Vulnerability of the Interconnected Society

NATO CCMS Short Term Project

Final Report

Oslo, October 2002

Summary

When NATO's Committee on the Challenges of Modern Society (CCMS) was established in 1969, a fundamental argument for the introduction of a non-military focus within the Alliance was the increasing societal vulnerabilities from sources beyond the traditional security framework. History has since proven this insight a visionary one with environmental degradation, food contamination, resource scarcity and as seen last in September of 2001, terrorism, as examples of international sources for vulnerability. These areas are being studied extensively in different national and international fora.

There is, however, an increasing attention to the additional vulnerabilities, and strengths, introduced through interdependencies and interconnected systems, be they technical or societal. The associated challenges are considerable. A more open global community, more complex technological systems, the dependency on electronic information and communications systems, intertwined systems for the production and delivery of food, the influence of climate change, global transportation systems, privatisation of services and a business community in continual and rapid change – all of these give rise to new and constantly changing manifestations of interconnected vulnerability.

Discussing this broad setting and observing relevant national and international processes, the participants in the VIS short-term project have drawn the following main conclusions:

- The aspect of interconnectivity of systems and its effect on societal vulnerabilities is in need of further study in an appropriate multilateral setting.

- Societal vulnerabilities must be seen in a global context. As these cannot be resolved by individual countries alone, interconnectivity becomes a network challenge. Further work should consequently focus on interconnectivity as a trans-national phenomenon.

- To provide a useful level of analysis and knowledge sharing, it is necessary to limit the scope of new initiatives and leave implementation into national solutions to established fora and actors.

- The key tool in dealing with future challenges is a systematic investment in training and knowledge dissemination

The VIS project has identified the below topics as a set of areas where common interests for future initiatives between countries are already present. It is consequently recommended that the CCMS adopt the list and provide it as a guidance to member and partner countries in an effort to initiate new projects or Pilot Studies under the auspices of the committee. This should not be to the exclusion of related topics where common interest exist, but more as "rallying points" for the committee and its national representatives.

- System resilience based on interconnectivity
- Training and education
- Media interaction
- Risk Communication
- Linking of vulnerability and security policy
- Clarification of national structures
- Develop conceptual clarity in a multidisciplinary setting

It is further recommended that a VIS Pilot Study be initiated drawing on interrelating findings of other relevant CCMS and NATO activities.

Contents

Introduction to the VIS Short Term Project

Societal vulnerability has been with us for centuries and the topic has been discussed by dedicated organisations in national and international settings for decades. It took the advent of the year 2000 challenge to computer systems, however, to draw public and global attention to the effects on societal vulnerability of the integration , automation and globalisation of all kinds of technical systems.

It is important to address the interconnectedness in itself in addition to the different sources of vulnerability and how to deal with them. This angle was raised at the 2000 Round Table discussion of the NATO Committee on the Challenges of Modern Society (CCMS) in Berlin in the context of new threats to security. As a result, a project was launched in 2001 to review the common challenges with regard to vulnerability and to identify areas where a cooperation within the framework of NATO could be beneficial.

The activities under the project has mostly been carried out as preparations for, and during, the three official meetings held in Oslo, Brussels and Zurich. With 15-20 participants at each meeting, representing a variety of organisational and professional backgrounds, the recommendations of the final report are well founded in both national priorities and processes in key multilateral cooperative efforts. The heterogeneity of the group has provided for both knowledge transfer and further confirmation of national views.

Attention to the topic has increased greatly during the project period due to the terrorist attacks in the USA on September 11. 2001. Although easing the challenge of communicating the concepts of vulnerability and risk to the public and the political communities, this development has highlighted the importance of avoiding duplication of work between different international fora. The final report from the VIS project consequently aims to provide a brief overview of relevant topics for further studies in a CCMS setting

1. Societal Vulnerability & Interconnectedness

Society should be shielded from threats to basic values such as life, national health and welfare, moral and cultural values, quality of the environment, the democratic system and its legal institutions, national control, national sovereignty, the nation's territorial integrity, material and economic safety and cultural values. "Societal vulnerability" describes the extent to which a society is susceptible to disruption of these functions and qualities.

Vulnerability can be understood as the collective result of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations. The vulnerability analysis covers a long-term perspective and gives focus to a sequence of events from the moment an emergency situation occurs until a new stabile situation has been reached

Based on a definition of "Vulnerability" as
"situations, processes or phenomena from internal life, which reduce the capacity to react against the existing or potential risks, or which facilitates their development,"

they can be limited to a national level or broadened to encompass a global setting. The above examples of threats indicate the complex framework of risk factors involved at any level.

To deal with vulnerabilities and non-military threats to society at a national level, most countries have one or, usually, many organisation responsible for different aspects of civil emergency

planning and operation. Consequently, the knowledge and methodologies employed are extensive and continuously improved by national and international experts and cooperation.

There is, however, an increasing attention to the additional vulnerabilities, and strengths, introduced through interdependencies and interconnected systems, be they technical or societal. The associated challenges are considerable. A more open global community, more complex technological systems, the dependency on electronic information and communications systems, intertwined systems for the production and delivery of food, the influence of climate change, transportation systems operating at greater speed and with increased traffic density, and a business community in continual and rapid change – all of these give rise to new and constantly changing manifestations of vulnerability.

Furthermore, the more open world economy and changes in the political landscape have led to substantial changes in potential threats emanating from criminal actions. On a more positive note, public awareness and knowledge of the dangers around us is increasing. This may enable a discussion of risks and preparedness, which, to a much greater degree than before, is founded not only on knowledgeable public authorities, but also on an informed public.

- Technological changes.
- Increasing complexity of modern society.
- Increasing demands for efficiency and cost effectiveness.
- Fewer personnel in numerous sectors.
- Increasing privatisation of public services.

To preserve security and protect society from a broad spectrum of challenges, a conscious effort from public authorities in many different fields is necessary. Co-operation and co-ordination – including other nations – becomes necessary if we are to prevent and/or handle crisis situations, as has been shown in the aftermath of September 11. The latter illustrates the increased interconnectedness of the military and the civilian security concerns, a key reason for introducing cooperation on vulnerability in a NATO context.

In the NATO CCMS setting, the project participants concludes that the aspects of national vulnerabilities should be left to other organisations and that vulnerabilities involving cross-border challenges should be the main focus of future initiatives. This will help highlight a necessary attention to the process of interaction between several "actors" in a network, involving processes and challenges beyond the control of any single actor.

Unlike the traditional models of interaction between countries, the network approach builds on the fact that such processes are not a set of discrete "action – reaction" situations, but consists of a number of parallel processes involving and influencing multiple actors. Consequently, the analysis of vulnerabilities must be raised to such a level to find applicability beyond a static situation where all actors are in control, a setting which only exists in theory.

One example of this is the inadequacy of traditional "perimeter security" where threats were easily identifiable and internal sources of disruptive activities were either under control or negligible. The establishment of the "Schengen zone" in Europe illustrates the systematic vulnerability flowing from integration.

The work of the project group has covered a number of challenge areas, mainly from the civil emergency agenda (see chapter 3). Taking the above network view, the group fully endorses a dual approach; one to reduce vulnerabilities enhanced by interconnectedness and one to increase resilience through the same. The latter is based on the fact that systems and services may draw strength and necessary redundancy from others in a well understood network setting.

As with the fore-runner of the Internet, DARPA-net, the interconnected systems of society provides resources for dealing with the loss of function in individual nodes of a network. Distributed information systems can provide crucial redundancy in case of accidental or intentional disruption. However, such strengths have to be developed and analyzed to be available when needed. Too often, even multinational and multidimensional systems rely on individual sources to function in a case of emergency.

The emergence of potential opponents other than nation states is yet another important development. However, it cannot be ignored that the changes in contingency planning efforts are to a large degree forced by unforeseen events and not as a result of a complete analysis of the full picture and the setting of underlying common goals. The result is an uncoordinated organisation of coincidental incoherent parts that have to a large degree been determined by the occurrence of various accidents and events.

It is important to separate several key terms: Interconnectedness, which make for dependencies, which can make for vulnerabilities that entails risks and than can open up access points for threats by states and non-states. There is no direct link between interconnectedness and threats, but a chain in between which may or may not lead to exposure to threats.

2. Key topics for future work

The participants in the VIS project were quite clear with regard to the need for avoiding duplication of work and parallel networking processes in the present situation. After September 11, a large number of international initiatives from workshops to cooperative studies, have been initiated, and parallel needs for knowledge and analysis is already taxing on national experts and their organisations.

As indicated above, however, there is the added dimension of interconnectivity which raises topics and challenges beyond those already dealt with or studied in the context of civil emergency planning (CEP). Although the proposed areas for future work within the CCMS framework necessarily has to be selected from the same list of topics, the below suggestions are aimed at introducing approaches specifically suited to the NATO setting and the opportunities presented through the EAPC.

2.1 Organisational challenges & solutions: Questions of institutional design

Throughout NATO and Partner countries, initiatives are presently being taken to review, or actually initiate, new organisational structures which are better positioned and organized to deal with the kind of threats and tasks associated with disruption of an interconnected society. As an important input to such processes and the associated assessments, the exchange of views and experiences between countries is important both for reasons of efficiency and future cooperation.

The additional aspect of a blurring of the traditional split between military and civilian threats and measures, makes NATO and the CCMS an opportune arena for addressing an integrated approach to societal security. To safeguard society is different from and requires more than territorial defence. We can see a slide in strategic planning from territorial security to functional security. NATO needs both aspects in order to be relevant to the security concerns of the future.

It is specifically observed by the project participants that countries are, in many cases, still trying to meet 21st century challenges through 19th century bureaucratic organisational structures. These are the structures dominating our governance traditions, while adversaries increasingly utilize the flexibility and network structures supported by new technology and modern information infrastructure. This ranges from terrorists, organized crime syndicates to young hackers. An

additional aspect of this is the fact that organisations cannot work through constant reorganisations. It then becomes part of the problem, not the solution.

Illustration 1: Organisational change

To improve security and preparedness in Norwegian society, the following recommendations have been made:

- *Merging of the work for public safety and security under the jurisdiction of a single governmental ministry with national safety and preparedness as its main task.*
- *The establishment of a co-ordinating body for the intelligence and security services.*

A co-ordinated strategy and the possible merging of relevant safety and security inspectorates.

- *Evaluation of the nation's operational rescue and preparedness resources.*
- *Joint investigation commission for major accidents and crises.*
- *Police forces and anti-terror /sabotage units*
- *Co-ordination of rescue services, preparedness for major accidents, fire department and civil defence.*
- *Co-ordination of preparedness efforts for complex crisis situations.*
- *Co-ordination of intelligence and security agencies and the assessment of overall national vulnerability and potential threats to national security.*
- *The development of methods and rules within the field of security and national contingency planning.*

Many Partner countries are now in a state of flux from the old, authoritarian structures to new democratically based institutions. It is very timely therefore to think through the consequences of various institutional design structures and try to find those most suitable for the country in question. Alternative solutions must be discussed with a focus on low cost, low-tech and flexibility of approach. To the extent that there exists commonalities of need between many EAPC countries, a common approach could be described.

Other organisational aspects which spring from interconnectivity is the possibility for inclusion of NGOs, business etc. as part of the extended organisational solution. This involves an assessment of different types of capabilities. An integral part is influence building, long term cooperation and mutual benefits

While nations traditionally base their solutions on sovereignty within their own borders, interconnectivity and vulnerability of cross-border systems requires a different set of measures than before. Such loss of control is currently enhanced through a drive to out-source government functions and focus on "core business". In an international setting, this may limit the ability of governments to allocate resources in a crisis situation

2.2 Crisis Management

The area of crisis management is a well established field with experts and guidelines from preparatory policy development to the phase of re-establishment of systems and functions. This provides ample knowledge for approaching the added challenge of interconnectivity.

Of special relevance to further CCMS initiatives, the VIS group has pointed to

- Development of generic approaches, whatever the crisis

- Focus on larger societal effects and ripple effects from a crisis

- Need for long term training at all levels, not only operational but also political, with emphasis on cross-sectorial and cross-border effects. Implies a need for changes in present curricula in both civilian and military training.

- Any approach must ultimately build on the individual as the primary line of engagement, the rest is in to support.

Strengthening the attention to threat assessment and crisis prevention, a number of "new" fields of knowledge must be drawn closer into any development process. Together with the increasing rate of change in technologies and modern societies, global interconnectivity drives the field of crisis management towards an emphasis on flexibility and organisational and human ability to change.

Among the challenges identified as part of improving Civil Emergency Planning and Crisis Management in general are:

- Innovative threat assessments
- Prevention: regulation and design
- Planning and preparedness
- Large-scale organizational operations
- Transcending the civil-military divide
- Management of uncertainty and complexity
- Communicating with media and the public
- Learning: knowledge production and transfer
- Consciousness raising and training programmes

Within each of these topical areas is contained the added dimension of technical, systematic, informational and political interconnectivity. As this aspect hightens the need for cross-border cooperation and interfacing between national systems and operational plans, the role of international fora must also be extended to common foresight activities.

While NATO has a long standing activity in the field of civil emergency planning, the CCMS aims to be an arena for less immediate and operationally focused studies, providing a long-term approach to the broad range of new challenges included in societal vulnerability. This role and the topic at hand open up possibilities for broader, cross-sectorial and interdisciplinary projects involving expertise from NATO and Partner countries. A Strategic View for this field is needed. This is no less important than previous geostrategic concerns during the Cold War focus on territorial defence.

2.3 Critical Infrastructure (CI)

Critical Infrastructures are systems whose incapacity or destruction would have a debilitating impact on the performance of vital services/functions of society including defence and economic security of a nation**.** Critical infrastructures[1] are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to:

- telecommunications,
- information systems
- electrical power systems,
- gas and oil,

[1] Presidential Decision Directive 63, The White House, May 22, 1998

- banking and finance,
- transportation,
- shelter
- water and food supply systems,
- environmental protection system
- government services and
- emergency services.

These are almost without exception interconnected systems dependent upon other types of systems in an international setting. This challenges the traditional focus on physical infrastructure and calls for a split between this and services as vulnerabilities and capabilities become trans-national.

Again the vulnerabilities resulting from privatisation and other types of organisational change becomes a key topic when discussing the robustness and resilience of the international society.

The critical infrastructures of nations have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both national and global security.

In "The International Critical Infrastructure Protection Handbook", the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology in Zurich, the following definitions and comments are presented:

- **Critical infrastructures** consist of all physical and information technology facilities, networks and assets essential to a minimum operations of the government, economy, and the society.
- **Critical Infrastructure Protection** (CIP) is an integral part of national security. It includes all methods and means to protect a nation's CI defined as above.
- **National Information Infrastructure** (NII): The computer networks play a key role in almost all sectors of CI. Hence, the national information infrastructure is a key subset of the national CI.
- **Interdependency**; The issue of interdependencies among critical infrastructures is a fundamental dimension of critical infrastructure protection. Infrastructure interdependency has been the least-studied aspect of infrastructure-specific concerns. It must be kept in mind that the bulk of critical infra-structures are interlinked today.

Examples, among many, of ways to counter CI vulnerabilities is diversification of economic productive systems and avoidance of technological monocultures. Attention is also increasingly given to the strengths in networking CI. Given improved protective measures against malignant use, the redundancy and the possible speed with which interconnected systems may be re-configured or re-built appears to be an important field for further study and cooperation.

There is also the topic of vulnerability beyond the traditional infrastructure definition as in human and organisational infrastructure as well as the wider societal dependencies as other infrastructures become dependent on information infrastructures. Contained in this complex concept is also the handling of supra-nationality.

NATO has always been paying attention to the wider scope of infrastructure, but with a priority to the military part. As the interdependency between military and civilian structures increases, the possibility of utilizing the NATO setting and capacity for analysis, planning and standardisation becomes both attractive and necessary. The developing tools for cooperation with Partner countries is also, in many ways, a unique advantage to dealing with CI through CCMS studies.

2.4 Communication, Information and Cyber Security

Communication to deliver information provides a seamless integration of systems and services and thus represents the quintessential interconnectedness to both the Government and the general public. Vulnerability due to the ever increasing dependence on information carried through communication systems across borders also illustrates the inadequacy of most traditional measures like government regulation.

Cyber (space) is a relatively new term. Rumour says it was coined by a science fiction writer. Cyber was the family name of some early computers from Control Data Corporation, one of those dinosaurs that produced computers in good old days. Those computers were sitting as nodes in the early Internet. So the term is mostly used for the Internet environment or information systems connected through the Internet. Cyber security threats are thus related closely to the Internet, hackers etc. They are not electronic, or radio-frequency based. Information warfare and information operations are the super sets. They include cyber security.

Although formally covered under the heading of critical infrastructure, communication, information systems and cyber security has become a topic on its own. With the ever increasing integration of telecommunication, computers and information systems, the topic of communications has to take on both the technical aspects often associated with IT, as well as the usage and miss usage of information systems. An important part of the latter is the challenge of managing both large national systems and global ones, as well as communicating the complexity of such systems to decision-making non-experts. De-regulation and subsequent effects of financial and competitive pressures are examples of organisational threats to resilient technical systems.

Cyber security is concerned with threats and vulnerabilities in cyberspace. Cyberspace[2] is here defined as the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. Internet is a vital part of cyberspace, so is most telecommunication systems. Cyber threats cover a large spectrum. Examples are Distributed Denial of Service Attacks, injection of malicious code and hacker attacks carried out by terrorists.

As with the perimeter defence discussed previously, an important vulnerability of present day information systems is due to internal sources of disruption. The role of such factors also increases with the global tendency to monopolize electronic information services which merge systems and services.

[2] Slightly divergent definitions are found through out literature

Looking to the future, the VIS group has identified systems built on broadband services (Ex: Health) as the next challenge both due to the sheer volume of data being transferred and the pervasiveness of continuous connection to the Internet. Both will lead to new levels of system development which may include an increased centralization of data storage with associated vulnerabilities. This might be dealt with under the topic of Critical Information Infrastructure (CII).

Such security threats are defined as threats of electronic, radio-frequency, or computer-based attacks on the information or communication components that control critical infrastructures. Accordingly the following subjects are covered with this definition:

- Information Assurance
- Information Warfare
- Information Terrorism
- Information Security
- Critical Infrastructure Protection

As confirmed by project participants, these are all topics featured high on national agendas both for reasons of national security and for safeguarding business activities. Threats to individuals and the topic of civil liberties are also relevant aspects of any analysis in this field. The links between technical/commercial structures and public/political ones constitute one further dimension in viewing the vulnerabilities stemming from the information dependence of modern society.

Specific studies of vulnerabilities of communication & information infrastructure are not envisaged as a priority area in itself under the auspices of CCMS. However, the topic is so pervasive , that it must be integrated and linked to most efforts undertaken by nations in this setting.

2.5 Media

The VIS group has returned to the discussion of media as newsmakers and distributors on many occasions throughout the project. Being an integral part of the communication revolution, media drive concerns over security, safety and vulnerability and function as a transmission belt across sectors and countries.

Forming the key target group for many disruptive activities, media serve as multipliers for terrorist attacks, hackers and hostage takers. Driven by the attention to sales figures and viewers and the need to appear independent of established power structures, most “actors” in this field face a challenging balancing act between crisis promotion and crisis prevention.

In the CCMS setting, avenues of interaction and need for communicating knowledge in the field of societal vulnerabilities, may be the most important topics to include in future initiatives. Specifically, the establishment of a dialogue on the role of media in a crisis with a view to accumulating vulnerabilities in an interconnected setting seems important along with the topic of risk communication.

It’s important to work more systematically with the latter field as one of several steps to strengthen risk awareness and risk management in the modern society. The strengthening of the safety of the society is dependent on the general risk awareness and risk knowledge among decision makers, planners and the general public. To ensure that these target groups have a good knowledge of risk, it’s important that risk-researchers and civil emergency planning professionals communicate risk findings in an easy and understandable language.

To strengthen and develop risk communications as a field, an awareness of research and development of theories and models to better identify, explain and manage risk, is necessary.

Definition: Risk communication can be defined as: "an interactive process of exchanges of information and opinion between individuals, groups and institutions, involving discussions of types and levels of risk and of measures for dealing with risks".

Risk communication means using language to convey an "image" of a hazardous situation. The challenge for the sender lies in communicating a risk image which the receiver also "sees", and thus perceives the same risk. One of the problems of risk communication is that different individuals may perceive the same risk image completely differently. The increased likelihood of injury or death in parachute jumping may deter one person without causing another the least concern. The latter can be seen either as taking a calculated risk, as confident of having the risk under control, or as being "blind" to the increased risk.

Risk perception is influenced by many factors; a situation one can influence oneself is often seen as less dangerous than one that is beyond one's control. Risk perception is also affected by such factors as whether the risk/disaster is natural or man-made, is familiar/ well-known or unknown/exotic, and affects everyone ("fair") or only a few ("unfair"). Typical objectives of risk communication are to change risky behaviour and/or convey information about a particular danger.

The 7 basic rules of risk communication
1. Accept and involve the public as legitimate actors (receivers of information)
2. Plan and evaluate all information measures thoroughly
3. Listen to the public's specific concerns (before, during and after the crisis)
4. Be open and honest
5. Coordinate and cooperate with reliable and credible partners
6. Satisfy the information needs of the media
7. Communicate your message clearly and with sympathy

The topic of risk communication and the interaction with media is an ideal setting for a multi-sectorial initiative involving a number of civilian “actors” and CEP experts as well as the defence community. Viewing the needs in a EAPC setting, a CCMS initiative is deemed both appropriate and timely.

2.6 Capacity Building

In cooperation dealing with societal vulnerabilities and all kinds of threats which are made more serious by the increased interconnectedness of our societies, it is important to take into account the inequalities in size and available resources between countries. Such differences often reflect both on the actual risks involved and on the possibilities for re-directing resources and changing priorities to suit international expectations.

The challenge then becomes one of capacity building in smaller countries and countries with limited resources. The balance between threats and resources requires a selectivity in the tasks to be addressed and special benefits to be had from cooperative efforts involving transfer of knowledge and experience from other countries.

Since NATO and the CCMS traditionally has given priority to capacity building through investing in human capital in Partner countries, this framework is already in place and ready to be used for

the topic at hand. New studies and initiatives would be attractive vehicles for developing common views on both future challenges and solutions. As the question of resources is a crucial one, studies and tools applicable to different levels of threats and capacities would be a high priority.

One way to build capacity is through training: build human & organisational infrastructures to deal with the technical infrastructures. Training can include seminars, exercises at national level and at best through multilateral fora to diffuse best practices and enhance local awareness of the problems to be met. NATO CCMS may also provide a setting for exploring non-traditional forms of training.

Finally, the VIS group underlines the need to include the topic of training in this field in other NATO studies. This should be an exercise in integration which may serve as a model for other parts of the work on vulnerability.

2.7 Future Knowledge needs

Among a large number of possible topics, the VIS group views an investment in awareness-raising and structures for knowledge dissemination as crucial areas for future development.

Established strategic- and security studies programs at leading schools must leave the primary focus on classic geo-strategic concerns and literatures to add the link between information technology, societal vulnerabilities etc. to their curricula. One can begin by reforming the military and civilian study programs of Defence Colleges of member and Partner countries. NATO Fellowships should be focused on this increasingly vital research and training agenda and not be locked into traditional thinking.

Mirroring the educational development and needs in other fields, the topic of vulnerabilities and interconnectedness relies heavily on cross-sectorial knowledge development.

Security should become an integrated part of information and communication technology education at all levels from high school to university. There is also a need for further competence within information and communication technology security and safety and to establish this as its own field of study at certain universities and colleges.

3. Conclusions

The participants in the VIS project have drawn the following main conclusions based on their discussions and the information available from other national and international processes:

- The aspect of interconnectivity of systems and its effect on societal vulnerabilities is in need of further study in an appropriate multilateral setting.

- Societal vulnerabilities must be seen in a global context. As these cannot be resolved by individual countries alone, interconnectivity becomes a network challenge. Further work should consequently focus on interconnectivity as a trans-national phenomenon.

- To provide a useful level of analysis and knowledge sharing, it is necessary to limit the scope of new initiatives and leave implementation into national solutions to established fora and actors.

- The key tool in dealing with future challenges is a systematic investment in training and knowledge dissemination

There is agreement among the participating countries that there are benefits to be had from a focused cooperation on vulnerability and interconnectedness within the framework of NATO CCMS. It is further important that initiatives be firmly anchored in national priorities and in the overall framework for "Preventing and Mitigating Societal Disruption" provided by the CCMS. There are a number of other areas of consensus identified by the group. These are sought reflected in the below recommendations.

4. Recommendations

The VIS project has identified the below topics as a set of areas where common interests for future initiatives between countries are already present. It is consequently recommended that the CCMS adopt the list and provide it as a guidance to member and partner countries in an effort to initiate new projects or Pilot Studies under the auspices of the committee. This should not be to the exclusion of related topics where common interest exist, but more as "rallying points" for the committee and its national representatives.

It is further recommended that the findings of the VIS project be integrated into the CCMS' work on "Preventing and mitigating societal disruption" and that the topic be included in any workshop or Round Table discussion organized by the CCMS.

Topics for further CCMS initiatives:

- System resilience based on interconnectivity
- Training and education
- Media interaction
- Risk Communication
- Linking of vulnerability and security policy
- Clarification of national structures
- Develop conceptual clarity in a multidisciplinary setting'

Format for future activities:

- Integrating VIS priorities into other activities and studies
- A VIS Pilot Study based on interrelating findings of other relevant CCMS and NATO activities
- A virtual Forum for discussing linking of national activities
    - initial round table / workshop organised by the CCMS to identify specific goals for future cooperation with a broad mix of participants
    - inclusion in the EAPC annual meeting
- CCMS initiated process with other NATO activities
- Inclusion of VIS in the Partnership with Russia. VIS should be mentioned specifically as part of the practical follow-up of the new cooperation with Russia.

Appendix 1: Participants

The following experts have been present at one or more of the project meetings:

Denmark	Drewsen	Freddie	Dish Defence Research Establishment
Denmark	Hammer	Jasper	Min. of Defence
Georgia	Dartsimelia	Giorgi	Min. of Environment
Hungary	Fömötör	Ferenc	Min. of Environment
Lithuania	Jonusauskas	Kasparas	Min. of Environment
Hungary	Tamás	Pál	Academy of Sciences
Moldova	Stratan	Alexandru	National Agency for Investment Policy
Moldova	Moruz	Ina	State Ecol. Insp.of Moldova
Norway	Steen	Roger	Dir. for Civil Defence & Emergency Planning
Norway	Fiskaa	Herborg	Dir. for Civil Defence & Emergency Planning
Norway	Henriksen	Stein	Dir. for Civil Defence & Emergency Planning
Norway	Johnsen	Tor-Petter	VIS Project
Norway	Stub	Sverre	Min. of Foreign Affairs
Poland	Podgorski	Marek	State Fire Service
Romania	Corneliu	Negulescu	Min. of Environment
Sweden	Lundberg	Jan	Agency for Civil Emergency Planning
Sweden	Sundelius	Bengt	National Defence College
Switzerland	Lagger	Anton	Min. Economic Affairs
Switzerland	Maridor	François D.	Min. of Defence
Switzerland	Metzger	Jan	ETH, Zurich
Turkey	Topuz	Erkan	
UK	Marshall	Greg	Min. of Defence
Ukraine	Marushevska	Olga	Min. of Environment
USA	Gray	Edwin Kent	US CDC
USA	Kosakowski	Michael	US EPA

Appendix 2: National Examples & References

1. Denmark

1.1 Main political focus at national level

1.1.1 Environment and pollution control

The Nature and Environment Policy is one of the government's most important tools for gaining overview and cohesion in the nature and environment initiative in Denmark. The many objectives and initiatives are all part of the government's strategy for creating a cleaner, better and healthier society.
The government's vision is based on the individual. Environmental conditions must help create a healthy environment for present and coming generations.
The government is therefore among other things working:

- To ensure biological diversity so that both plants and animals will continue to exist in viable populations in their natural habitats in the future
- To protect and regulate the use of renewable natural resources (water, forests, agricultural land) so that it does not destroy the balance of nature or deteriorate the quality of these resources both in the short and the long term, and
- To manage the natural resources that cannot be renewed with care, while developing alternatives and reducing dependency on these resources.

In the area of pollution control at sea, there is a co-operation between The Danish Environmental Protection Agency and the Naval Command. The Naval Command has the responsibility of monitoring the sea by air and ships and to take out samples of pollution from ships, which is under suspicion of pollute. It is the National Environmental Research Institute who makes the chemical analysis.

1.1.2 Digital administration

A co-operation between the local authority and the county is being carried through as a base for the public conversion to digital administration. The purpose of the project is to improve the level of service and efficiency in the public service through a close co-operation between the authorities and private corporations. It is expected that the Danish people will be able to receive a digital signature from their local authority at the end of 2002.

1.1.3 Organizing the it security area

Due to the increased focus on it security there is a need for considering the future policy and organization of the it security. Ministry of Science, Technology and Innovation have in 2002 earmarked 3 million DKR. for initiating initiatives in that area - among them statistics of data-security, analyses of international it security models, materials for education and various guidance about it security.

1.1.4 Readiness

Denmark has a well-prepared system in the day-to-day emergencies and at larger accidents and catastrophes. In this way contingency plans have been made and tested for the Great Belt Bridge and the tunnel belonging to the bridge. The Great Belt Bridge is an important part of the Danish infrastructure.

Plans have been made to get new mobile communication systems, which will increase the possibilities for at co-ordinated and integrated effort.
The threat assessment and the present state of readiness is built upon however, has changed since the terror attacks in USA in September 2001. Because of that there might be a need for changing the readiness in the shot term and consider in the long term to redefine the readiness in the light of the present threats.
The terror attacks in the USA was characterized by being without warning, using civil resources as weapons, being aimed at the civilian population in a built-up area and finally so far at an unseen dimension.
In connection with other forms of terror attacks with a risk of considerable loses in consequence of for instance attacks with chemical weapons, biological weapons and attacks on nuclear plants there will be a need for a capacity, which exceed the day-to-day readiness.

1.2 Main organisations working on vulnerability assessment at a national level and their area of responsibility

1.2.1 National Security Service

The National Security Service is organizational placed under the Commissioner of Police. It is the National Security Service main task to follow, prevent and counteract actions, which are considered to be a threat to the independence, security and social order in the Kingdom of Denmark

The National Security Service tasks are counterespionage, counter terrorism, counter extremist activities, and hinder the spread of weapons of mass destruction and serious attacks on the Danish it-systems, which are of security concern for Denmark. Finally the National Security Service issues safety clearance for national electronic information systems and networks, which are used in connection with classified information. The aim of the National Security Services investigation is prevention of crime.

The National Security Service has a co-operation between Danish and foreign authorities. In some areas there is a close co-operation with Danish trade and industry. Since still more and more information are electronic stored and communicated, The National Security Service has a special it security section. The section helps with protecting classified information and gives guidance to the authorities about data protection. Within the military forces the Defence Intelligence Service carries out the security authority.

1.2.2 National Investigation support-centre

The main object of the National Investigation support-centre is to monitor organized or complicated crime.
It is the purpose to provide and maintain a high level of information and knowledge in order to provide the best possible general view of international crime for the police in the local areas. Furthermore the National Investigation support-centre is able to support the local police in investigation and give analysis-assistance. The National Investigation support-centre is also the link to other foreign authorities and partners.

1.2.3 Special about it crime

The National Investigationsupportcenter takes part in national and international it crime workgroup within Interpol, Europol and International Working Group on Cyber Crime. The Investigationsupportcenter is responsible for the link to a special G-8 network. The network is

to be activated in case of international electronic attack on member countries technological infrastructure.

1.2.4 Danish Emergency Management Agency

The Emergency Management Agency is a governmental agency under the Ministry of the Interior. According to the Danish Preparedness Act the principal task of the Emergency Management Agency is to manage the National Rescue Preparedness Corps, to supervise the national and municipal rescue preparedness and to advice the authorities on matters of preparedness. The national rescue preparedness has a staff of some 700 persons. About 140 of these are employed in the central Emergency Management Agency. The rest are employed at the Agency's seven rescue centres and three schools.

1.2.5 CERT/UNI-C

UNI-C is the Danish Computer Emergency Response Team and represent the Danish part of the international security organization CERT. CERT distribute information and tools for preventing it crime. CERT solves tasks within security for authorities, business and individuals.

1.3 Major recent national initiatives

1.3.1 Optimise the possibilities for an effective investigation

The government made a Bill in December to make some changes in the law of administration of justice. The Bill contains an obligation for the Internet Service Providers and others to record telecommunication for a possible hand over to the police in case of investigation on complicated and serious crime.

1.3.2 Readiness

The Government also works on enhance the readiness within among others the following areas:

- Establishing one more national readiness-level (level 4) in two places in Denmark with special equipment and communication assets.
- Strengthen the readiness in securing and buttress damaged buildings in connections with natural disasters.
- Enhance the capacity to search for trapped persons.
- Strengthen the exercise activities.
- Enhance the effort to put out heavy fires in inflammable liquid.
- Better communication between authorities within the disaster area.
- Better protection against chemical by means of protection dress.
- Strengthen the biological readiness in order to cope with a biological crisis.
- Increased information on the early warning systems.
- Increased focus on risk- and vulnerability analysis in relevant areas of society.
- Strengthen the co-ordination in readiness planning between authorities.

At the same time the Government will priorities the gathering and use of knowledge from larger accidents and disasters in the fight against terror attacks.

1.4 Three potential areas for cooperation in the NATO context

1.4.1 Cyber Security & Protection

Cyber Security is an area of increasing importance. Taken from the Internet world, the term has now been expanded to include the critical infrastructure as well. This broadening is due to the pervasive use of information technology in critical infrastructure systems and the interconnectivity between the critical infrastructure and the Internet.
Subtopics for cooperation could be:

- In forensics
- Intrusion Detection Systems
- Distributed Denial of Service Attacks
- Malicious software

1.4.2 Counter Terrorism

This area needs no introduction or explanation.
Subtopics for cooperation could be:

- Information gathering and sharing
- Information fusion
- Military and non-military coordination and cooperation
- Modelling and simulation of threat scenarios

2. Romanian Strategy for National Security

Adopted by the Parliament on December 18. 2001. Published in "Monitor Oficial al Romuanei" nr. 822, on December 20. 2001.

Law nr. 363 from June 7. 2002 – for the approval of the Government Ordinance nr. 88/2001 about the nature, organisation and operation of public community services for emergency situations. Published in "Monitor Oficial al Romuanei", part I, nr. 447, 26.06.2002.

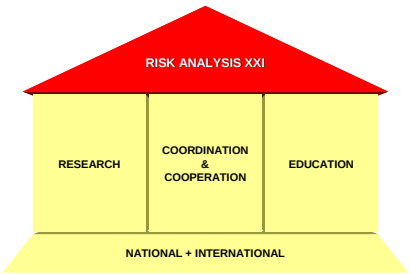
3. The Swedish Emergency Management Agency

The new Swedish organisation was established in June 2002.

Web-site: http://www.krisberedskapsmyndigheten.se/

4. Switzerland

The vulnerability of the interconnected society is not just a technological safety issue but also very much a security policy issue. An integrated, multidisciplinary, real-world approach to risk analysis and decision-making is needed. Traditional quantitative methods have to be evaluated with regard to their capability to address modern dynamics. Need for a dialogue between social scientists and natural science risk experts, to constitute a new



problem-oriented community of security policy risk analysis. Understanding of risks with regard to complexity and interdependency is needed.

The new project "Risk Analysis XXI", is focused on the concept of "risk culture" / "risk awareness". Aim is to have a free hand – as far as possible – in crisis situation and to reach a better allocation of the resources, at the right place and at the right moment.

Risk Analysis is a mean, which shall help making steps from the traditional one-dimensional perspective of security policy (military threats, power politics) towards a Comprehensive risk analysis (interdependency analysis of threats and critical infrastructures).

Within the Federal department for Defence, Protection of the Population and Sports, the Directorate for Security Policy is responsible for this concern, in cooperation within the several departments and offices within the federal administration as well as with high schools and private sector. The project shall be useful both to conceive the future security policy of Switzerland and to implement it, within the formulation of the relevant strategies.

Further, an extended risk analysis is foreseeing to get a better integration of the vulnerability towards risks. This expert's work shall provide the authorities with information so that they have an overview of the possible development, before making an important decision.

Information Assurance – The Swiss Modell

Business, sciences and federal administration build up together a system for the security of information and communication infrastructure. The objective is to discern dangers in time, work out preventive measures in advance and provide help in the event of claims.

In June 2000 Swiss government allocate tasks to four bodies:

Foundation InfoSurance: Prevention; Increase the awareness for risks
Registration and Analysis Office: Early warning; Cope the cause of crisis
Task force Information Assurance: Decision Support for government in times of crisis
Domain ICT-Infrastructure: Means and measures against crisis; Reconstruction

more: www.bwl.admin.ch, www.isb.admin.ch and www.infosurance.ch

5. Poland

5.1 General remarks

A new character of threats that have lately appeared (e.g. growth of quantity and intensity of natural calamities – floods, droughts, hurricanes, heavy rains, epidemical threats – BSE, foot and mouth disease, bio – terrorism) has caused necessity for reconstruction of civil protection system in Poland. Also, political, economical and administrative changes (privatisation of economy, accession to NATO, administrative reform – set up second self - government level, efforts for accession to European Union) have influenced in this scope.

Therefore, Polish authorities have started wide – spread activities to establish legal frames for new civil protection and crisis management system. The main principle of this system is integration of local and governmental authorities, rescue services, civil defence formations, non-governmental organisations and other bodies activities. So far, Polish Parliament has enacted:

- State of Natural Calamity Act (2002),
- State of Emergency Act (2002),
- State of War Act (2002),
- Environmental Protection Act (2001) – this act codifies all aspects of environmental protection, among other control of major - accident hazards involving dangerous substances (implementation of European Council Directive Nr 96/82/EC – SEVESO II).

Besides, a group of experts has been appointed by the Minister of Interior Affairs and Administration to prepare new solutions in scope of civil protection, crisis management and rescue system.

Now, the main task is to introduce above mentioned acts into live. During this process we will take into consideration following aspects:

- compatibility of solutions have already established with solutions which are under preparation,
- protection of existing solutions that have been positively verified during really rescue actions (e.g. National Rescue and Firefighting System),
- adjustment of new solutions to international standards, mainly to NATO and European Union requirements,
- adjustment of new solutions to financial capabilities.

In regard to above mentioned conditions, existing plans and procedures are just really modified. Unfortunately, very often that modifications are taken directly in the face of a danger.

5.2 Critical infrastructure assessment

Interdepartmental Expert Group to revise of legal and organisational conditions in scope of critical infrastructure protection was appointed by Polish authorities in June 2002. Also, this group will work to prepare appropriate protection procedures concerning this area, adjusted to wide spectrum of new challenges and threats. In this context Poland is interested in development and promotion of trans - boundary and regional cooperation in scope of civil safety. In our opinion it gives opportunity for better adjustment of civil planning and crisis management process to challenges and threats really existing in particular regions.

First step done by the Expert Group was sending a critical infrastructure questionnaire to all departments, with request filling up it. The questionnaire included among other:

- general information about filling up department and persons,
- lawful and organised aspects, as e.g.: lawful bases of activities, management structures, critical infrastructure segments under competence scope and activity,
- technological aspects of critical infrastructure, as e.g.: databases in possession and their protection and using; used monitoring, management and controlling systems, digital maps, applications concerning decision support processes, information systems and their parameters, computer systems and their parameters, needed special protection: buildings, constructions and systems,
- critical infrastructure protection against destruction it, as e.g.: protection ways against physical destruction (included terrorism acts), protection ways of computer and information systems and mitigation ways, short describing of operational plans and procedures being in possession,
- possibilities of infrastructure reconstruction, as e.g.: describing of reconstruction plans, describing of maintenance ways of critical infrastructure main functions in case disruption and destruction possibilities in reconstruction scope of computer, teleinformation systems,
- international co-operation.

At the end of the questionnaire, there should be pointed an order of importance critical infrastructure segments. There were 14 segments: banking, common public safety, food and water supplies, energy, finances, working of public administration structures, health care, post office, public order, strategic industry (among other defended), teleinformation, telecommunication, transport.

There is prepared a first report from the polling. The report includes a lot of conclusions, among other, points at the most important segments of critical infrastructure, i.e.: energy, common public safety, teleinformation.

5.3 Critical Infrastructure Mitigation

There are many general safety requirements concerning all kinds of building, installations and other objects in Poland. Also, we have particular requirements for objects that are important from public safety point of view. But, in light of last experience, we assess that in scope of WMD (weapons of mass destruction) and terrorism threats, many solutions have to be modified. One of important point is to set up new procedures in scope of restoration of objects (buildings, installations, systems) were effected by WMD. Of course, firstly we should conduct detailed inventory of individual segments of critical infrastructure.

5.4 Laws and Authorities

As was mentioned at the beginning, Polish civil protection and crisis management system is changing at the moment. Despite this situation general rules and competent authorities are known. So, main responsible bodies are leaders of public administration on separate levels. Crisis management teams are organised to help them. Now, we have different teams for individual kinds of threats. In future we would like set up only one crisis management team at the separate administrative levels. Also, competence and activities co-ordination of rescue services, non- governmental organisations and other civil protection bodies must be clarified.