coordinating what is often a complex set of disaster responses.

10) International Federation of Red Cross and Red Crescent Societies, "Disaster Preparedness", n.d., http://www.ifrc.org/docs/pubs/who/policies/disaster-policy-en.pdf.

11) Steve Sternberg, "Katrina 'War Room' In Gear", USA Today, September 14, 2005, http://www.usatoday.com/news/nation/2005-09-14-katrina-war-room_x.htm.

12) Peter G. Petersen, "Public Diplomacy And The War On Terrorism", *Foreign Affairs,* September/October 2002, http://www.cfr.org/publication.html?id=4762.

13) Ibid.

Here, an accurate understanding of the evolving European media environment is essential. In today's rapid, evolving news cycle, governments can choose to follow two broad paths. The first, as adopted by governments such as China and Iran, among others, is **restrictive**. It entails the government manipulation of media mediums via the closure of press outlets, the imposition of news blackouts, and the slowing down or complete closure of the Internet. Such an approach lends itself to the authoritarian model of government, where governmental control is paramount and the concerns and opinions of citizens are rarely if ever taken into account. Given Europe's open and democratic values, however, such an approach is neither practical nor desirable.

Instead, European governments need to leverage the Continent's open, interactive media environment to formulate an **inclusive** model of public information. Such a proactive approach involves:

1) Anticipating adverse media coverage of the crisis, including graphic images of the disaster.
20 Pre-formulating key messages, both for various specific audiences and for the general public, in response.
3) Identifying relevant agencies and spokespersons to interface with the European public, taking into account multiple languages, distinct ethnicities and cultural differences.
4) Exploiting diverse media outlets, including "new media" such as social networking sites, through both traditional and innovative tactics (video messages, blogging, etc.).
5) Preserving clear and consistent messaging to all relevant parties.[14]

These principles are explored more fully below, via three distinct scenarios that utilize the "Aether" problem set previously enumerated.

✓ *3.1 Scenario I: Prompt Apprehension and Containment*

The first notional set of events relating to the Aether Scenario is one in which a biological attack using aviation is carried out, but promptly identified and properly contained by Finnish authorities. In such a fictional scenario, the airliner carrying biological agents and infected personnel would arrive in Finland, but prior notification to authorities would permit Helsinki to put into motion a crisis response plan that would isolate the aircraft upon its arrival. In such a scenario, the primary responsibilities of the Finnish government would be fourfold.

First, authorities would need to *contain* the incident geographically. This will require local and first responders to physically cordon off the area where the aircraft is located following landing. Passengers and those affected would not be allowed to deplane or disembark. They

14) For more specificity on basic public information principles, see Anthony Holmes, "7 Principles Of Crisis Management", www.anthonyholmes.org, n.d., http://anthonyholmes.org/7principles.aspx; *Principles of Crisis Management In A Viral Age: Integrating The Tools And Lessons Of Search 2.0 Into A Comprehensive Crisis Response*, January 2008, http://internetetopinion.files.wordpress.com/2008/01/crisis_management.pd; "Basic Principles For Crisis Communications", Global PR Blog Week 1.0, n.d., http://www.globalprblogweek.com/archives/basic_principles_for.php.

would remain onboard the aircraft, with doors sealed, while the plane is directed to move to a pre-designated location. This would likely entail at least a temporary cessation of air traffic, and a prompt relocation of the aircraft to an isolated area – either on the tarmac or in a hangar – where the scenario can be successfully addressed by first responders and specialists without the danger of additional infections from among the general population.

Once the aircraft is so isolated, authorities will need to *quarantine* those infected or affected. By this time, many of the passengers on the affected "Aether" aircraft can be expected to be sick, dying or deceased. They should not be permitted to mingle with the general population. Rather, authorities will need to isolate and contain them while the biological agent in question is identified. Once it has been, authorities will be able to determine the logical course of action; if the agent is resistant to treatment, extremely virulent or rapidly progressing, decontamination may not be possible, and extended isolation of the passengers until the disease has run its course may be required. If, however, antidotes for the biological agent are readily available, they can be administered to those passengers whose symptoms have not progressed irrevocably. Those successfully dosed can thereafter receive medical treatment, first at an isolated facility and thereafter – should circumstances warrant – at Finnish hospitals. Such a triage, while difficult, will be necessary to ascertain the proper and prudent course of action for dealing with those "Aether" passengers still alive.

Thereafter, authorities will need to *decontaminate* both individuals and affected facilities. This will entail chemical treatments for passengers to whom antidotes have been provided, the destruction of clothing and personal objects, and a comprehensive "scrub" of the "Aether" aircraft. The virulence of the biological agent will dictate the level of severity of the decontamination, and whether or not personal items and the aircraft itself can be salvaged, or whether comprehensive destruction is required.

The Jalasvirta Group article explicitly outlines a strategy that can be taken to address patient care and outbreak containment and decontamination in the event of a CBRN attack. As the paper outlines, a clear chain of command needs to be in place, as does a systematic set of distinct zones, including areas for collection, treatment, and evacuation, through which patients will move depending on the severity of their symptoms.

The study likewise notes the importance of triaging patients, and of acting efficiently and quickly to decontaminate affected individuals, as well as those suspected of being so. Thorough decontamination must be carried out through multiple aqueous and non-aqueous methods, from the simple water shower to reactive foams. Equipment such as protective gloves, boots and garments must be made readily available in order to facilitate proper action without compromising the safety and health of the responders.

On a local level, first responders involved in such a scenario will include, most directly, medical personnel and firefighters. In Finland, municipalities can choose whether the fire and rescue services are provided by a professional fire brigade, a "half-ordinary" fire brigade or a volunteer one. Half-ordinary and voluntary fire brigades rely on non-professional voluntary firefighters who have been trained appropriately.15 The responsibilities of these firefighters include

15) Rescue Services of Finland, "Rescue Operations", n.d., http://www.pelastustoimi.fi/en/rescue-operations/.

containment and damage mitigation, making them "first on scene" in a scenario such as the one outlined above.

With the immediate crisis scenario dealt with, authorities will need to *investigate* the source of the incident and its perpetrators. Doing so will require the combined efforts of local, national and international law enforcement agencies, given that the origin of the incident is located overseas. Critical information to be gathered includes: the perpetrators of the attack; their objectives and/or demands; agents and operatives located inside Finland; as well as agents and operatives located throughout Europe and beyond. As with the attacks of September 11, 2001, authorities need to know promptly the origins of the attack, its motivations and its likely intended effects in order to gauge whether an ongoing threat to national security exists, as well as to aid with criminal forensics and identification of the biological agent itself.

The scenario above will entail a multi-tier public relations strategy on the part of the Finnish government, carried out to communicate three overarching messages.

1) *Transparency*. Given the nature of today's 24-hour news cycle, and the transnational character of the "Aether" attack itself, the news media should be expected to become a factor early on in any such crisis. The imposition of a news blackout for an extended period of time will be difficult, if not impossible. Rather, the Finnish government should strive to be transparent in its handling of the crisis, clearly communicating to its citizenry the steps that have been taken to assure their security and resolve the situation. Given the gravity of the scenario – that of a WMD attack upon Finnish soil – the population will need knowledge of, and assurances about, the steps being taken by their government.
2) *Competence.* As they do so, it will be extremely important for national authorities to communicate to Finnish citizens promptly that the situation is under control. Details of the protocols being taken by first responders, and evidence that the Finnish government possesses a competent and comprehensive plan for securing and defusing the crisis, will be necessary to establish and maintain public trust throughout the disaster period.
3) *Containment*. In the aftermath of the immediate response to the "Aether" scenario, authorities should take pains to reassure the populace that the outbreak has been successfully contained and defused. Doing so would allay public fears, and stave off public disorder, mass movement or social disturbances that may otherwise result.

In fulfillment of these objectives, a series of practical steps should be taken. These include convening press conferences and establishing dedicated telephone lines for inquiries from concerned citizens and family members. As well, it would be prudent to create a dedicated official website (or, at the very least, a resource webpage), which would serve a dual purpose: to disseminate information among the general population and media, and to allow those with information regarding the incident to identify responsible officials and communicate with them. Additionally, Finnish authorities would benefit from embracing social media outlets such as Youtube and Twitter, and harnessing them to provide rapid, responsive messages (via video or text) that communicate official messages regarding the disaster to diverse audiences.

These responsible parties to do so are clearly defined under Finnish law, which states

that municipalities are jointly responsible for rescue services within regions determined by the Government. There are twenty-two such rescue service regions in Finland.[16] Each ministry, within its mandate, directs and monitors the implementation of measures relating to securing vital functions and the required development of capabilities, which are monitored by the government's *Security and Defense Committee*, which in turn relays updates to the national political leadership. With regard to communications and informational measures, the general rule is the municipal and regional agencies overseeing disaster response activities are also responsible for the content of their communications. Each disseminates information about its activities. The Government Communications Unit, meanwhile, is responsible for the Government's and the Prime Minister's communications, as well as for coordinating the dissemination of official information.[17] The municipalities would report to the Ministry of Defense and the Ministry of the Interior who would coordinate with first responders and the media. It is important to note here that, though there is an emphasis on municipalities maintaining control over emergency situations in theory, in practice were a bioterrorism attack to occur, these ministries would likely be much more heavily involved and become the primary players in the response.

✓ *3.2 Scenario II: Breakout and National Crisis*

The second notional set of events relating to the Aether Scenario envisions a biological attack using aviation that is not contained, and expands to become a national crisis within the borders of Finland. Such a scenario presupposes that the affected aircraft and its passengers are not promptly and/or properly sequestered and decontaminated, and that as a result the biological agent is introduced into the broader Finnish population (either through the mingling of infected passengers with ordinary citizens, through the proximity of uninfected citizens to contaminated objects or air, or some other method).

In such a notional scenario, the nature of the biological agent would be extremely important. Levels of severity, and speed of dissemination, would dictate the scope of the national response that would need to be mobilized to adequately respond. In the event that the agent is slow-moving, or transmitted by bodily fluids or touch (rather than airborne), authorities would do well to focus their response plan primarily on constraining the movement of infected individuals, and sequestering them. On the other hand, if the agent is particularly virulent and/or airborne, a quarantine of the general population – via curfews, or even the imposition of martial law – may become necessary.

The immediate burden of response in such a crisis scenario would fall to regional rescue services. Finland is divided into twenty-two rescue service regions. The functions of regional rescue services are performed in cooperation between the municipalities of the region, as outlined by law. Within a particular rescue service region, there is a rescue department with full-time and part-time personnel.

Regional rescue services must be able to respond to the incident swiftly and efficiently,

16) Ministry of the Interior of Finland, "Rescue Services: Organisation", n.d., http://www.intermin.fi/intermin/home.nsf/pages/33EB8BEA7326C131C22573B7004328C3?opendocument.

17) Office of the Prime Minister of Finland, *Government Communications in Crisis Situations and Emergencies*, Prime Minister's Office Publications 20/2008.

and to competently coordinate collaboration as needed with other rescue service regions. Success here hinges upon the speed of response and the type of help summoned to the accident site. As a result, rescue service regions are divided into risk areas on the basis of accident probability. Accident probability is greatest in places where there are lots of people, buildings, traffic, or industrial activities. In risk area 1, a rescue unit must arrive at the accident site within six minutes, in risk area 2 within ten minutes, and in risk area 3 within twenty minutes from the alarm. In risk area 4 (i.e., sparsely populated areas), no such time limit has been set.[18]

Communications between regional responders is also crucial. Command centers equipped with communications links are built during normal conditions. In situations of emergency, the Ministry of the Interior, provinces, and rescue services regions will bring these centers into use. Each municipality also is required to build a command center that can function during any emergency situation.[19] These communications nodes would be used in responding to a national bioterrorism incident. That being said, this method is only effective if there is training on messaging that would be appropriate for a massive bioterrorist attack. The lack of information indicating this kind of training indicates a certain level of unpreparedness in the Finnish system of emergency response.

The public information response in the event of such a national disaster is likely to be governed by the Finnish Defense Administration. One of the Administration's main messages is that "Finland has the willpower, the skills and the means to defend itself".[20] This is practically accomplished through a system of military service; capable and efficient defense forces; a strong national will to defend the country coupled with voluntary military service; and cooperation between authorities. All of which provide a cadre of military personnel capable of assisting in national response in the event of an attack such as the one described in the "Aether" scenario.

The actors and their respective responsibilities are outlined in the *Public Policy Strategy of the Finnish Defense Administration*. The Ministry of Defense is responsible for coordinating communication within its own administrative branch and coordinates central matters related to communication between the defense administration and the rest of the state. The ministry sets strategic goals for defense administration communication and ensures the preconditions for it are met, as well as directing and monitoring defense communication practices as a whole.

The Public Information Division of the Defense Staff is responsible for directing the external messaging of the Defense Forces. These include centralized communication, community marketing and public image control. In addition, it provides expert services on communication and it is in charge of military music and entertainment in the Defense Forces.[21] Also, the Defense Administration's Building Unit is responsible for the implementation of its communication activities in accordance with the defense administration communication framework. The strategic objectives of this communication would be to "plan, implement and develop ways in which the administration can be in touch with society".[22]

18) Rescue services in Finland, "Standard of Service In Regional Rescue Services", n.d., http://www.pelastustoimi.fi/en/267211/.

19) Rescue services in Finland, "Standard of Service In Regional Rescue Services", n.d., http://www.pelastustoimi.fi/en/267211/.

20) Ministry of Defence of Finland, *Public Policy Strategy Of The Finnish Defence Administration*, n.d., http://www.defmin.fi/files/1274/Public_policy_strategy.pdf.

21) Ibid.

22) Ibid.

The Finnish Government has multiple agencies that would be integral in the response to a bioterrorist attack. On a national level, the Ministry of the Interior, who developed the nation Rescue Services strategy, would be in contact with some of the first responders, such as the police force and those working on border control.[23] In addition to the aforementioned first responders, the medical responders would report to the Ministry of Social and Health Services. Vaccinations would flow through this Ministry to address a national pandemic situation or the like. This Ministry would also activate a nationwide digital authority network, called VIRVE, which is operated by the state-owned State Security Networks. The Ministry of Transport and Communications likewise would be heavily involved in delivering information through various media channels, as well as establishing communications networks.[24]

The Ministry of the Interior would then work with the Ministries of Defense and the Cabinet Committee on Foreign and Security Policy on implementing the larger Finnish counterterrorism strategy.[25] The objectives of this effort would be similar to those of the initial scenario listed above. The most immediate need will be for federal authorities to *contain* the incident and *isolate* those infected. Contrary to the conditions identified in Scenario I, however, doing so will not simply be a function of isolating the affected plane and controlling the movements of its passengers. Rather, the presumption is that – as a result of initial confusion, oversight, or violation of decontamination/isolation procedures – those passengers and/or items affected are allowed to travel, expanding the zone affected by the biological agent geographically far beyond the immediate confines of the airliner and airport.

In this case, the net cast by first responders would need to be much broader, and encompass not only those immediately affected as part of the "Aether" scenario, but also people subsequently placed into close proximity with them. Authorities should expect a series of secondary and tertiary "breakouts," in which those subsequently exposed to the biological agent via human transmission become ill themselves. In such events, those who have fallen ill will need to be quarantined also, and the people that had been in close proximity to them identified, isolated and placed under close observation.

Depending on the nature of the pathogen, the Cabinet will issue recommendations to first responders, medical profession, and general public. To the extent possible these recommendations must be generic and prepared well in advance, so that the only modifications during the crisis are based on the nature of the disease and its contagion pathways.

A successful containment in a breakout scenario is likely to entail the establishment of isolation and quarantine facilities in multiple cities throughout Finland, corresponding with the cities of origin and destination of passengers on the affected airplane. It is also likely to entail a large cadre of first responders and local authorities to be placed on alert to watch for subsequent incidents of illness or outbreak.

23) Ministry of the Interior of Finland, "Finland's Participation In International Crisis Management in 2010-2011", n.d., http://www.intermin.fi/intermin/home.nsf/pages/index_eng.

24) Ministry of Transport and Broadcasting of Finland, "Television Broadcasting", n.d., http://www.lvm.fi/web/en/7.

25) Government Communications Unit of the Government of Finland, "First National Counter-Terrorism Strategy Being Prepared", Press Release 61/2010, http://www.government.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=288506

Depending on the severity of the symptoms and virulence of the biological agent, the federal government would also need to consider ways to control the population. Such steps, from the imposition of a curfew to the closure of schools and public meeting spots to the enactment of martial law and mandatory sequestering of citizens, would be intended to control the movement of the population and thus the spread of the disease. Doing so may entail a mobilization of the nation's armed forces. Unlike institutions such as the U.S. Federal Emergency Management Agency (FEMA) or the Russian Ministry of Emergency Situations, Finland does not currently have a special emergency authority. In lieu of this, Finland has developed a strategy of "Total Defense," which includes dispersed mobilization and flexible readiness responding to various military threats. Defense planning is organized to counteract a regional crisis that may have effects on Finland.[26]

Likewise, authorities will need to lock down and subsequently *decontaminate* affected facilities. Unlike in Scenario I, however, these may not simply be airplanes or hangars. Rather, depending on the duration of the crisis and its scope, it may require treating dozens of public meeting places in various cities throughout Finland, at considerably monetary cost and via the mass mobilization of emergency response and hazmat response personnel and equipment. Irrespective of the specifics, authorities should expect certain buildings, neighborhoods, or even parts of cities to experience travel and mobility restrictions, and stand ready to have law enforcement or military personnel enforce guidelines for ordinary citizens.

During a national crisis, the Emergency Response Center Administration, which is maintained by the government, operates under the Ministry of the Interior. It consists of fifteen emergency response centers throughout the country.[27] It would assume a leading role in coordinating such a decontamination operation, even as smaller emergency response centers serve as communication centers for rescue, police and social and health authorities, supporting and assisting first responder units.

Finally, as in Scenario 1, authorities will be required to *investigate* the source of the biological attack. Doing so will require the combined efforts of local, national and international law enforcement agencies, given that the origin of the incident is located overseas. Critical information to be gathered includes: the perpetrators of the attack; their objectives and/or demands; agents and operatives located inside Finland; as well as agents and operatives located throughout Europe, Asia (where the flight originated) and beyond. As with the attacks of September 11, 2001, authorities need to know promptly the origins of the attack, its motivations and its likely intended effects in order to gauge whether an ongoing threat to national security exists, as well as to aid with criminal forensics and identification of the biological agent itself.

Like Scenario I, this fact pattern entails the creation of an official multi-tier public information strategy, focusing on much the same core messages. As the crisis sweeps over the country, it is likely to be both picked up and amplified by local and international media. With a high novelty value attracting attention, a nationwide incident of this sort, media exclusion from the decision

26) Finish Defence Staff, International Division, "Annual Exchange Of Information On Defence Planning 2005", March 2005, http://www.mil.fi/perustietoa/julkaisut/defence_planning_2005_finland.pdf.

27) Ministry of the Interior of Finland, "Emergency Response Centres", n.d., http://www.intermin.fi/intermin/home.nsf/pages/473F8F0385949A27C22573B70043E036?opendocument

making cycle is simply not an option. Rather, the Finnish media will need to be fed with timely, accurate information that they can convey to the citizenry about the nature of the threat, and the state of the federal response. Moreover, as a bio-terror attack in Europe is an unprecedented security event, Finland will quickly become an international source of news and mass media magnet. In such a situation the Finnish government needs to prepare a global communications strategy, complete with multi-lingual resources and messages that are well-thought-through in advance and counter the inevitable panic.

To avoid widespread panic, the Finnish government will need constant, clear and reassuring messaging to its citizenry, neighboring states, EU partners, and the world. Utilizing all available media (radio, television, World-Wide Web, and print), authorities will need to communicate the current state of the response effort. They will also need to provide ordinary Finnish citizens with step-by-step instructions and guidance as to how to 1) keep themselves safe and avoid contamination; 2) what steps the Finnish government is currently taking; and 3) what is required from ordinary citizens to assist with this goal.

In fulfillment of these objectives, a series of practical steps should be taken. These include condemnation of those involved in the attack. It would also communicate the formation of an emergency team that would be available to provide additional support and manpower to localities.[28]

Furthermore, messages should describe and communicate the skills and competence of the first responders and medical teams, including doctors and nurses. Interviews with health providers should be arranged, where they can communicate proper procedures aimed at stemming the spread of infection, prevent panic, calm the population down and boost morale.

Communications on the Internet would also be essential. The Defense Administration uses their contacts with authorities, external partners and target groups to influence the public via experts. In regard to internal publicity, communication is maintained inside and between the actors of the defense administration. International publicity is defined as having contact with foreign partners (diplomatic missions, security and defense establishments), international organizations and foreign media.[29]

If the situation requires immediate protective measures, people are informed through a general alarm siren. Then, people would listen to the radio and television to learn the instructions for further steps. Instructions include information on how and when to protect foodstuffs and go outdoors. There will be news bulletins on every channel. They will interrupt whatever broadcast is currently occurring. Specifically regarding a bioterrorist attack, Finland's National Infectious Disease Register (NIDR), would transmit real-time information over the internet to local, regional, and national health authorities.[30] As ordered by law, the Public Health Institute would use a web-based sentinel surveillance system, that is akin to a viral surveillance system,

28) Ministry of Foreign Affairs of Finland, "Finnish Government Condemns London's Terrorist Attacks And Does Not Believe They Affect The World Championships", July 7, 2005, http://formin.finland.fi/Public/default.aspx?contentid=64468&nodeid=15145&contentlan=2&culture=en-US.

29Ibid.

30) http://stm.teamware.com/Resource.phx/vastt/tervh/lintuflunssa/kieliversiot.htx.i753.pdf

which would automatically extract information from patient record databases and transfer that data into the NIDR every 24 hours, allowing for an effective method of monitoring epidemics.[31] What develops from the monitoring of any breakout of a pandemic would be used to inform the public on the progress of any possible pandemic.

If necessary, a Government Information Center will likewise be established. The entity can issue orders to state authorities as regards the content of information. According to the Finnish government's strategy, the information service has a role in maintaining overall psychological crisis tolerance.[32] This kind of communication is intended to keep the public calm, as well as ensure that the information the public is receiving is accurate.

3.3 Scenario III: Breakout and Continental Response

In the event that the "Aether" scenario reaches the level of Continental pandemic, the response would be both similar and different from those outlined above. Most directly, two responses would be required:

Containment. Unlike the above scenarios, the spread of the "Aether" agent outside of the borders of Finland, and throughout the Eurozone, would create a crisis of civil defense, a containment failure, and a public information crisis of truly continental proportions. Individual member states that are affected would each need to establish containment protocols, health surveillance and reporting procedures, and treatment routines and facilities, in various urban centers if necessary, in order to mitigate – or at least slow – the spread of the biological agent. They would also need to coordinate closely with the European Commission, creating a horizontal approach involving multiple EU agencies and governed by the EU's 2003 *Strategy against Proliferation of Weapons of Mass Destruction* – also known as the EU WMD strategy – and other related operational instruments.[33]

The containment protocols followed by these agencies will likely be similar to those developed following the global outbreak of the H1N1 "swine flu" some two years ago. At that time, the European Union developed a strategy for responding to EU-wide or international pandemic threats, which states that "all necessary appropriate measures should be taken for public health protection."[34] This includes travel restrictions and other policies aimed at protecting European citizens and coordinating the evolving response to the A/H1N1 virus on the Continent.[35]

Isolation and treatment of the infected. In the event of pandemic, the sheer number of the sick, infected and/or dying is likely to be extensive. High volumes of such patients, particularly highly contagious ones, are likely to put significant strain on existing national resources among member states – especially less prosperous ones. Here too, a coordinated approach among

31) Ibid.

32) Office of the Prime Minister of Finland, *Government Communications in Crisis Situations and Emergencies*.

33) *EU Action Plan On Chemical, Biological, Radiological And Nuclear Security*, n.d., http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0030_en.htm.

34) European Commission, "Message From Commissioner Vassilou: 'Pandemic (H1N1) 2009: We Need To Ensure That Europe Is Prepared", n.d., http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0030_en.htm.

35) Ibid.

Member states is essential. By virtue of the disease's spread, some states and municipalities are likely to be harder hit than others. It will be necessary for a "federal" level agency or body to coordinate and allocate resources according to need and demand. Such a function can be played by the European Center for Disease Control, or ECDC. In order to support the Member States in their capacity to respond to outbreak situations related to communicable diseases or diseases of unknown origin, the ECDC aims to ensure the rapid mobilization of outbreak assistance teams whose expertise may include epidemiology, clinical medicine, public health, infection control, etc. The Center pays particular attention to the mobilization of microbiology expertise, through the outbreak assistance laboratories network.[36]

Beyond the immediate response, an Aether pandemic scenario is likely to involve an extensive – and extended – mobilization of resources across the Continent. On a national level, the Member states are primarily responsible for many of the areas of work covered by current policy. They are responsible for protecting their citizens from CBRN threats through a host of different measures, and with the involvement of a wide range of responsible authorities. It is the States' law enforcement, civil protection and medical services which will be first on the scene of an incident, and it is their ambulances, hospitals and stockpiles of counter-measures which will need to provide both for emergency medical assistance as well as aftercare. [37]

However, given the transnational nature of the scenario, these responses would need to be overseen – and, when necessary, augmented – by the European Commission and its relevant institutions. These would be rapidly re-tasked or mobilized as necessary to assist in mitigating the crisis. They include:

- the European Centre for Disease Control;
- the European Food Safety Agency;
- the Civil Protection Monitoring and Information Centre (MIC);
- the Joint Research Centre (JRC);
- Europol; and
- the Joint Situation Centre of the European Council

The European Union likewise would have multiple health agencies at its disposal to react effectively to contain and address the spread of a health threat. The Health Security Committee and existing information exchange mechanisms such as the Early Warning Response System, Rapid Alert System-Taskforce on. Biological and Chemical Agent Attack and the Rapid Alert System for Food and Feed play an important role in the implementation of health related measures of the Action Plan.38 Additionally, one of the more influential agencies is the European Union Task Force on Biological and Chemical Agent Threats. The Task Force provides guidelines for different bioterrorism scenarios, such as plague, anthrax, and smallpox. These guidelines briefly outline if isolation is needed, what antibiotics are to be administered, and provide a description of symptoms.39

36) European Centre for Disease Prevention and Control, "Response", n.d., http://www.ecdc.europa.eu/en/activities/response/Pages/PreparednessandResponse_Response.aspx.

37) Ibid.

38) *EU Action Plan On Chemical, Biological, Radiological And Nuclear Security*, n.d.,http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0030_en.htm.

39) European Commission, "European Clinical GuidelinesFor Bioterror Agents", n.d., http://ec.europa.eu/health/ph_threats/Bioterrorisme/clin_guidelines_en.htm.

With regard to communications, a number of procedures exists that would be applicable for such a pandemic scenario.

- *Early warning to European citizens and to the world*. As the disease spreads and governments struggle to keep the contagion under control, it will be imperative for both National and Continental authorities to prevent further infection. To do so will necessitate an "early warning" protocol under which citizens of Eurozone nations not yet affected by the pandemic are apprised of the situation and instructed to take specific precautions to avoid contamination. Such an "early warning" plan would need to be simultaneously implemented along multiple professional and mass media (print, television, Internet), leveraging the EU's latent capabilities enumerated under the EU's *COUNCIL CONCLUSIONS ON ADDRESSING CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR RISKS AND ON BIO-PREPAREDNESS*. For example, the EU's Rapid Alert Systems can help provide timely and lifesaving notification.[40] .[41] Though one can assume that the EU and its Member States would come in contact with other global players, such as the US, China, and WHO, there currently is no procedure outlined on what those direct communications would be from the EU itself. This is underlined by the subjective nature of the relationship between each Member State as other nations, particularly the United States.
- T*ransparency and confidence-building*. By its nature, mass pandemic will cause mass panic. There is likely to be considerable migration, both within the European Union and from the EU abroad, as citizens seek to escape the disease. Such a scenario, if left unchecked, runs the risk of spreading the disease further, as individuals who unknowingly had been exposed to the bioagent carry it with them abroad. To head off such an eventuality, citizens of the EU and its constituent countries will need to know that their respective government, and the EU itself, has implemented a comprehensive, timely and far-reaching response plan – and that such a response plan is producing the desired results. Like the "early warning" protocol outlined above, this message would need to be communicated across multiple mediums simultaneously, and done so by figures of national and Continental authority. The principal goal would be to allay the quite understandable panic that is likely to set in as the crisis progresses. Mass media program should clarify that "standard of care" against infectious diseases is as high or higher than anywhere in the world, and that the EU governments have capacity to stop the epidemic, so that the citizens are better off staying in the EU area.
- *Hardening and protection*. At the same time, it will be important for the EU and its Member states to communicate to the general public that measures are being taken to ensure the safety and security of existing WMD material within the EU area itself. The volatility of CBRN arsenals, and public concern about them, suggests that the issue of WMD security, while not an immediate worry under the scenario outlined, would quickly rise to become an issue of widespread concern. Assurances that Continental stockpiles are safe and secure therefore will need to be an important secondary public policy message.

40) Document of the Council of the European Union, November 16, 2007, http://register.consilium.europa.eu/pdf/en/07/st15/st15127.en07.pdf.

41) Document of the Council of the European Union, November 16, 2007, http://register.consilium.europa.eu/pdf/en/07/st15/st15127.en07.pdf.

- *Response and Prediction*. Crucial to public trust in the aftermath of a pandemic is a credible message that such a disaster will not happen again. The credibility of European authorities in this regard will rest upon their predictive capability – the sum total of the intelligence and law enforcement capabilities marshaled by the EU to identify and apprehend the perpetrators of the attack, and to monitor similar potential threats. The European public must be made aware of the scope of this ongoing intelligence effort, in order to be reassured by it.

The implementation of these priorities and messages would be undertaken primarily by existing EU structures, as outlined in the EU Action Plan.[42] However, as needed, these could be augmented by a small number of new working structures – temporary working arrangements with "specific and time-limited" goals that would be created by the EU and its constituent bodies. As in Scenarios I and II above, the media to be used would be radio, television, print and Internet (including social networking tools), and the methods would be varied and dynamic. Given the size of the European continent, public messaging in the midst of and after a bioterror pandemic would need to be continuous, innovative and encompassing of both EU and national media outlets.

4. Gaps in Current Policy

In both the European Union and among individual European states, there is at present no central body responsible for a strategy in communications to the public in emergency situations. The European Union currently boasts multiple, overlapping agencies with a mandate for public information dissemination, but without a clear hierarchy or chain of command as to the agencies themselves or the messages they would formulate. Among many member states, meanwhile, current protocols dictate the involvement of multiple ministries and branches of government, often to the detriment of message cohesion and clarity. The reasons are practical; these agencies need to better ensure that local authorities and responders are trained to respond and communicate properly, and more effectively use multiple forms of media beyond traditional broadcasting (i.e., Web 2.0, Twitter, etc.)

On a greater level, there is a lack of consistency of messaging between Member States involved in the crisis and EU bodies, as was demonstrated during the Madrid bombings. This gap can be traced back to the lack of single EU body responsible for communications and public information; simply put, there are too many bodies that touch upon only a fraction of the media message that would be intrinsic to any bioterror response.

To this end, the establishment of an EU body or committee that creates a uniform and consolidated messaging campaign during crises would help alleviate contradictions in messaging and disaster response delays. Such a body, to be effective, would require professional staff familiar with social media, as well as conventional broadcasting. It would also need to collect and consolidate information from other various EU bodies involved in the crisis – in effect serving as an information clearinghouse. The establishment of such a system on an EU-wide scale, similar to what the U.S. has done, should be seen as essential for member states to prepare for a massive bioterrorism attack, and to maintain the authority and reputation of the EU.

42*) EU Action Plan On Chemical, Biological, Radiological And Nuclear Security.*

Heikki Silvennoinen, Timo Lairio & Pertti Jalasvirta: Patient Handling - Decontamination of CBRN Situations: Description of the Process

1. Introduction

This study is focused on a CBRN incident with symptoms on a passenger plane. However, the basic principles, methods and equipment can be utilized for various passenger numbers and also for other transportation measures (bus, ship, train, subway etc.).

The purpose of this study (patient handling) is divided into three main targets, and four additional targets for the LIVEX exercise:

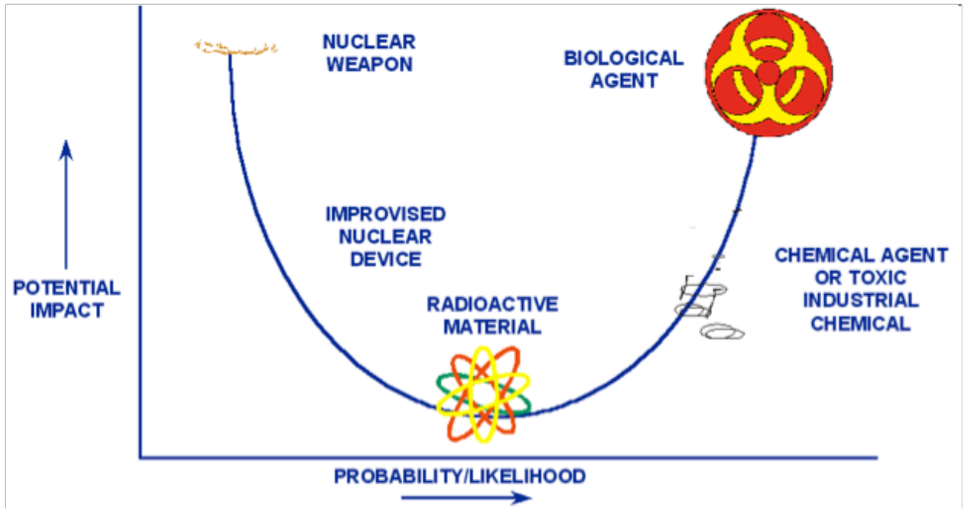
- To generally introduce the CBRN threats during a crisis and peace time.
- To generally introduce the decontamination methods and procedures.
- To generally introduce the principles and operations of passenger handling in case of a CBRN incident.

2. Definitions

- CBRNE = Chemical, Biological, Radiological, Nuclear and Explosives
- NBC = Nuclear, Biological, Radiological (older abbreviation of CBRNE)
- CWA = Chemical Warfare Agent
- BW = Biological Warfare
- Pulmonary = Lung related
- Cutaneous = Skin related
- Virus = Requires cells to reproduce, contagious
- Bacteria = Living organisms, contagious
- Toxins = Poisonous, do not reproduce, non contagious
- Detection = First alarm of substance (no verification)
- Analyzed = Confirmed definition of substance
- PPE = Personal protective equipment (mask, suit, gloves, boots etc.)
- Hot Zone = Contaminated area
- Warm Zone = Decontamination area
- Cold Zone = Contamination free area
- Triage = Casualty prioritization
- PPE = Personal Protective Equipment
- PAPR = Powered Air Purifying Respirator
- Hazardous substance = defined as any substance an exposure to which may result in adverse effects on the health or safety

3. CBRN Threats - General

CBRN-threats are based on agents causing a widespread disaster when compared to conventional weapons. Among these are chemical (C), biological (B), radiological agents (R) and nuclear weapons (N).



Picture by Heikki Silvennoinen, 2003.

The society should be prepared to counter these threats by means of various measures.

- Understanding the threats and preparing for them
- Co-operation between various authorities (time is the essential dimension)
- Alarm and surveillance networks
- Material preparedness and logistics
- Training and practice of operators and methods of action in a CBRN situation

The threats range from local accidents to international conflicts and even to terrorism. These threats are potential during peace or increased international tension. The threats are presented in order of seriousness.

International experts have repeatedly stated that acts of CBRN-terrorism are only a matter of time and extent and no nation can in the future be sure of the security of herself and her citizens.

The present doctrines of the superpowers have taken into account the possibility of threat and employment of CBRN-weapons in achieving a political goal.

The daily running of the society involves numerous operators using substances classified as CBRN-agents, which can cause unintended or deliberate hazardous situations.

✓ *3.1. CBRN Warfare*

3.1.1. Chemical Warfare Agent (C)

A chemical agent is defined as a chemical substance which is intended for use in military operations to kill, seriously injure, or incapacitate man through its physiological effects. The term excludes riot control agents when used for law enforcement purposes, herbicides, smoke and flames.

Chemical agents can attack different physiological systems and variously enter the human body by ingestion, inhalation or through the eyes and the skin. They can be classified, for example, as blood, choking, nerve or blister agents.

They can also be divided into lethal, damaging and incapacitating agents although there is not always a sharp dividing line between the effects.

They can be delivered as vapour, liquid, solid or aerosol form. CW agents are likely to be employed to produce casualties (non-persistent) or contaminate ground and/or equipment (persistent). Both may have a similar effect on personnel.

3.1.2. Some categories of CWAs

- Blister Agents/Vesicants - Chemicals that severely blister the eyes, respiratory tract and skin on contact.
  - Mustards, Distilled Mustard (HD), Mustard Gas (H) (sulphur mustard), Mustard/lewisite (HL), Mustard (T), Nitrogen Mustard (HN-1, HN-2, HN-3), Sesqui Mustard (H), Lewisite/chloroarisine Agent (L, L-1, L-2, L-3), Phosgene oxime (CX)

- Blood Agents - Poisons that affect the body by being absorbed into the blood.
  - Arsine (SA), Carbon Monoxide, Cyanide-Cyanogen chloride (C, Hydrogen Cyanide (AC), Potassium Cyanide (KCN), Sodium Cyanide (NaCN), Sodium monofluoroacetate (compound 1080)

- Choking/Lung/Pulmonary Agents – Chemicals that cause severe irritation or swelling of the respiratory tract.
  - Ammonia, Bromine (CA), Chlorine (CL), Hydrogen Chloride-methyl bromide, methyl isocyanate, Osmium Tetroxide, Phosgene, Diphosgene (DP), Phosgene (CG), Phosphine, Phosphorus (elemental, yellow or white), Sulfuryl fluoride

- Incapacitating Agents - Drugs that make people unable to think clearly or that cause an altered state of consciousness.
  - 3-Quinuclidinyl Benzilate (BZ), Fentanyls and other opiods.

- Nerve Agents – highly poisonous chemicals that work by preventing the nervous system from working properly.
  - G-agents-Sarin (GB), Soman (GD), Tabun (GA)
  - V-agents-organophosphates (VX)

3.1.3. Non-Persistent Chemical Warfare Agents

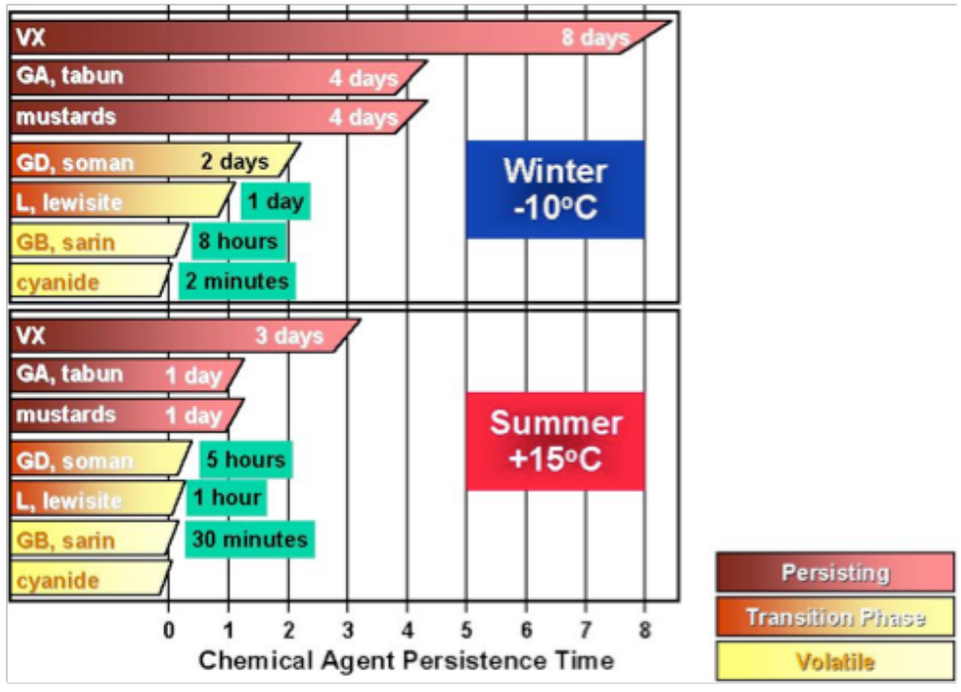
Non-persistent chemical agents have a considerable casualty producing capability, mainly by inhalation. The time in which they present a hazard is relatively short compared to persistent agents, and they usually do not significantly contaminate ground, personnel or equipment, unless absorbed into paint, rubber, plastics etc.

3.1.4. Persistent Chemical Warfare Agents

Persistent chemical agents produce contact, ingestion and respiratory hazards and can be disseminated in liquid, aerosol or solid forms (dusty agents).

Contamination from persistent agents decomposes naturally with time and can last from hours to weeks, depending on the agent type, quantity delivered, weather conditions and the degree of chemical hardening of the contaminated surface.

The contamination problem created depends upon the extent to which the agent has been absorbed into surfaces. Adsorbed agents pose a respiratory hazard that will persist for longer than the hazard associated with free agents. The desorption of a persistent, non-volatile agent can also create a residual contact hazard.



Persistence of some CWAs
Figure by Noblis.org

3.1.5 Modified or Thickened Chemical Warfare Agents

The physical properties of chemical agents may be changed by the addition of different materials so that:

a. The proportion of agent disseminated by missile or aircraft spray tanks that will reach the target is increased.
b. The persistency of the agent will be increased.
c. The adhesion of droplets to vertical surfaces will be increased.
d. Decontamination will be made more difficult, although the physical appearance of the thickened agents may make them easier to locate.

✓ 3.2. Biological Agents (B)

There are many types of potential biological agents, including materials such as bacteria, viruses and toxins. They can be delivered, usually as an aerosol, either through some form of spray or bursting ammunition.

Unless deposited as a spore (e.g. anthrax) many Biological Warfare (BW) agents may present only a short duration hazard since they decay in climatic conditions of heat and humidity and under ultra-violet light but some of them could be present for a longer time. Whilst most BW agents are effective through the respiratory or ingestion route into the body, some toxic biological agents are effective through the skin.

3.2.1. Clinical Features

- Pulmonary - Incubation period is 2 to 60 days. Flu-like symptoms follow inhalation. 2 to 4 days after the initial symptoms, abrupt onset of respiratory failure and hemodynamic collapse, widened mediastinum and chest radiograph are suggestive of meiastinal lymphenopathy and hemorrhagic mediastinitis. Gram positive bacilli on blood culture usually shows after the first 2 or 3 days of illness. High mortality occurs if treatment is initiated after the onset of respiratory symptoms.

- Cutaneous - Incubation period is 1 to 7 days. Local skin involvement is evident after direct contact with spores or bacilli. It is usually non fatal if treated with antibiotics.

- Gastro-intestinal - Incubation period is 1 to 7 days. Abdominal pain, nausea, vomiting, bloody diarrhoea and fever usually occur following ingestion of infected foods. Meat is the most common food. Usually fatal after progression to toxemia and sepsis.

The particle size range of a biological challenge delivered will be dependent upon many factors including the nature of the challenge (virus, bacteria etc.), its mode of delivery, dissemination efficiency and environmental conditions. The respirable range for a particulate matter is considered to be in the range 0.1 to 10 µm, with the larger particles in this range being mostly retained in the upper respiratory tract and the smaller particles in this range being less efficiently retained in the lung. Ultrafine particles (<0.1 µm) also deposit in the deep lung due to diffusion. Information indicates that a substantial proportion of viral agents may be in the form

of particles less than one micron in diameter and that these sub-micron particles may retain their infectivity.

A significant fraction of these inhaled particles may be deposited in the deep lung. A bacteriological agent such as Anthrax has a Mass Median Diameter of 2.5 µm or less with a Number Median Diameter of 1.1 µm, a particle size in the middle of the respirable range.

The high priority B-agents (category A):

- Anthrax (Bacillus anthracis)
- Botulism (Clostridium botulinum toxin)
- Plague (Yersinia pestis)
- Smallpox (Variola major)
- Tularemia (Francisella tularensis)
- Viral hemorrhagic fevers (filoviruses, Ebola, Marburg] and arenaviruses [e.g., Lassa, Junin, Machupo]

The second highest priority B-agents (category B):

- Brucellosis (Brucella species)
- Epsilon toxin of Clostridium perfringens
- Food safety threats (Salmonella species, Escherichia coli O157:H7, Shigella)
- Glanders (Burkholderia mallei)
- Melioidosis (Burkholderia pseudomallei)
- Psittacosis (Chlamydia psittaci)
- Q fever (Coxiella burnetti)
- Ricin toxin from Ricinus communis (castor beans)
- Staphylococcal enterotoxin B
- Typhus fever (Rickettsia prowazekii)
- Alphaviruses [Venezuelan encephalomyelitis, eastern equine,western)
- Water safety threats (Vibrio cholerae, Cryptosporidium parvum)

✓ 3.3. R & N Warfare Agents (RN)

Nuclear weapons can produce residual radioactive contamination from neutron-induced activity and fall-out. Such contamination poses proximity, contact, and inhalation and ingestion hazards. Militarily significant fallout can form a contamination hazard stretching for many tens or hundreds of kilometres from the point of detonation.

Unlike chemical or biological contamination, radioactivity cannot be destroyed but only moved from one place to another until it decays naturally.

Radiological challenges may also arise from aerosolised radioactive material derived from weapons involving the deliberate dispersal of radiological material or from damaged nuclear reactor facilities, resulting in the release of radioactive material containing multiple radioisotopes. The particle sizes of a nuclear or radiological challenge will vary depending upon the nature of the weapon employed, distance from the detonation point and environmental factors. The respirable range for particulate material is considered to be in the range 0.1 to 100 µm. The larger particles in this range are mostly retained in the upper respiratory tract and the smaller particles in this range are less efficiently retained in the lung.

✓ *3.4. CBRN Threats During Peacetime*

There is a real threat of a CBRN based incident also during peace time. This threat is caused by natural reasons (like nature, industry or transportation/NaTech) or by terrorist activity (asymmetric threat).

Many counter-terrorist specialists are confident that a major CBRN terrorist attack is only a matter of time. This claim has been repeated several times during the last 15 years.

3.4.1. Domestic or Neighbouring Area Nuclear Power Plant Disaster

There are several power plants based on various technologies e.g. in Finland and neighbouring areas, operating in many types of communities. Even if domestic nuclear security is of very high standards, we must take into account that all closely located power plants are not up to the same security level.

Among the threats are fires, errors in operation, maintenance (e.g. Oskarshamn in 2008), internal and external security and external threats (e.g. airplane accidents).

3.4.2. Transport of Dangerous Substances

E.g. on Finnish roads a total of approx. 12 million tons of substances hazardous to human health are transported yearly (flammable liquids, corrosive materials and gases). Statistically an accident is likely to happen to a truck transporting chlorine/ammonium or sulphur dioxide, a potential cause of an extensive catastrophe.

Rail and sea transport of hazardous substances is another story of its own.

3.4.3. Natural Catastrophes

These may include e.g. pollution of the Baltic Sea, sudden rise of the sea level and other forms of flooding, effects of climate change and seismic incidents. The actual consequences are caused by secondary reasons: availability of drinking water, electricity, hygiene, epidemic diseases, increase in crimes, communal unrest (the Tsunami, Katharina) etc.

3.4.4. Terrorism and Threats by Organized Crime

The so called "dirty bomb" is a weapon of terrorism. The function of the bomb is to create widespread pollution and cause health problems and panic among the population and disturb the structures of society.

Criminals are using more and more threatening means by obtaining e.g. nuclear materials or agents classified as narcotic drugs (e.g. the drifting of the BZ-hallucinogen from former Yugoslavia to the Finnish market). Also smuggling in itself creates a risk of its own.

"Dirty Bomb": What Are the Likely Effects?

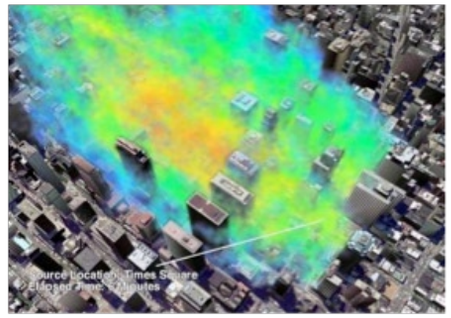
The amount of the explosive need not be large and may not kill anyone. It is unlikely that any immediate fatalities would result from the explosion rather than any effect of the nuclear

material. However, anyone nearby would know a bomb had exploded but would not know it was a dirty bomb unless they were told, since you cannot taste, smell, feel or see radiation. Anyone coming into contact with radiation increases his or her risk of developing cancer. Following the detonation of a dirty bomb attack, only those who receive extremely large doses and are unable to be decontaminated quickly could potentially suffer radiation sickness. Their symptoms might include hair loss and vomiting. Views vary on the number of fatalities that may ensue; there are many variables. The International Atomic Energy Agency (IAEA) in Vienna attempts to keep track of many kinds of radioactive materials as they move around the globe. However, security standards reflect the degree of hazard presented by each material and radioactive materials are used extensively in medicine, industry, agriculture and research. Many of these are easier to acquire than the materials that would be required to produce a nuclear explosion.

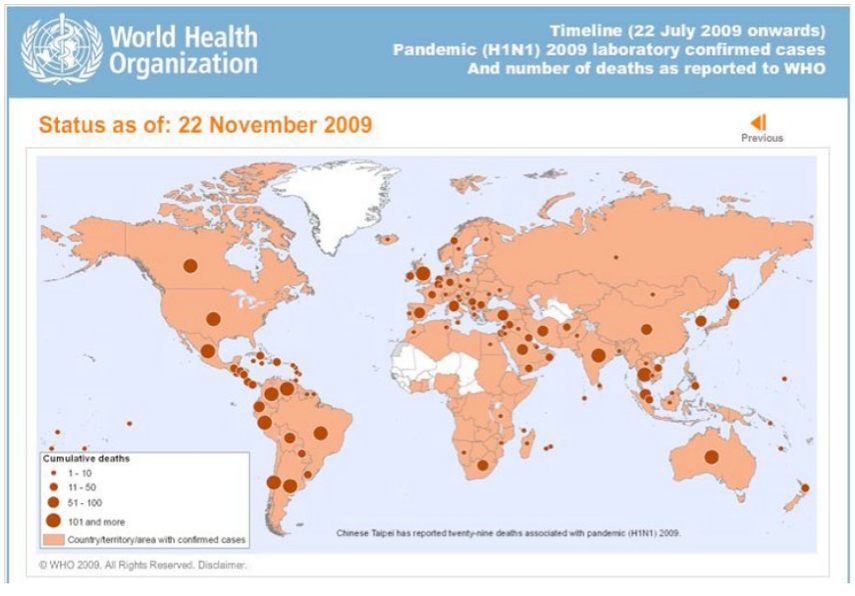
"A bioterrorist attack need not involve nations with advance military powers. One nightmare scenario involves the release of contagious biological agents in a crowded urban area of densely populated developing nation, without the health and scientific infrastructure necessary to identify and quickly respond to the attack".

Marc Ostfied

SAIS Review vol XXIV, 2004 p131-146



Picture by SAIS, 2004.



Picture by WHO presentation/ Pandemic 2009.

3.4.5. Contagious Diseases

The rapidly increasing international travel of citizens exposes society to pandemics easier than before. This problem is accentuated by slow reaction (long germination time) and lack of processes and tools. In addition to this the threat of local bioterrorism (deranged persons) cannot be ruled out.

3.4.6. Hazards Caused by the Infrastructure

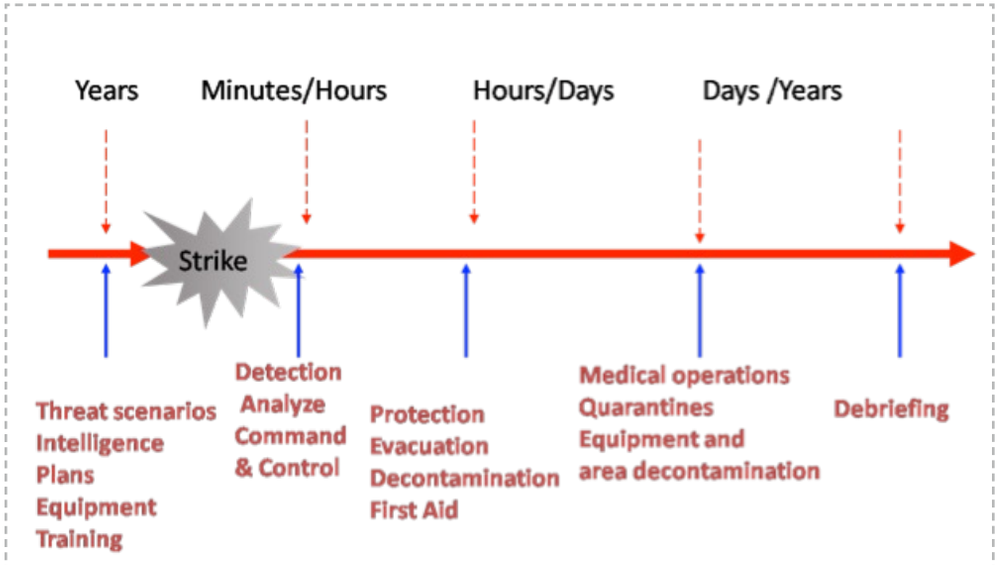
The structures of society itself contain various hazards, such as water pollution (Nokia), contamination of provisions and their supply chain, radiation sources (hospitals, medical industry), Internet (Myyrmanni 2003) and different kinds of production plants and chemical production facilities (e.g. Bhopal, India).

✓ 3.5. Reaction Times to Actualized CBRN Threats

The following describes briefly the CBRN-countermeasures, which by co-operation between different authorities secure the continuity of the vital operations of society and care of citizens at the time of actual CBRN-threat.

The planning and preparations must be done in advance AND trained on yearly basis.

The countermeasures described here are operational actions to limit the CBRN-threat/damages, to save lives and decontaminate exposed persons, equipment and areas and for subsequent operations.



Picture by Heikki Silvennoinen 2010.

4. Decontamination - General

Decontamination is defined as the reduction or removal of chemical (or biological) agents so they are no longer hazards. Agents may be removed by physical means or be neutralized chemically (detoxification).

✓ 4.1. Purposes of Decontamination

The three most important reasons for decontaminating exposed victims are:

- Remove the agent from the victim's skin and clothing, thereby reducing further possible agent exposure and further effects among victims;
- Protect emergency responders and medical personnel from secondary transfer exposures;
- Provide victims with psychological comfort at, or near, the incident site, so as to prevent them from spreading contamination over greater areas.

Rapid physical removal of the agent from the victim is the single most important action associated with effective decontamination. Physical removal includes scraping or blotting off the visible agent from the skin, disrobing, using adsorbents to soak up the agent, and flushing or showering with large quantities of water.

Decontamination of skin is the primary concern, but decontamination of the eyes and wounds must also be done when necessary.

Since the most important aspect of decontamination is the timely and effective removal of the agent, the precise methods used to remove the agent are not nearly as important as the speed at which the agent is removed.

For instance / ANY NERVE GAS:

Even small amounts (several droplets) of liquid nerve agent contacting the unprotected skin can be severely incapacitating or lethal if the victim or responder is not decontaminated rapidly (within minutes) and treated medically.

✓ 4.2. Principles of Decontamination

The following principles of decontamination need to be recognized:

As soon as possible. The sooner decontamination takes place the less contamination is absorbed into material surfaces and the more effective the process will be, so reducing the time and effort needed. This will increase opportunities for reducing personal protection levels and restoring full combat capability.

Only what is necessary. Decontamination procedures place heavy demands on scarce

resources and time. Thus, only those items critical to the pursuit of the mission should be decontaminated.

As close to the contamination as possible. Decontamination needs to be conducted as close to the contaminated area as tactically feasible, both to minimise the spread of contamination and to avoid the relocation of mission critical assets.

Priority. Priority for decontamination of military resources needs to be considered and laid down by the commander so that the achievement of operational objectives is optimised.

The general principles identified to guide emergency responder policies, procedures, and actions after a chemical agent incident were (by SBCCOM/iii):

- Expect at least a 5:1 ratio of unaffected to affected casualties
- Decontaminate victims as soon as possible
- Disrobing is decontamination; head to toe, more removal is better
- Water flushing generally is the best mass decontamination method
- After a known exposure to liquid chemical agent, emergency responders should be decontaminated as soon as possible to avoid serious effects.

✓ *4.3. Decontamination types*

Decontamination can be divided into four types:

Immediate decontamination. Decontamination carried out by individuals upon becoming contaminated, to save life and minimize casualties. This may include decontamination of some personal clothing and/or equipment.

Operational decontamination. Decontamination carried out by an individual and/or a unit, restricted to specific parts of operationally essential equipment, materiel and/or working areas, in order to minimize contact and transfer hazards and to sustain operations. This may include decontamination of the individual beyond the scope of immediate decontamination, as well as decontamination of mission-essential spares and limited terrain decontamination.

Thorough decontamination. Decontamination carried out by a unit, with or without external support, to reduce contamination on personnel, equipment, materiel and/or working areas, to permit the partial or total removal of individual protective equipment and to maintain operations with minimum degradation. This may include terrain decontamination beyond the scope of operational decontamination.

Clearance decontamination. Decontamination of equipment and/or personnel on temporary or permanent removal from an operation to a standard sufficient to allow unrestricted transportation, maintenance, employment and disposal.

✓ *4.4. Methods of Decontamination*

From scientific literature showing the effectiveness of different types of solutions in preventing chemical effects and the wide-spread, ready, availability of large quantities of water that

can be rapidly used in decontaminating large numbers of people, the MCDRT determined that mass decontamination can be most readily and effectively accomplished with a water shower system.

Decontamination must be conducted as soon as possible to save lives. First responders should use resources that are immediately available and start decontamination as soon as possible. If specific decontamination systems are not available, the most expedient approach is to use currently available equipment to provide an emergency low-pressure deluge.

The following forms of water-based decontamination are available:

- **Water alone.** Flushing or showering uses shear force and dilution to physically remove a chemical agent from skin. Water alone is an excellent decontamination solution.

- **Soap and water.** By adding soap, a marginal improvement in results can be achieved by ionic degradation of the chemical agent. Soap aids in dissolving oily substances like mustard or blister agent. Liquid soaps are quicker to use than solids, and reduce the need for mechanical scrubbing; however, when scrubbing, potential victims should not abrade the skin. A disadvantage of soap is the need to have an adequate supply on hand. Additionally, extra time may be spent employing it, and using soap may hydrate the skin, possibly increasing damage by blister agents.

- **Bleach and water.** Bleach (sodium hypochlorite) and water solutions remove, hydrolyze, and neutralize most chemical agents. However, this approach is not recommended in a mass decontamination situation where speed is the paramount consideration for the following reasons:
  - Commercial bleach must be diluted and applied with equipment not generally available to e.g. fire-fighters.
  - Skin contact time is excessive. Laboratory studies show that chemical agents and relatively nontoxic, aqueous decontaminants may need to be in contact for durations longer than expected shower durations for a significant reaction to occur.
  - Laboratory studies suggest that bleach solutions at the 0.5% level may not be better than flushing with water alone.
  - Medically, bleach solutions are not recommended for use near eyes or mucous membranes, or for those with abdominal, thoracic, or neural wounds.

In summary, the issues associated with the use of soap and bleach solutions include time delay, dilution and application, medical contraindications, and its efficacy compared to water.

These limitations make the use of soap or bleach solutions less desirable than using water alone.

✓ *4.5. Decontamination Procedures*

Decontamination by removing clothes and flushing or showering with water is the most expedient and the most practical method for mass casualty decontamination.

Disrobing and showering meets all the purposes and principles of decontamination.

Showering is recommended whenever liquid transfer from clothing to skin is suspected. Disrobing should occur prior to showering for chemical agents; however, the decision to disrobe should be made by the Incident Commander based upon the situation.

Wetting down casualties as they start to disrobe speeds up the decontamination process and is recommended for decontaminating biological or radiological casualties.

However, this process may:

- Force chemical agents through the clothing if water pressure is too high
- Decrease the potential efficacy of directly showering the skin afforded by shear forces and dilution
- Relocate the chemical agent within the actual showering area, thereby increasing the chance of contamination spread through personal contact and shower water runoff.

The recommendation is that victims remove clothing at least down to their undergarments prior to showering. Victims should be encouraged to remove as much clothing as possible, proceeding from head to toe. Victims unwilling to disrobe should shower clothed before leaving the decontamination area.

The water pressure should be higher than standard household shower pressures to ensure the showering process physically removes the viscous agent.

The actual showering time will be an incident-specific decision but may be as long as two to three minutes per individual under ideal situations. When large numbers of potential casualties are involved and queued for decontamination, showering time may be significantly shortened. This may also be dependent upon the volume of water available in the showering facilities.

In the course of decontaminating victims, first responders may inadvertently become contaminated. High-pressure, low-volume decontamination showers are recommended primarily for wet decontamination of emergency responders in Level A suits after a HAZMAT incident.

This gross decontamination procedure forcibly removes the contaminant from the personal protective equipment (PPE) worn by the emergency responders while conserving water.

Often a secondary wash, and possible a tertiary wash, and rinse station are used. However, for decontaminating potential victims, a consensus exists among the medical experts that high pressure could force the chemical agent through the victim's clothing onto the skin.

✓ *4.6. Non-Aqueous Decontamination Methods*

The use of dry, gelled, or powdered decontaminating materials that adsorb the chemical agent are appropriate if their use is expedient.

Commonly available absorbents include dirt, flour, Fuller's earth, baking powder, sawdust, charcoal, ashes, activated carbon, alumina, silica gels, zeolites, clay materials, and tetracalcium aluminate. Although these absorbents may be expedient means of decontamination, their efficacy has not been determined.

However, while these non-aqueous materials are effective in removing spots of liquid chemical agent contamination, they may not be suitable for treating mass casualties due to potentially limited availability, relatively high labour requirements, and the need to use these kits quickly after the victim is contaminated.

Reactive foams are often polymeric materials with reactive sites that can readily decontaminate chemical warfare agents. Oxidants, nucleophiles, and/or enzymes are bound to the polymeric backbone of the foams or gels, and when the chemical warfare agents contact the foam or gel, they encounter the reactive site and are detoxified.

Bacterial organophosphorus acid anhydrases have been placed in fire fighting foam to increase decontamination efficiency within 30 minutes with low residual contact hazard (~1 g/cm2). They have also been placed into the fire fighting spray ColdFire and have shown >99% decontamination efficiency within 15 minutes with the same low residual contact hazard as in fire fighting foam.

Enzymes were used by TEU in support of the 1997 G7 summit in Denver. The foams can be mixed with water and various co-solvents to aid in their deployment. Foams can be engineered to use limited amounts of solvent in order to reduce their dependency upon solvent volume and to aid in the cleanup after deployment. After the solvent evaporates, the foams collapse and turn into a powder, allowing for a simplified, final clean-up operation.

However, since researchers have not identified a single enzyme that is effective on all classes of chemical agents, several enzymes would have to be used simultaneously.

✓ *4.7. Operators Personal Protective Equipment (PPE) - Considerations*

During victim decontamination procedures, the hazard to healthcare workers is strictly from secondary exposure and "depends largely on the toxicity of the substance on the victims' hair, skin, and clothing; the concentration of the substance; and the duration of contact [first responders have] with the victim".

Application: Protective equipment, including personal protective equipment for eyes, face, head, and extremities, protective clothing, respiratory devices, and protective shields and barriers, shall be provided, used, and maintained in a sanitary and reliable condition wherever it is necessary by reason of hazards of processes or environment, chemical hazards, radiological hazards, or mechanical irritants encountered in a manner capable of causing injury or impairment in the function of any part of the body through absorption, inhalation or physical contact (vi.).

Evidence in the U.S. and abroad show that unprotected healthcare workers can be injured by secondary exposure to hazardous substances when they treat contaminated patients.

However, operators that make a conscientious effort can limit the secondary exposure of healthcare workers to a level at which chemical protective clothing (including gloves, boots, and garments with openings taped closed) and PAPRs will provide adequate protection from a wide range of hazardous substances to which first receivers most likely could be exposed.

4.7.1. Respiratory Protection

Respirators protect the user in two basic ways. The first is by the removal of contaminants from the air. Respirators of this type include particulate respirators, which filter out airborne particles; and "gas masks" which filter out chemicals and gases. Other respirators protect by supplying clean respirable air from another source. Respirators that fall into this category include airline respirators, which use compressed air from a remote source; and self-contained breathing apparatus (SCBA), which include their own air supply.

Respiratory protection is effective only if:

- the correct respirator is used,
- it's available when you need it,
- you know when and how to put it on and take it off, and
- you have stored it and kept it in working order in accordance with the manufacturer's instructions

The filter cartridges protect against only certain inhaled airborne substances. Some dangerous chemicals are absorbed through the skin. Properly selected and worn gas masks and escape respirators must be combined with protective clothing to completely prevent injury from these chemicals.

4.7.2. Gloves and Boots

No single glove or boot material will protect against every CBRN substance.

Most glove manufacturers offer detailed guides to glove materials and their chemical resistance. Butyl rubber gloves generally provide better protection than nitrile gloves for chemical warfare agents and most toxic industrial chemicals that are more likely to be involved in a terrorist incident, although the converse applies to some industrial chemicals. Foil-based gloves are highly resistant to a wide variety of hazardous substances and could also be considered when determining an appropriate protective ensemble. A double layer of gloves, made of two different materials, or foil-based gloves resist the broadest range of chemicals. A combination of gloves, for example, butyl gloves worn over inner nitrile gloves, is often the best option for use by workers during emergencies and mass casualties involving hazardous substances.

4.7.3. Protective Garments

The optimal garment material for first responders will protect against a wide range of chemicals in liquid, solid, or vapour form (phase). Because first responders might become contaminated with liquid or solid (dust) contaminants through physical contact with a contaminated victim, the ideal fabric will repel chemicals during the incident. Additionally, the optimal garment will restrict the passage of vapours, both through the suit fabric and through openings in the suit. Finally, optimal clothing is also sufficiently flexible, durable, and lightweight for long-term wear (up to several hours) during physically active work.

The ability of protective garment fabric to withstand physical abrasion and tearing is also important. When assisting non-ambulatory victims, first responders might subject the protective garments to physical stresses that should be considered in garment selection.

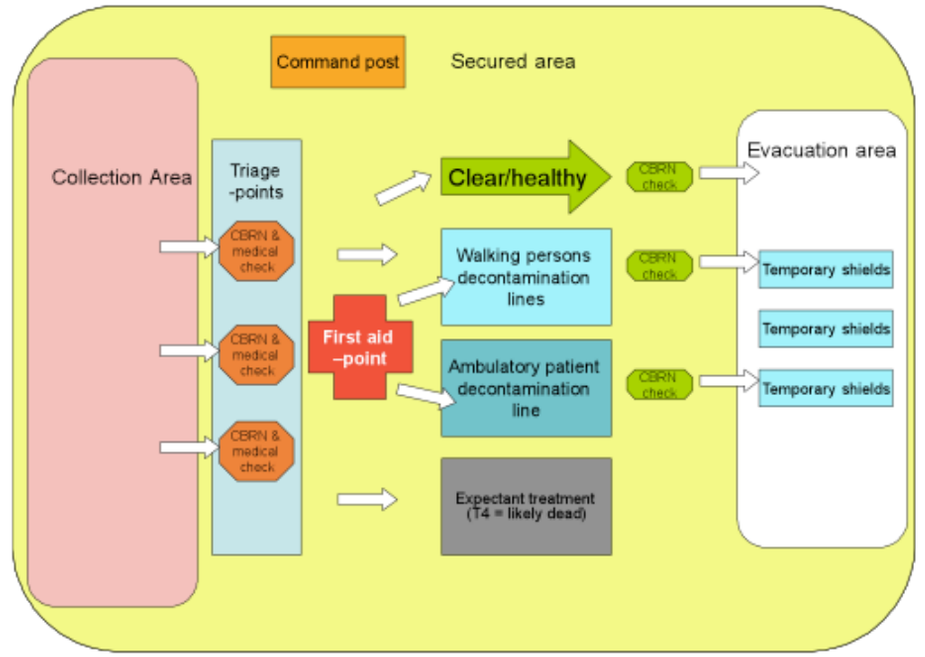
5. General - Operations in Case of a CBRN Incident

The action and reaction concept consists of four (4) main phases. All these comprise several detailed actions and tasks, but they are not covered in this document. The actions are described in order of execution following first alert or information of the incident.

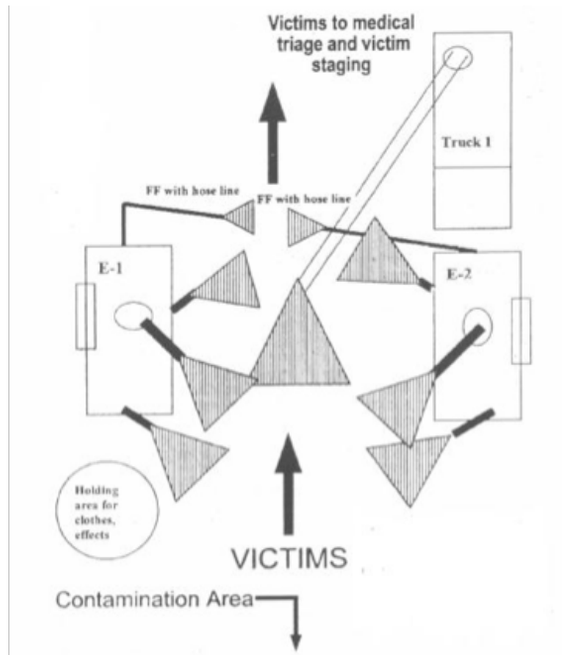
✓ *5.1. Various Operation Flow Lay-outs*

In this chapter a few possible operation flow lay-outs are introduced by figures.

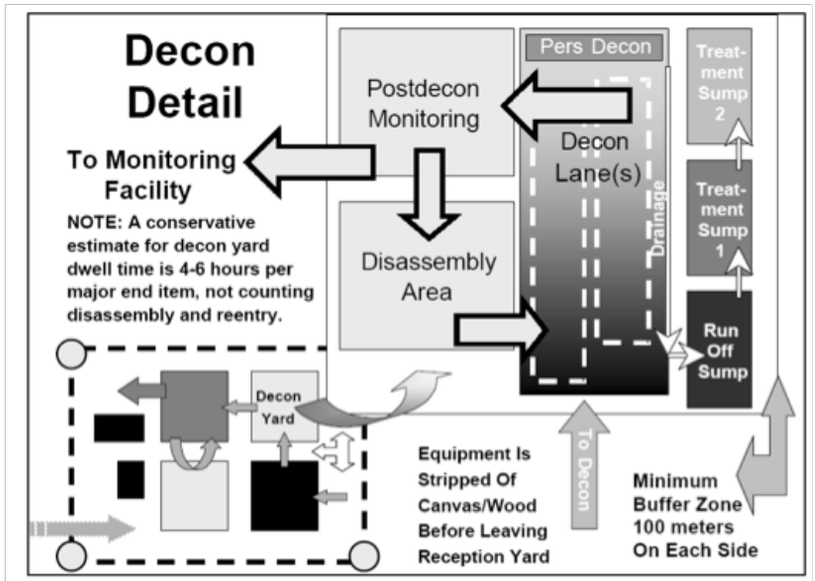
These are only examples and numerous other variations are possible.



Choice1. by Silvennoinen & Lairio, 2008



Choice 2. by (iii) U.S. Army Soldier and Biological Chemical Command (SBCCOM), January 2000.



Choice 3. by (v) US ARMY Air /Land/ Sea application center, September 2000.

✓ *5.2. Deployment and Status (What, Where, When?)*

After the incident the management must quickly assess the scene and assign personnel to coordinate and manage both the medical triage and decontamination functions.

Always assume a "worst case scenario" situation until it is ruled out. Scale back response activities as evidence and information become available.

The second priority in the management of an incident involves ascertaining the identity of the agent alleged to have been used in the incident.

- Determination of the status/nature/substance/area of the threat.
- Reconnaissance by specialized personnel equipped with personal protective equipment, CBRN-detectors and sampling systems. Samples shall be sent for analyze immediately. The exact nature of the threat is essential information concerning the following procedures.

Wider situation status definition. Some factors that will help the management determine which method of decontamination to use include the following:

- Available resources (personnel, equipment, water etc.)
- Number of potential victims
- Number of symptomatic victims
- Age of victims
- Outdoor ambient temperature

Determination of the necessary action plan, personnel (authorities, medical care, CBRN), equipment a/o resources.

Immediate define and restrict of the Hot Zone (contaminated area).

- Marking the areas: Hot Zone, Warm Zone (decontamination area) and Cold Zone (contamination free area). Warm and Cold Zones must be located to upwind.

Command. Establishment of official co-operation and chain of command (advance function) inside the organization and between authorities.

Responsibilities of each operator/organization should be clear.

✓ *5.3. Initializing of a Case Adapted Action Plan*

Adaptation of the pre-planned programmes/plans. These plans should be prepared in advance and trained on a yearly basis.

Planning of the operation area (lay-out) and set up of operation posts:

- According to marked areas (Zones)
- Triage measures posts
- First aid points (life saving)
- Decontamination systems
  - ❍ Ambulatory

- ❍ Non ambulatory
- ❍ And their logistics. If available resources are only sufficient for a single system, non-ambulatory victims triaged as immediate are of higher priority than the ambulatory victims triaged as immediate!

- Temporary shelters (unclothing/clothing/collection) and equipment
- Command posts and communication systems
- Operators personal protective suiting and equipment area
- Supporting areas (toilets etc.)
- Waste collection systems

✓ ***5.4. CBRN Countermeasures - Operations***

5.4.1. Collection of Victims

Evacuation, reassuring, information and maintaining of order.

Note: Immediate decontamination may only involve removal of clothing unless the victim is grossly contaminated with liquid agent. Once initial triage and/or decontamination prioritization is performed and adequately trained responders are available, ambulatory victims should be placed in a separate collection area in the upwind area of the Hot Zone for secondary triage.

Should a second decontamination system be placed in operation at the same site, ambulatory victims may be assigned to the second station, leaving the initial station for the non-ambulatory victims. It is recommended that all non-ambulatory victims who are exhibiting serious chemical signs and symptoms receive highest priority for decontamination.

However, some of these victims will not survive, and decontamination resources would be better spent on other victims.

5.4.2. Triage and First Aid

The consensus from emergency responders and medical practitioners is that the term "decontamination prioritization" be used to describe the process of deciding the need for and order of victim decontamination.

Triage is the medical process of prioritizing treatment urgency within a large group of victims. Both processes may be executed at the same time. The number of apparent victims from a chemical agent terrorist incident may exceed emergency responders' capabilities to effectively rescue, decontaminate, and treat victims, whether or not they have been exposed to a chemical agent. Responders, therefore, must prioritize victims for receiving decontamination, treatment, and medical evacuation, while providing the greatest benefit for the greatest number. Although many emergency response services prepare for such incidents, few are currently capable of treating victims inside the Hot Zone. Therefore, whenever large numbers of victims are involved, it is recommended that they be sorted into **ambulatory** and **non-ambulatory** triage categories.

5.4.2.1. Prioritizing Casualties for Decontamination (Triage)

Prioritization for decontamination can effectively be performed in a manner that will maximize treatment while minimizing the number of emergency responders exposed to a chemical agent.

Triage Definitions

- **Ambulatory Casualties:** Victims able to understand directions, talk, and walk unassisted. Most ambulatory victims are triaged as minimal (green tag/ribbon or Priority 3) unless severe signs/symptoms are present.

- **Non-Ambulatory Casualties**: Victims who are unconscious, unresponsive, or unable to move unassisted (red tag, red ribbon, or priority 1).

The highest priority for overall decontamination will be those casualties who are medically triaged as immediate (i.e., red tag, red ribbon, or priority 1) and are in need of immediate life-saving medical procedures that can be done quickly with the medical resources available on-site. Usually these casualties have breathing or circulatory problems but might also include those victims with severe nerve agent poisoning who need antidote or ventilation immediately. Severely intoxicated nerve agent casualties may be the highest priority for decontamination within this category; for these casualties, decontamination completed as soon as possible after the exposure may be lifesaving.

The next priority is those ambulatory casualties who were not as close to the point of release, and may not have evidence of liquid deposition on clothing or skin, but who are clinically symptomatic. Victims suffering conventional injuries, especially open wounds, should be considered next. The lowest decontamination priority goes to ambulatory casualties.

The triage operation can be performed according to NATO triage classes too:

(1) Immediate treatment (TI). RED
(2) Delayed treatment (T2). BLUE
(3) Minimal treatment (T3). GREEN
(4) Expectant treatment (T4 = likely dead). BLACK

This classification is used by the military.

5.4.2.2. Triage Practices

Due to the complex nature of some of these casualties (i.e., mixed chemical and conventional casualties), the medical triage and decontamination sectors should work closely together to maximize their collective sorting and management of casualties.

Individuals exhibiting symptoms of chemical exposure should be treated immediately (if possible, without exposing responders to the agent), followed by prompt field decontamination.

Asymptomatic individuals should be examined for physical signs of chemical agent contamination and observed for onset of symptoms. Those with signs or symptoms of agent exposure should receive priority for decontamination; the remainder should be carefully observed and decontaminated as soon as possible.

If the victims can walk, responders should have the victims remove their contaminated clothing and then lead them out of the Hot Zone to the Warm (decontamination) Zone.

These victims should be instructed to remove contact lenses, if present, and flush skin, eyes, and hair with water. If the victims are unable to walk, the rescuers should assist the victims with the removal of their contaminated clothing before transporting them on a backboard, gurney, etc. If there is no other means of transport, the victims should be carefully carried or dragged to safety; however, responders need to ensure that they do not drag victims through a contaminated area or transfer visually identifiable contamination on clothing or personal items from the Hot Zone to the Warm Zone. The contaminated items, such as clothing and personal belongings, must be left in the Hot Zone.

The triage of non-ambulatory victims in a Hot Zone may be difficult to perform and may be highly incident-specific. These victims are the only group that should receive medical treatment within the Hot Zone. They may need to receive an auto injection of atropine and Oxime (2-Pam C1) prior to their removal or decontamination.

There may also be victims that have expired by the time triage personnel arrive. Expired victims and those who are black tagged are the last concern for emergency responders, and they may choose not to address these victims at all, leaving these victims to be handled later, during site cleanup and remediation.

NOTE! When the situation is severe enough and resources are overwhelmed, individuals who show no chemical agent contamination or symptoms, and who are not otherwise suspected of being contaminated, may be allowed to proceed to the Cold Zone. The Incident Commander may make this allowance, if it is believed that such action will speed the decontamination process for genuinely contaminated and symptomatic people, and ultimately result in more lives saved.

5.4.3. Immediate Decontamination (Ambulatory/Non-ambulatory Persons)

There are three main purposes for decontamination:

- Remove the CBRN agent from the victims
- Protect response and medical personnel
- Offer psychological comfort to victims

If the victims are actually contaminated with a CBRN agent, timely physical removal of the agent is of primary importance to accomplish lifesaving decontamination procedures. Therefore, the key to successful decontamination is to use the fastest approach that will cause the least harm and do the most good for the majority of the people. In most situations, this will be a combination of disrobing and water flushing. Where feasible, if victims are obviously contaminated, self-decontamination by physical removal of the agent should be encouraged while responders are en-route to the scene.

Regardless of the ambient temperature, people who have been exposed to a known life-threatening level of chemical contamination should disrobe, undergo decontamination with copious amounts of high-volume, low-pressure water or an alternative decontamination method, and be sheltered as soon as possible.

6. CBRN Medical Care and Preparation for Evacuation

The patients (passengers) can NOT be sent (evacuated) to ordinary Health care system prior assuring they are contamination free.

NOTE! This paragraph is not included in this study, but it is included for further considerations. All topics are quite extensive and demanding processes, and require further interest and consideration in discussion and conclusion phase.

<u>The medical and logistics main topics are as follows:</u>

- Field medication systems
- Temporary accommodation
- Provisioning (food, drink and medical/medication support)
- Hygiene (showers, toilets, waste etc.)

Care must be exercised after mass casualty decontamination to prevent unnecessary exposure of the victims to the environment during cold weather. Whenever possible, some form of shelter or dry clothing should be provided.

All nearby hospitals should be informed of the type of agent involved so that medical staff can prepare themselves psychologically and prepare the necessary drugs and procedures before the victims arrive.

In addition to minimizing physiological hazards from exposure, the shelter can afford an opportunity to provide gender segregation pending availability of clean clothing. Gender-segregated shelter may help minimize psychological stress from the decontamination experience. In cold weather situations where shelter or dry clothing cannot be provided, victims decontaminated with water should be observed for signs of shivering. Shivering generates body heat and is an indication of normal bodily response to the cold environment. Should shivering STOP in such situations, medical attention should be sought immediately since cold weather injury could be imminent.

Hospitals and hotels have access to large quantities of robes and linens, eliminating the need for first responders to haul their own supply.

If not completed earlier, there should be a complete listing of all individuals decontaminated and/or deferred from decontamination for observation.

The triage personnel positioned at the entrance of the Cold (support) Zone must be certain that victims have either undergone basic decontamination or are not suspected of having been contaminated, before leaving the Warm Zone. It is recommended that triage personnel question all people leaving the site that have not showered. If possible, the first 25 meters of the Cold Zone should be treated as a vapour hazard zone where only victims and responders in transit should be allowed in the area.

Victims who have undergone proper decontamination, or have no more than one physical sign and indicate verbally no known exposure, pose less risk of causing secondary contamination. These victims should be retained at the site in a safe area for observation for up to several hours if possible. Cold Zone emergency response personnel require no specialized respiratory protective gear when treating these people, provided they are properly positioned outside of the Hot and Warm Zones.

Evacuation to hospital (guiding/isolation/hypothermia/transport equipment/special hospital processes in a CBRN-situation).

Behavioural effects:

Historical experience with Sarin attacks in Matsumoto and Tokyo serve as real-life models of the impact of human behaviour on a situation. In these emergencies, the risk for psychological injury was greater than the health risk posed by exposure to the chemical — 80% of the victims in those incidents were suffering from psychological trauma or were part of the worried well. Only 20% of the victims were chemically contaminated.

A first responder may be unable to ascertain whether chemicals or stress or cold injury incapacitates a person.

7. Subsequent Actions (not included in this study)

NOTE! This paragraph is not included in this study, but it is included for further considerations. All topics are quite extensive and demanding processes, and require further interest and consideration in discussion and conclusion phase.

<u>Check list for subsequent actions main topics are as follows:</u>

- Decontamination and maintenance of operators and equipment
- Collection/handling/transport/destroying of contaminated material
- Decontamination and inspection of operation area and vehicles
- After care; exposed persons, operators and authorities (update of plans etc.)
- Information (victims, press and public)
- Analyze: lessons to learn
- Debriefing of the operators and organizations
- Plan & equipment updates
- Training

Resources:

- i. AJP-3.8 Allied Joint Doctrine for NBC defence (NATO /pfp unclassified), July 2003.

- ii. Guidelines for Mass Fatality, Management During Terrorist Incidents Involving Chemical Agents: U.S. Army Soldier and Biological Chemical Command (SBCCOM), January 2000.

- iii. Guidelines for Mass Casualty Decontamination During Terrorist Incidents Involving Chemical Agents: U.S. Army Soldier and Biological Chemical Command (SBCCOM), January 2000.

- iiii. Middlesex-London Health Unit, CBRN-E Incident – Public Health Management Guidelines (2008)

- v. Multiservice procedures for nuclear, biological, and chemical (nbc) defense of theater fixed sites, ports, and airfields, US ARMY Air /Land/ Sea application center, September 2000.

- vi. United States Department of Labor, Occupational Safety & Health Administration, OSHA BEST PRACTICES for HOSPITAL-BASED FIRST RECEIVERS OF VICTIMS from Mass Casualty Incidents Involving the Release of Hazardous Substances. (http://www.osha.gov/dts/osta/bestpractices/html/hospital_firstreceivers.html#61).