CRN-Workshop Report

Stockholm, Sweden, 2004

Societal Security and Crisis Management in the 21st Century

Swedish Emergency Management Agency

supported by
the Comprehensive Risk Analysis and Management Network (CRN)

SWEDISH EMERGENCY MANAGEMENT AGENCY

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

This report is also available on the Internet: www.isn.ethz.ch/crn

Author: Ulrike Kastrup

Postal address:
Krisberedskapsmyndigheten
Box 599
101 31 Stockholm
SWEDEN
Tel. +46 8 593 710 00
Fax +46 8 593 710 01
www.krisberedskapsmyndigheten.se
kbm@krisberedskapsmyndigheten.se

Center for Security Studies
ETH Zentrum SEI
8092 Zürich
SWITZERLAND
Tel. +41 1 632 40 25
Fax +41 1 632 19 41
www.isn.ethz.ch/crn
crn@sipo.gess.ethz.ch

6th INTERNATIONAL CRN EXPERT WORKSHOP
STOCKHOLM, SWEDEN
APRIL 22-24, 2004

Societal Security and Crisis Management in the 21st Century

Content

General information on the CRN:

The Comprehensive Risk Analysis and Management Network (CRN) is a Swiss-Swedish Internet and workshop initiative for international dialog and cooperation between governments, academics, and the private sector. As a complementary service to the International Relations and Security Network (ISN), the CRN is run by the Center for Security Studies at the ETH Zurich (Swiss Federal Institute of Technology).

The CRN's research covers a broad range of topics in the academic field of applied threat and defense analysis. Members of the research group are undertaking research in political violence movements, terrorism, the protection of critical infrastructure, and emergency response and management.

Twice a year the CRN organizes a workshop with its partners from Switzerland, Sweden, Austria, and Norway to discuss topics relevant to security politics.

The present report includes the presentations and findings of the 6th International CRN Expert Workshop that took place in Stockholm, Sweden, from 22-24 April 2004 and was organized by the Swedish Emergency Management Agency (SEMA). The topic of the workshop was **Societal Security and Crisis Management in the 21st Century**.

For more information please refer to the following websites:

Comprehensive Risk Analysis and Management Network (CRN), Switzerland
http://www.isn.ethz.ch/crn/

International Relations and Security Network (ISN), Switzerland
http://www.isn.ethz.ch

Center for Security Studies, ETH Zurich, Switzerland
http://www.fsk.ethz.ch

Swedish Emergency Management Agency (SEMA), Sweden
http://www.krisberedskapsmyndigheten.se/english/index.jsp

Directorate for Civil Protection and Emergency Planning, Norway
http://www.preparedness.no

Austrian Bureau for Security Policy/National Defence Academy, Austria
http://www.bmlv.gv.at

Introduction

In the past, military defense was considered the task of armed forces when protecting the state or fighting enemies, sometimes in close alliance with other countries. Security forces also provided intelligence, police, and search and rescue services. Armed conflicts were generally assumed to take place between states or to challenge the internal stability of individual countries through civil war. Recently, threats from international terrorism and the growing awareness that critical infrastructures and key assets are highly vulnerable have changed our concept of security and safety.

With the reassessment of security issues, new concepts and organizations can emerge. One example is the concept of homeland security in the US, whose emergence is a reaction to the threats faced during and after the attacks of 11 September 2001.

In Europe we have seen threats in the form of conflicts and war throughout most of the 20th century. The traditional answer to conflict has been to employ military resources and civil defense organizations within the framework of total defense systems.

Since the end of the Cold War, when the two opposing alliances ceased to fight for supremacy in Europe, the battle field has changed. Since 11 September 2001 and the conflicts that followed, the threats the Western world faces have become highly asymmetric. Today's threats are a challenge to the core values and concepts of modern Western democratic societies: stability, security, and trust. The recent terrorist attack in Madrid emphasizes the need to address societal security[1] within the European Union and the West as a whole.

The CRN workshop attempts to plot these changes in national security concepts and find models and concepts for redistributing responsibilities funding, in order to face the challenges of the 21st century.

[1] The workshop uses the term Societal Security in the context of a European version of Homeland Security (see: e.g., Sundelius, B., and Grönvall, J., *Strategic Dilemmas of Biosecurity in the European Union*, in: Biosecurity and Bioterrorism: Biodefense Strategy: Vol. 2, No. 1, pp. 17-23(7), 2004). The organizers and author are aware, however, that there is another, different use of the term Societal Security, that only relates to the threat to the *identity* of a collective, where a collective can represent a nation but also a religious or an ethnic group, etc. (e.g., Buzan, B., Wæver, O., and de Wilde, J., *Security: A New Framework for Analysis*, Boulder CO, Lynne Rienner, 1998).

Official Opening of the Workshop

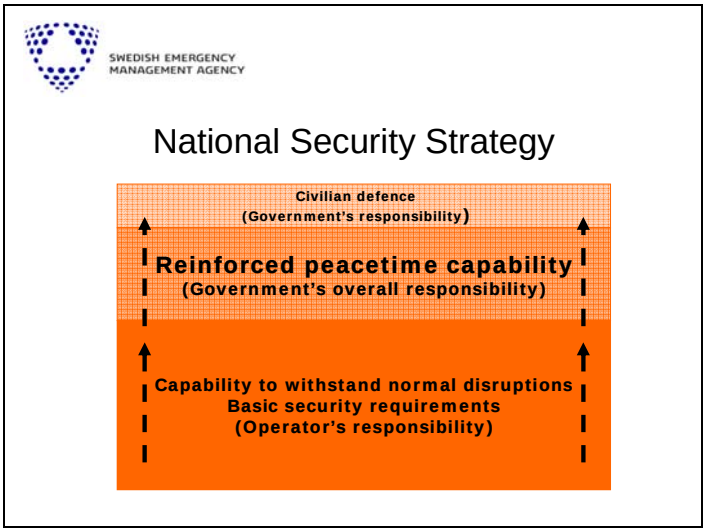
Mr Lars Hedström,
Deputy Director-General
Swedish Emergency Management Agency, Sweden

In 2002, the Swedish Emergency Management Agency was launched, with the idea of creating a new crisis management system. The agency's role is to support actors at a national, regional, and local level, to coordinate planning, and to contribute to the building and dissemination of knowledge within the system. SEMA promotes interaction between the public sector and the business sector in the emergency management area.

Why a new crisis management system and a new agency? Sweden has changed its concept. Total defense should be seen as one part of a larger national security concept, including all crises that can seriously jeopardize national security. The focus has changed from preparedness against war to preparedness against severe peacetime crises. Swedish society needs to enhance its crisis management capability. This can be achieved with a new perspective, with developed forms of cooperation, and with new forms of financing both basic security requirements and reinforced peacetime capability.

SEMA has proposed a national security strategy to the government for its Defense Resolution 2004 and its Defense Bill 2005. Planning and preparedness for severe peacetime crises needs its own perspective.

The following figure gives a basic overview of the national security strategy.



The boundary between the private and the public spheres has changed. This development has been particularly obvious in the infrastructure area. How do we share responsibilities in a time when government control is decreasing due to deregulation, privatization, and internationalization? The answer to this question calls for clear rules and for the delegation of responsibilities to government agencies and businesses. What methods shall we use to define minimum standards for security and to determine who is responsible for what?

Regarding financing, other sources of money than the current one need to be considered, such as taxes, fees, and voluntary financing. Some of the questions of how to achieve what kind of security is needed and who is responsible for it, legally and financially, will be subject this workshop.

The aim of this workshop is to discuss changes in concepts of national security and to create models and concepts for redistributing responsibilities, including power and financial means, in order to develop ideal structures for dealing with the challenges of the future.

I am looking forward to an open and fruitful dialog during this workshop, and I wish you all a warm welcome to Stockholm.

Goals of the Workshop

Mr Jan Lundberg
Swedish Emergency Management Agency, Sweden

"It takes a network to beat a network" -- We are witnessing the consequences of acts from international terrorist networks. It was not long ago that innocent commuters lost their lives in Madrid. Such acts are not acceptable in our societies. Governments have an obligation to protect their citizens and innocent civilians. This must be done while preserving our core values as democracies, an open society, the rule of law, transparency, and accountability. In order to achieve that goal, we have to cooperate within our countries, bilaterally and in international forums. We must create and maintain good networks to meet the challenges of societal security in the 21st century. Networks are structures where cooperation between various groups is fostered. The network we are working in aims at coping with security and safety challenges. The first goal of the workshop is to better understand these challenges of security threats and emergencies in modern society.

"Societal security" is the umbrella term for efforts to cope with modern security threats to society. The figures below list the desirable characteristics for a national strategy with respect to societal security issued by the United States General Accounting Office (here with special emphasis on combating terrorism). The second goal of the workshop is to achieve a better understanding of two of these objectives: One concerns the field of resources, investment, and risk management, and the other concerns organizational roles, responsibilities, and coordination.

To summarize:
The aim of the first day of the workshop is to get a better understanding of security concepts as a whole, with special emphasis on societal security; the aim of the second day is to narrow down societal security to the two objectives of finance and responsibility.

In detail:
Day 1 / Panel I
The challenge of security threats and emergencies in modern society

Core questions for Panel I:

- What is the specific content of the emerging security panorama in regard to the nation state's responsibilities?
- What challenges do the management of threats and vulnerabilities in modern society create?

- What are the objectives and rationale behind the security concepts? How applicable are they?

Goals for Panel I:

- Increase the understanding of various security concepts.
- Discuss a framework for analysing security concepts.

Day 2 / Panel II

Distribution of responsibilities and funding when dealing with societal security, public safety and emergency management

Core questions for Panel II:

- How can vertical and horizontal security, and safety co-operation be optimized?
- Who should set preventive priorities and define security standards?
- Who pays for and who will benefit from dealing with vulnerabilities?

Goals for Panel II:

- Analyse and identify the various *responsibility interfaces* (public-private, civil-military, federal-regional, etc.)
- Identify ways of creating effective instruments for safeguarding societal security.

Table 4: GAO Desirable Characteristics for a National Strategy

Desirable Characteristic	Brief description
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
Problem definition and risk assessment	Addresses the particular national problems and threats the strategy is directed towards.
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.

Source: GAO

Desirable Characteristic	Brief description
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.
Integration and implementation	Addresses how a national strategy relates to other strategies' goals, objectives and activities – and to subordinate levels of government and their plans to implement the strategy.

Source: GAO.

Source: GAO

Presentations

Transatlantic Homeland Security and Societal Security

Dr Daniel S. Hamilton
Johns Hopkins University, USA

The transatlantic link must become stronger than it is today. Together, the EU and the US can win. Divided, both sides will lose. On 12 September 2001, NATO's mutual defense clause, Article V, was invoked. This threat was not only symbolic; it was also an active expression of a very basic point: We share a common security space, and an attack against one shall be considered an attack against all (NATO, PfP, EU). We need, then, to think globally and to find a way to move from the local space to the global space. The transatlantic link is the only way to link the local, national, and regional with the global, with a global perspective on the challenges facing us. We must have a transatlantic consensus in order to build and protect on a global level.

Why must we think globally?

- Terrorists are recruiting, training, funding, and carrying out attacks in many countries.
- We need to think not only 9/11 but now also 3/11 (the Madrid bombings). The events of 9/11 and 3/11 clearly show that Al Qaeda poses a threat not only to the US but also to Europe.
- If the US and European systems cannot cooperate, how are other, far less similar systems going to cooperate?

Given the current state of affairs in a post-9/11 world, we must ask ourselves the following questions:

- Are we going to come together or not? Are we going to focus on similarities or differences between Europe and the US? We must remember, too, that both sides are in fact extremely polarized *within* themselves and not simply between one another.
- The use of war metaphors has a long tradition in US policy-making and in periods of ideological shift (war on drugs, war on poverty, war on Communism). In this case, we are looking at a war on terrorism. However, the "war" is much more than a metaphor. The Bush administration truly believes it is – we are – at war and is trying to rally international support around this war. Can countries in Europe accept this war analogy, particularly since Europe often thinks in terms of "systems" analogies (i.e. the analogy with crime) rather than war-related analogies? Europe and the US are, in a sense, approaching the issue of terrorism from different viewpoints, and this must somehow be addressed.
- Should an attack occur, do we in fact have a transatlantic homeland today, either as regards prevention or protection?

Regardless of these obstacles, we are not only lazy but also irresponsible, if we do not work together. In our efforts to attain greater collective civil security, we can employ the following strategies: 1) Go after terrorists, 2) deny them weapons (e.g. weapons of mass destruction, planes), and/or 3) protection (civil). The area of civil protection is in particular need of further development. There have been some developments in the area of civil protection since 9/11, although there need to be more. In terms of US-EU cooperation, some examples include Eurojust, European Arrest Warrant, terrorist assets seizure provision, and mutual assistance agreements. In terms of intra-EU cooperation, we have seen, among other things, the EU Solidarity Clause and the suggested appointment of a head of counter-terrorism. (As usual, the US isn't really sure what all of these developments within the EU actually mean, but they are pleased that things are actually happening in Europe.)

- What has the US been doing wrong thus far in terms of civil security?
  The US has been far too focused on the domestic sphere and has then attempted to simply export its domestic model. Thus, the US model of civil security is still not transatlantic enough.
- What has the EU been doing wrong thus far in terms of civil security?
  The EU is very confusing, legally. There are far too many unresolved legal issues between the EU member states and the pillars. This makes it difficult, if not impossible, to know who to contact for what.

There are many areas in which we need to change and/or do better, if we want to improve civil security. These areas will, however, require some sort of renegotiation of sovereignty questions (local, regional, national, supranational), as well as of civil liberties issues:

- Rather than controlling on our own territory goods that could potentially be used for terrorist acts, as we have done so far, we need to control these goods *before* they reach our own territory, as well as goods *on other people's* territory. This means taking measures at airports and ports *outside* the US, i.e. before shipping containers leave their port of departure. More sophisticated passports can provide better control of the people entering the country and of their former movements. A transatlantic standard of arrest is needed and already partly in place. However, the US death penalty is not an option for many countries and thus cannot be part of an arrest standard.
- We need to establish some systematic way of ensuring that there is no competition between areas where there should be collaboration. For example, we want to avoid a situation in which, say, Arlanda airport and Frankfurt airport compete with one another.

- Cyberspace/Internet (privacy versus security): In the use of cyberspace and the Internet, privacy issues collide with security issues. Using cyberspace and the Internet to trace terrorists' past activity can result in the invasion of the privacy of uninvolved people.
- More regular and more comprehensive intelligence sharing. We have a history of this with our allies, but we must all consider the gaps that may exist not only between but also within our own intelligence systems.
- Bio-terrorism: Issues related to bio-terrorism have been neglected in the past and need to be seriously addressed. Bio-terrorism has to become a central part of the security discourse. Bio-terrorism issues provide a necessary and important link between the US and Europe. To advance in this matter, both sides have to agree on the same language and process. Thus, bioterrorist threats have to be considered as serious threats equal to nuclear threats. Further, it is necessary to have a productive dialog between biological and chemical weapons. And medical authorities and security authorities have to be alerted.

- We should use summit meetings to tackle some or all of the points reviewed above (NATO Istanbul Summit).
- The US should think seriously about adopting total defense concepts along the lines already developed and pursued in certain European countries (e.g. Sweden and Switzerland)—the idea of societal security and mobilizing *all* sectors of society to protect society. The US does not yet have this sort of "psychology," although Homeland Security is a step in this direction. This would mean listening to US partners and not just US allies.

Concluding remarks

For the EU and the US, NATO, rather than, say, the PfP, is the best way to address these vital civil security issues. This is the track that the US and Europe should pursue. Let us revitalize NATO. However, we must still allow for a focus on natural disasters. Let us also pursue greater cooperation with Russia on civil protection, and by all means let us welcome the EU enlargement and explore the ways in which homeland security may fit into this process. Both the EU and the US benefit from an enlargement that works to create, with the aid of EU norms and EU influence, a strong, standardized, and therefore safer space.

Panel I

The challenge of security threats and emergencies in modern society

The Challenge of Security Threats and Emergencies in Modern Society

Prof. Bengt Sundelius
Uppsala University and the National Defence College, Sweden

Security challenges

During the Cold War the world was primarily focused on state threats – armed attacks by other states. However, since the end of the Cold War, the spectrum of risks has widened. Figure 1 lists an overview of the various types of threats we have to be prepared to deal with today.

Figure 1: Security Challenges

		Examples
Actor-focused threats	1. Armed attack by another state	Military invasion
	2. Armed attack by another actor	Terrorists
	3. Attack by another state	Trade, finance, energy
	4. Attack by another actor	Information operations, critical infrastructures
Structural threats	Collapse of neighboring systems	Nuclear, energy, epidemics, violent civil unrest
	Severe domestic disturbances	Accidents, riots, epidemics, loss of democratic values

Two types of threats can be distinguished: *actor focused threats* and *structural threats*.

1. Actor focused threats
An actor can be a state, a formal or informal group, or an individual. A threat by a state can be a "traditional" threat, i.e. the threat of an armed attack. However, threats can occur through the trade, finance, and energy sectors. Cyber warfare is an example of an actor-focused threat that has received a lot of attention but for which interest is declining; this does not mean, however, that the threat has gone away. With respect to actor-focused threats we need to ask what happened, why did it happen, and who could have an interest in causing the threat. For example, if your computer fails, you want to know whether it was an accident or an attack and who or what caused it? Was it a state, a network, or a student in Arizona?

2. Structural threats
Structural threats are unintentional, non-military threats. Such incidents “simply happen” without any ill will being involved. Examples are threats arising from the collapse of a neighboring system that might result in serious energy problems due to subsequent bad maintenance. We also need to be prepared for severe domestic disturbances like epidemics and riots (for example, events like the Gothenburg riots in 2001 during the Swedish EU presidency). As mentioned above structural threats are non-military. Military actions could, however, cause structural threats such as the military metal scrap in the Barents Sea or the collapse of societies linked to warfare.

We must understand that we must not focus only on threats related to armed attacks. The shift from the protection of the sovereignty of nations to the protection of infrastructures and services does not change the overall aim we have to strive for: a guarantee of national security.

Concept and domain of European societal security in the making

(see Figure 2)

1. State security (law and order) and human safety (rescue services) operate in very different ways. There are barriers between the two; they have separate cultures, competencies, and thus often difficulties working together.

2. Societal security is the new dimension that is being constructed. It is meant to bridge the gap between state security and human safety. There have been various reforms, in Sweden and elsewhere, where new systems for crisis management and societal security are emerging. There is also an international element, as experts recognize that it is important to build security through international missions. But the example of the EU shows that it is difficult to link domestic and external security and safety at an international level. For one thing, there is a priority problem: What should be safeguarded and protected and why? What are the vulnerabilities? We also need to have recovery capacity, and we should focus not only on prevention and protection but also on the management and recovery from crises.

There is not enough money to do everything to counter every threat, so we have to decide: What is worth investing in? What is worth investing against? Where do we invest? What are our priorities?

3. We have to be aware of the link between the international and the domestic spheres – the *intermestic* sphere - as threats are emerging from both fields. In the intermestic sphere of Europe, for example, human safety is not only a national responsibility but also a European responsibility, as, for example, civil protection is not only a national but also a European issue. In the field of societal security, the European initiative of a solidarity clause came into being in March 2004. This means that member states shall support each other’s societal security with both military and civilian tools. Member states have to prepare for the implementation of the clause at the national level and through joint actions.

The following should influence our thinking about security in the European Union:

- It has to be multi-sector; we have to have safety and security cooperation and preparation in the health, financial, food, and transport sectors
- It has to be multi-level; the consequences have to be managed and prepared at all levels – local, regional, national, and European
- It has to be multi-institutional; the EU Commission (also the various directorates), the EU Council, and NATO have to be involved and have to be able to cooperate

- It has to be multi-national; there are 25 countries in the EU, plus the Brussels complex, that need to have a functioning relationship
- It should be multi-continental, including the EU, the US, and Euro-Russia

It is important for the future that a crisis *within* the EU does not become a crisis *for* the EU. This is a difference that we need to be aware of. The attack in Madrid was a crisis for Spain, but it also became a crisis for the EU. Such events, whether disasters or terror acts, should not become crises for the EU in the future.

Figure 2: Concepts and domains of European societal security in the making

OBJECTIVE	DOMAIN		
	Domestic sphere	**INTERMESTIC SPHERE**	International sphere
State security	Law and order	**Counter terrorism**	National defense
SOCIETAL SECURITY	**CM capacity**	**Solidarity clause**	**International CM capacity**
Human safety	Rescue services	**Civil protection**	International disaster assistance

Sweden: *"A New Security Strategy"*

Mr Michael Mohr,
Swedish Defence Commission, Sweden

Colleagues

I can see many familiar faces in this professional gathering. For those of you who don't know me already, my name is Michael Mohr and I am the Principal Secretary of the Swedish Defence Commission.

The Swedish Defence Commission is a forum for consultations between representatives of the Government and representatives of the political parties of Parliament in matters concerning the long-range development of Swedish Defence and Security Policy.

The Swedish Defence Commission is now working on a bill for a co-ordinated Swedish security strategy. I will give you a basic outline of the strategy as it appears at the moment. A decision concerning a Swedish security strategy is expected during 2005.

But let me begin by explaining why a co-ordinated Swedish security strategy is needed.

The structures that were built for securing Sweden's national security during the Cold War were based on the idea of total defence. At the time, this was the overall concept for how the country's co-ordinated resources could best be mobilized for meeting the total war. The Cold War ended long ago and as the EU expands, Sweden is now part of a Europe where most countries are members of the EU and NATO. Sweden's security policy situation, from the beginning of this century, has experienced fundamental changes.

A general trend is that borders have disappeared. Not only geographic borders, which were most obviously manifested during the Cold War by the Iron Curtain that divided Europe. The rapidly increasing use of electronic communications, and the globalisation of trade and commerce have led to an interconnected world. Over the past few years, major power failures have emphasized the vulnerability of our critical infrastructure. A common feature was that the disruption could not be stopped in time, large geographical areas were affected, and two or more countries were involved.

Country borders cannot stop natural disasters, technological breakdowns, or contagious diseases. Nor organized crime. In many conflicts, crime, and economic interests are the underlying causes. Criminal or failed states provide a breeding ground for instability in the international system, a base for drug and people trafficking, and a refuge for international terrorists.

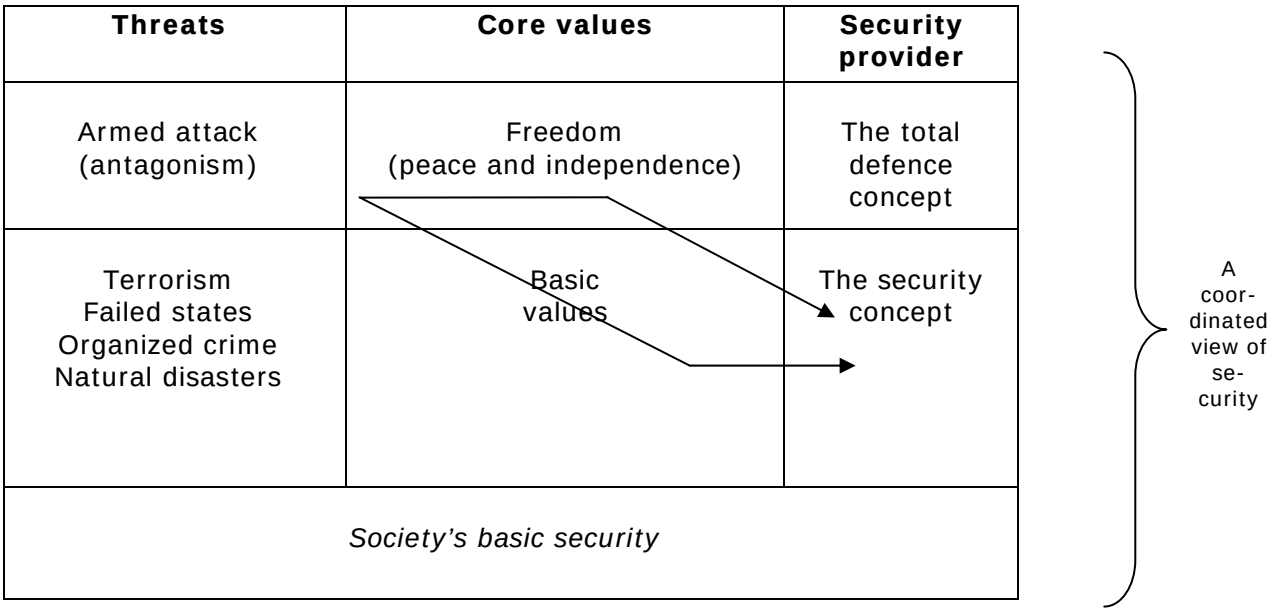
The boundary between private and public has also been changed. Deregulation and changed views of what a public undertaking involves has meant that many critical services are now provided of private companies. This development has been particularly obvious in the infrastructure area. This calls for clear market rules and for the delegation of responsibilities between government agencies and businesses.

The increasing threat of international terrorism is a reality that all countries have to deal with. Networks of groups and individuals exploit the vulnerability of our society. In the USA, Indonesia, and Spain, we have witnessed the effects of terrorism that aims to cause the maximum damage possible. A few terrorists have succeeded in spreading fear and terror throughout the community. A nightmare scenario is terrorists who acquire weapons of mass destruction.

I have now described some of the developments that underlie the need for a co-ordinated security strategy. To summarize, the Cold War security concept is no longer viable for protecting today's society and its individuals.

Our society is built upon certain basic principles, i.e. democracy, human rights, security, freedom, tolerance, pluralism, and legal security. These values are fundamental in the sense that they underpin and legitimize the institutions of our society. These institutions give society a positive focus for its development and coherence. Some of the most important institutions are the Government, the market, defence, the legal system, medical services, the media, schools and science. All of these institutions comprise standards and regulations. Most of the institutions also have obvious physical structures that represent important symbolic values.

The following diagram summarizes developments from the total defence concept to a new security concept. The three dimensions: threats, core values and security provider describe the successive security policy development.



The purpose of a co-ordinated security strategy is, in one context, to structure the views of threats to, and the goals for, Swedish security. It will also address views concerning funds, players and methods for creating prerequisites for an effective and rational use of resources for the prevention and management of all types of strains in the scale of threats, both national and international. Such a strategy will create prerequisites and attempt to, for example:

- create a common policy for security-building efforts for the whole scale of threats, and across several policy areas
- highlight the connection between everyday security work and efforts to strengthen society's capacity for handling more serious crises
- highlight the co-ordinated national-international dimension of security-building efforts
- define Sweden's role from an international security perspective
- provide a basis for forming Sweden's contribution within the framework of the EU's security strategy and the subsequent expectations of Swedish actions
- create an appropriate balance between military and civilian resources

- create a common and co-ordinated basis for adapting and renewing policy areas, instruments of control, government agency structures, and financing forms

When forming a co-ordinated view of security, it is important to maintain a broad perspective. This should include the more traditional dimensions of security, with obvious links to the military security component, and the broader perspective where other dimensions of security policy are considered, including security as a prerequisite for development. This is essential for finding an overall security concept that can handle the broad spectrum of threats and risks to which society and its individuals are exposed.

When the basis is that the Government with specifically assigned funds will be responsible for funding the measures that target extreme events with low probability, but that these funds will not finance the basic security that must exist in order to handle everyday accidents and strains, the basic security requirements in different areas of critical operations must be made clear.

In order to create an operation that strengthens our society in the best way possible, the balance between the requirements of different sectors must be evaluated from a holistic perspective, and the boundary between these basic security requirements and the requirements within the framework of a strengthened capacity should be regularly revised and tested.

The Swedish Emergency Management Agency has made a request to review existing security requirements over the next few years in order to clarify the demands on each responsible player, and to compare these with demands in other sectors of society. Balanced and well-adjusted basic security requirements are essential for creating an effective structure and operation for society's overall security and emergency preparedness.

I understand that you will discuss the delegation of responsibilities and venture financing in the area of societal security during panel II. Because of the intensive work in the Swedish Defence Commission I cannot stay, but I certainly look forward to seeing the results of your discussions.

I do have time to answer some questions, however.

My e-mail address has also been included in the list of participants, so please feel free to send me your views or comments.

Austria: "*Comprehensive Security"*

Dr Henriette Riegler
Austrian Institute for International Affairs, Austria

In the 1970 and 1980s, the concept of comprehensive security was formulated, following an immense debate on ecological and environmental problems. In contrast to military security, which dominated security politics during the Cold War, comprehensive security also takes non-military threats, such as nuclear safety and climate change, into account. The discussion on extending the security concept into non-military fields was mainly led by non-state actors (e.g., NGOs) and was later also taken up by the academic community. The traditionalists, who support the traditional understanding of security (i.e.military security), were not in great favor of such a development. However, the inclusion of the non-military security field has proven to be more and more necessary. Thus, when we advance the concept of security today, we have to move away from a traditional, state-centered understanding of security and must look ahead towards a comprehensive understanding of security.

The problem nowadays is, however, that our society feels uneasy when it is confronted with security issues and threats. Many countries believe that if they do nothing bad (in their understanding), nobody will be provoked into harming them – so, why worry? This is a misleading perception, as we learnt by the attacks of 11 September. In Europe, many also fear that whatever measures the EU might take, the measures could be detrimental to civil liberties. It is thus most important to open up the public discourse and involve the people into the discussion about the measures for countering today's threats against our Western values, such as democracy, liberalization, and the division of state and religion. Terrorism could be the litmus test of Western cohesion; it will show if and how Western society can be influenced by outside actors.

In Austria it is still unclear how to react, if Austria should become the object of a terrorist attack. This issue will become important to many other security problems, for example, migration. A question that might come up is what will happen if immigrants do not want to integrate into Austrian society? Will this cause segregation? What impact could that have on the political system? Will it lead to a non-demographic society or even a fascist political system?

These are questions that need to be addressed when we discuss today's threat to modern Western society. They cannot be answered by a pure military perception of security; they require a broader vision, and they require a comprehensive understanding of security.

Risk and Uncertainty Management Strategies

Prof Jan Hovden
Norwegian Technical and Natural Sciences University, Norway

Introduction

The modern awareness of risk is not about our own experiences or about the current statistical risk image of deaths, harm, and injuries. Rather, it is about an uncertain future. Fear and anxiety of threats about which we are uncertain or ignorant are a great challenge for risk management, even though the probabilities of such events occurring may be very small. The frightening thing is that we don't know and have no control. We feel like victims. Therefore, the risks are real but also in a way unreal and unintelligible. A main difference from traditional risks is that they are independent of the place where you live or work. Radiation is spread by wind, toxic materials are spread by rivers and ocean currents, IT viruses are spread by global networks, epidemics are spread by airplane travelers, and hate by fanatic groups results in terrorist attacks in New York, and Madrid.

This presentation aims contributes to the discussions at the workshop on the concepts of risk and uncertainty and related management and governance strategies in different domains of threats and hazards.

In dealing with risk and vulnerability issues, we can cite Aristotle: "It is probable that the improbable will happen" and Roman historian Pliny the elder: "Solum certum, nihil esse certi". The new technological, nuclear, chemical, ecological, biologic, and genetic risks and the political and social risks, such as terrorism, are difficult to separate and survey in time and space and to explain with the rules of causality, and it is difficult to define guilt and punishment and to compensate and to insure such risks, which represent "produced uncertainties", to quote U. Beck (1986).

Scope Figure 1 illustrates the scope and variety of the subject. The vertical axis gives the links between the global, international, national, regional, local, and individual stressors and the actors at various levels who deal with risks. A main challenge is to coordinate the information and actions between the levels and layers of risk and vulnerability management systems.

The horizontal axis shows that the field covers everything from acts of God and man-made and technologically induced disasters to deliberate, malicious acts against others and self-destructive behavior. Societal vulnerability usually refers to problems related to the survival and recovery of vital societal functions, i.e. threats to infrastructures, energy supplies, and ICT (Hovden, 2001). Many important risk activities and phenomena lie somewhere between the two extremes, e.g. unintentional and non-malicious shortcuts

and law and rule violations. Individuals and companies are gambling with safety and security requirements, as most of the time nothing goes wrong.

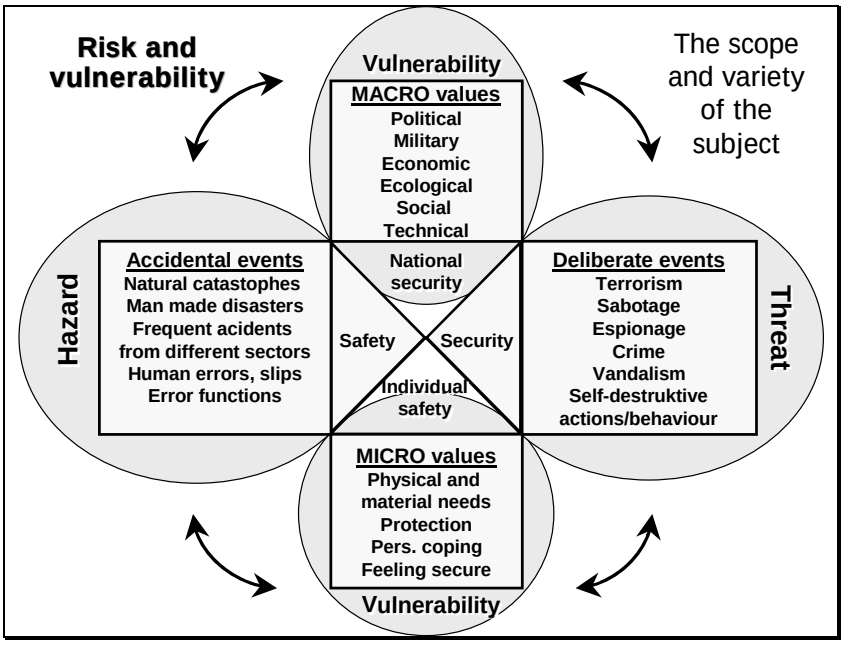


Figure 1 The vertical macro-micro perspective on risk management combined with types of hazards, threats, and events (Hovden, 1998).

Epistemological approaches to risk

The dichotomy above between natural-scientific objectivism and cultural relativism can be detailed and paraphrased as follows (partly based on Lupton, 1999):

- *Rationalist* – The rationalist sees risks as real world phenomena to be measured and estimated by statistics, prioritized by normative decision theory, and controlled by scientific management.
- *Realist* – The realist sees risks as objective hazards or threats that exist and can be estimated independently of social and cultural processes but that may be distorted or biased through social and cultural frameworks of interpretation.
- *Constructionist* – The constructionist sees nothing is a risk in itself. Rather, what we understand to be a risk the constructionist sees as the product of historically, socially, and politically contingent ways of seeing.
- *Middle positions* between realist and constructivist theory – Proponents of a middle position sees risk as an objective hazard or threat that is inevitably mediated through social and cultural processes and can never be known in isolation from these processes.

For an in-depth review of scientific positions and theoretical approaches in risk research, I recommend Jaeger, Renn, Rosa & Webler's book Risk, Uncertainty, and Rational Action (2001).

Different risk arenas and domains have different traditions and approaches to risk and uncertainty management. The fields of environmental risks, industrial safety, food and

product safety, transportation, defense, ICT security, and the types and approaches to crime can learn a lot from each other.

Risk and uncertainty management strategies

Ortwin Renn and his colleagues at the Center of Technology Assessment in Baden-Württemberg, Germany, have made a valuable contribution to risk management strategies. A brief review of their proposals is presented below.

Renn (2002) describes the common features and limits of the traditional method of assessing risk as follows: The traditional method relies on the relative frequencies and statistical data for expressing probabilities. The only effects considered undesirable are physical harm to humans and to ecosystems. This method thus excludes social and cultural impacts. Only rough estimates for socially induced risks, such as sabotage, terrorism, and human errors, are part of this modeling. The probability and extent of adverse effects are normally multiplied, that is, this is an expected value approach.

The proposed risk classification by the Global Change Council of the European Commission (EC) attempts to respond to the challenges of risk assessment challenges (Renn, 2002):

- Probability
- Potential for harm
- Uncertainty (variability, statistical, genuine, ignorance)
- Ubiquity
- Persistence
- Delayed effects
- Equity violations
- Potential for social mobilization.

Combining these dimensions of the EC risk concept, Klinke and Renn (2001) developed six main types of risks that determine risk management strategies. These risk types, named after characters from Greek mythology, include:

- *Damocles:* high catastrophic potential, probabilities (widely) known*Cyclops:* no reliable estimate on probabilities, high catastrophic potential at stake*Pythia:* causal connection confirmed, damage potential and probabilities unknown or indeterminable*Pandora:* causal connection unclear or challenged, high persistency and ubiquity (bio-accumulation)*Cassandra:* intolerable risk of high probability and great damage but long delay between causal stimulus and negative effect*Medusa*: perception of high risk among individuals and large potential for social mobilization without clear scientific evidence for serious harm.

When these six risk types are presented in a risk diagram (see Figure 2), we get a visual impression of the uncertainties related to the different risk types, that is, the areas covered by the actual risks. I have added the threats from terrorism to the figure.

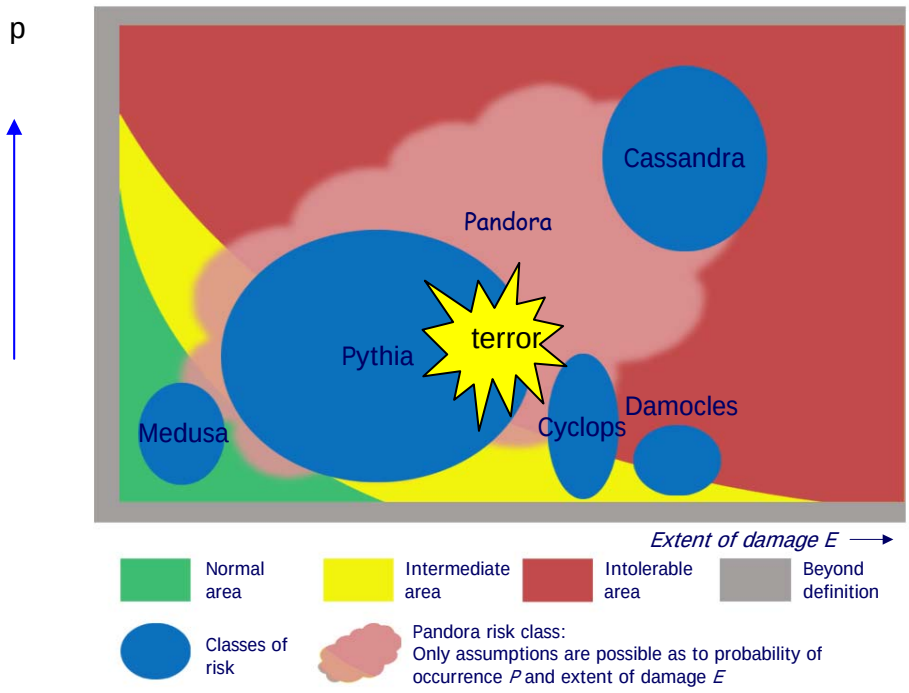


Figure 2 Risk classes. Source: WBGU, German Advisory Council on Global Change. The figure is a copy from a presentation by Renn (2002).

As most risk evaluation processes do, Figure 2 also distinguishes between three categories of risk: the normal, the intermediate, and the intolerable area. The diagram avoids the terms “acceptable”, “ALARP region”, and “unacceptable” due to possible moral implications. The terms “tolerable” and “intolerable” are ethically less emotional or sensitive. In practice in decision-making, the meaning is almost the same.

To deal with the important features for the six risk types, Klinke & Renn (2001) propose three alternative – or combined risk management – strategies:

- Risk based or risk informed management strategies (Damocles and Cyclops)
  - Sufficient knowledge of key parameters
- Precautionary or resilience based strategies (Pythia and Pandora)
  - High uncertainty or ignorance
- Discursive management strategies (Cassandra and Medusa)
  - High ambiguity

Risk-based management is characterized by an emphasis on scientific assessment, reduction of exposure and/or probabilities, risk management according to expected values on risks and benefits, and reliance on inspections, auditing, and routine controls. Examples are: industrial plants, large dams, bridges and highways, liquefied natural gas terminals, transportation (road, railway, shipping, and aviation), classic infectious diseases, and health risks.

Resilience-based management is characterized by an emphasis on trans-disciplinary research and investigations, the containment of application (in time and space), constant monitoring, redundancy and diversity in safety design, (strict) liability, and a no tolerance policy for risk control – in extreme cases, prohibition. Examples are: biotechnology, Internet sabotage, new epidemics (new mutations), bovine spongiform encephalopathy (BSE), and extreme weather events due to global climate change.

Discourse-based management is characterized by an emphasis on reaching political consensus or agreement, the importance of procedure and transparency, the establishment of trust-generating institutions, an investment in risk communication, the involvement of stakeholders, including industry and governmental organizations, and public participation. Examples are: genetic engineering, industrial food production, biochips for human implementation, electromagnetic fields, and risks to consumers' way of life.

The main conclusion in Klinke & Renn's article is that risk management strategies need to be tailored to the main characteristics of the risk source in question. That means that in a security and crisis management regime, there should be a number of different means and strategies for dealing with the variety of risk types we face.

Concluding remarks on the government of risk and uncertainty

A comparative study of the anatomy of risk regulation regimes by Hood et al (2001) shows a substantial variety in the way hazards and threats are dealt with within countries and between countries. This supports Klinke & Renn's arguments on tailored risk management systems. However, it is difficult to conclude that one strategy is better or worse than another. It depends on the actual hazard or threat to be controlled and the specific context and political-administrative culture of each country. Nevertheless, there are some common problems and challenges.

According to a report by the Norwegian Commission on a vulnerable society (NOU 2000:24) – a comparative review on how countries like Sweden, the Netherlands, Germany, Switzerland, Britain, and the US have organized their safety, security, and crisis and emergency organizations – the concrete principles and ways of organizing these institutions and services differ considerably, i.e. the regulatory "jungles" are different. None of these countries could demonstrate a system superior to the others. Behind each system design there are traditions, political cultures, and contingencies specific to each country. However, what the countries have as common challenges are a lack of transparency, coordination, and unambiguous lines of responsibility.

A common trend in Europe and the US for the last 10-15 years is the dominance of a risk-cost-benefit analysis culture (risk-based approach) in more and more societal domains, i.e. the EU's New Method, ALARP principles, and functional requirements. Deregulations and globalization seem to require more and more complex and sophisticated risk regulations and governance. A paradox? The answer to the challenges of the risk society (Beck, 1986) is a risk regulatory state, an audit society, and a tremendous increase in standards and soft laws.

As mentioned in the introduction, the modern risk awareness is not about our own experiences or the current statistical risk picture of damage, deaths, and injuries. Rather, it is about an uncertain future. Societal security and crisis management institutions cannot solve these uncertainties, but by dealing with the hazards and threats in a constructive way, trust can be achieved and maintained. That makes it more comfortable to live with uncertainties.

References

Adams, J. (1995) *Risk.* UCL Press, London.

Beck, U. (1986) *Risikogesellschaft: Auf dem Weg in eine andere Moderne.* Suhrkam Verlag. Frankfurt am Main. or Beck, U. (1992) *Risk Society: Towards a New Modernity.* Sage Publ., London.

Galbraith, J.K. (1977) *The Age of Uncertainty.* London.

Giddens, A. (1990) *The Consequences of Modernity.* Polity Press, Cambridge.

Giddens, A. (1991) *Modernity and Self-Identity.* Polity Press, Cambridge.

Habermas, J. (1990) *Moral consciousness and communicative action.* MIT, Cambridge, Mass.

Hood, C., Rothstein, H. & Baldwin, R. (2001) The Government of Risk. Understanding Risk Regulation Regimes. Oxford University Press.

Hovden, J. (1998) Ethics and safety: "mortal" questions for safety management. Paper at the conference *Safety in Action,* Melbourne, Febr, 1998.

Hovden, J. (2001) Public Policy and Administration in a Vulnerable Society. Paper at *The 5th International Conference on Technology, Policy and Innovation. Delft2001,* Den Haag.

Jaeger, C.C., Renn, O., Rosa, E.A. & Webler, T. (2001) *Risk, Uncertainty, and Rational Action.* Earthscan Publ., Ltd., London.

Klinke & Renn (2001) Precautionary principle and discursive strategies: classifying and managing risks. In *Journal of Risk Research*. 4 (2), 159-173

Krimsky, S & Golding, D. (eds.) *Social Theories of Risk.* Praeger Publ., Westport.

Luhman, N. (1993) *Risk: A Sociological Theory.* Aldine de Gruyer, N.Y.

Lupton, D. (1999) *Risk.* Routledge, London.

Perrow, C. (1984) *Normal Accidents. Living with High-Risk Technologies.* Basic Books. N.Y.

Rasmussen, J. (1997) Risk management in a dynamic society. A modelling problem. In *Safety Science.* Vol. 27, No 2/3, 183-213.

Renn (2002) Risk Classification and Risk Management Strategies. Handouts at the seminar *"Risk and Uncertainty"*, Oslo.

See also http://europa.eu.int/comm/food/risk/session1_1_en.pdf

Sagan, S.D. (1993) *The Limits of Safety: Organizations, Accidents and Nuclear Weapons.* Princeton Univ. Press, Princeton.

Shrader-Frechette, K.S. (1991) *Risk and Rationality. Philosophical Foundations for Populist Reforms.* Univ. of California Press. Berkeley.

Turner, B.A. & Pidgeon, N.F. (1997) *Man-Made Disasters.* Butterworth-Heinemann, Oxford.

Panel II

Distribution of responsibilities and funding when dealing with societal security, public safety and emergency management

Minding the Gap:
Reconciling Responsibilities and Costs in the Provision of Societal Security

Jan Joel Andersson and Andreas Malm

This paper is a slightly revised version of an earlier paper entitled "**Distribution of Responsibilities and Money in Dealing with Societal Security, Public Safety and Emergency Management**" presented in April, 2004 at the 6th international expert workshop under the auspices of the Comprehensive Risk Network (CRN) and organized by the Swedish Emergency Management Agency (SEMA). We wish to thank the participants at this conference for their helpful comments and suggestions.

Jan Joel Andersson, *jan.joel.andersson@4cstrategies.com*
Andreas Malm, *andreas.malm@4cstrategies.com*
The views in this paper represent the views of the authors and not necessarily those of 4C Strategies AB

Introduction

Over the past two decades, great shifts in economic policy have taken place in Europe. Among the most important of these shifts have been the privatization of public monopolies, infrastructure networks, and the deregulation of service provision – functions classically associated with national governments.[2] Driven by poor performance and inspired by neo-liberal economics, public monopolies have undergone dramatic transformation. In many European countries, the provision of energy, communication, transport, financial services, and health care have all been, or are being, privatized and previously protected markets deregulated. These changes are meant to increase competition, improve productivity, provide more consumer choice, and lower prices. However, while liberalization in many cases has improved efficiency and productivity, it has also led to concerns regarding the accessibility, equality, reliability, and affordability of services.[3] Moreover, the privatization of public monopolies and infrastructure networks and the deregulation of service provision have important implications for national and international emergency preparedness and crisis management.

To survive in a market driven economy, companies need to minimize costs and maximize profits. With pressure to cut costs less resources are available for security and crisis management. Keeping reserve stock, maintaining redundant systems, and employing back-up staff all cost money. To save money, activities and support functions previously performed by in-house experts and staff are frequently contracted out to external consultants. While costs may be reduced, emergency preparedness measures and crisis management capabilities are also reduced. Yet in a modern society, uninterrupted energy supply, communication, transport, financial services and health care, must be maintained at all times.

In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing functioning systems and services. However, assigning responsibility for securing such systems and services in a liberalized global economy is more problematic. Who should implement and pay for the protective measures that have to be taken to ensure homeland security? Which measures should be the responsibility of national and local governments and which the responsibility of the private sector? How do national solutions to these problems fit with the internationalization of markets for goods and services and the emergence of transnational information and communications networks?

The first step towards greater homeland security is effective emergency preparedness and crisis management measures. While there is wide agreement that emergency preparedness is important, the question of what should be done and who should pay for it nonetheless remains.[4] Public-private partnerships (PPPs) have been proposed as an answer to the questions of responsibility and financing. In fact, PPPs are considered by many to be a panacea for all governance problems in a deregulated economy.[5] As we argue in what follows, it remains to be seen, however, the extent to which such partnerships are a panacea rather than a Pandora's box.

In this paper, we aim to do three things. First, we will discuss why public-private partnerships have emerged as a preferred choice for governments when it comes to

[2] Cerny 1995.
[3] See, for example, Héritier 2001, 2002.
[4] See, for example, O'Hanlon et al 2003.
[5] Partnerships between public and private actors to fulfill public functions are on the increase at every level of government. Public-private partnerships have been suggested to improve everything from inner city urban development to relations between third world countries and multinational corporations. In the United States and Canada, for example, PPPs currently operate in most policy areas, and in the US trial programs are planned by the Internal Revenue Service, the Census Bureau and the Social Security Administration. See, for example, Beck and Hardcastle 2003; Madanaipour and Magalhase 2002; Davids 1986; Osborne 2000; Vaillancourt-Rosenau 2000; Stiles and Williams 2000; Stephensons 1991.

providing market-corrective regulation in a liberalized economy. Second, we will outline some of the prospects and pitfalls of this approach and examine why PPPs might constitute only a *second*, or less desirable, choice for private actors. Rather than a panacea for liberalized economies, such partnerships may instead become a Pandora's box for many governments—an unreliable and unpredictable solution to the problem of under-provision of governance in deregulated sectors of society, particularly in the areas of national emergency preparedness and crisis management. We will subsequently explore this argument by examining the cases of energy and financial services sectors.

The Problem

Why is it particularly problematic when it comes to the provision of emergency preparedness measures in a liberalized economy? A fruitful way to think about emergency preparedness is to view it as a service for managing risks. Basic economic theory tells us that the optimal level/amount of emergency preparedness is reached when consumers' willingness to pay for extra emergency preparedness is just equal to the cost of providing it. In practice, we should think of this level/amount as a "zone of adequacy" within which both the value of emergency preparedness and the cost of providing it will be relatively stable rather than a singular point. In a liberalized economy the question of primary importance then becomes whether markets are likely to respond effectively to current and expected future risks.

Proponents of liberalized markets argue that appropriate amounts/levels of emergency preparedness can be provided by the market on its own and does not necessarily imply any kind of government intervention.[6] Private actors should have a very strong incentive to provide pro-active and effective emergency preparedness and crisis management without any government intervention or regulation. After all, it ought to be any private actor's worst nightmare to fail in providing a key service to its customers because of inadequate emergency preparedness and crisis management.

However, while individuals and companies may have strong incentives to provide effective emergency preparedness and crisis management, private motivation is unlikely to be sufficient to provide an optimal amount of emergency preparedness for society as a whole. In fact, private motivation may not even be enough to provide emergency preparedness and crisis management capabilities to ensure individual corporate safety(!), let alone safety for society at large.[7] A recent disaster research study conducted by the University of Texas shows that only six percent of companies that experience a disaster with catastrophic losses survive in the long run (two years and beyond).[8]

While the market, in theory, may deliver emergency preparedness that could be adequate for society as a whole, there are several reasons to believe that it will not be able to do so. First, market failures and imperfections generally exist to such a degree that they may prevent the market mechanism from functioning efficiently. Second, even with a perfectly functioning market, the assumption that the market clearing "zone" of emergency preparedness is adequate for society at large seems inappropriate from a societal perspective. Since no system can ever be totally secure, the question of how much security and preparedness is enough is always present. It does not take much to see that a government may have higher ambitions of security and emergency preparedness than the market by itself is willing to contribute towards.

---

[6] See for example Shuttleworth et al. 2003.

[7] Stephen Castella at Morgan Stanley once asked the question "Have you ever wondered why you have never heard of a company that did not have a contingency plan?" Stephen Castella, CPM, www.contingencyplanning.com, BCP 102: *Continuity of Information Foundations for Successful BCP in Your IT Department*, January 2001

[8] University of Texas, Texas A&M University Hazard Reduction and Recovery Center, http://hrrc.tamu.edu, *Business Disaster Recovery Study*, 2001

In short, while individuals and companies in a liberalized economy have strong incentives in theory to provide effective emergency preparedness and crisis management, private motivation is in reality unlikely to be sufficient to provide an optimal amount of emergency preparedness for society as a whole. There are several reasons why private actors are unlikely to respond in a manner efficient for society as a whole to current and expected risks in the provision of emergency preparedness measures on their own in a liberalized economy. Among these reasons, the most important are associated with market failures, imperfect information, and moral hazard. Let us examine these reasons in more detail before discussing why some form of government intervention is necessary to ensure an optimal level of emergency preparedness for society as a whole.

Market Failures

A first reason why national emergency preparedness will be undersupplied by private actors is because it is a public good.[9] If one citizen is protected by national emergency preparedness, no other citizen is less protected. The problem with emergency preparedness (like all public goods) is that once it is produced, the marginal cost of consuming it is 0. Hence, the price of this good should also be 0. However, if the good is costly to produce, no private firm will produce it since it cannot charge for it. In a free market, private actors will undersupply non-excludable public goods.[10] Since national emergency preparedness measures are a non-rival good and costly to supply, private actors will undersupply it in a liberalized market.

A second reason why market failure occurs in providing national emergency preparedness measures against large crises is negative externalities. An externality is an effect of actions of an individual that affects the welfare (utility) of others.[11] For example, a poorly maintained power grid can lead to a major power outage. However, the full cost to society that follows from a major power outage is not borne by the power grid operator alone. Hence, the power grid operator will not consider the full effect on society as a whole when he/she decides on what amount of emergency preparedness to have. As a result, the market rate allocates resources inefficiently.

In general, a negative externality can also arise whenever the emergency preparedness of a firm is adversely affected by poor emergency preparedness at another firm. Such interdependent security problems can lead to "contamination effects" and affect the willingness of one firm to reduce its exposure to risk due to the lack of appropriate behavior of other firms.[12] In such a case, private actors will under invest in emergency preparedness and crisis management measures that would be desirable for society as a whole. Private actors deciding how to best prepare for large scale emergencies and crises are unlikely to take the external costs of such an event fully into account. They will therefore generally provide an inefficiently low level of preparedness against major emergencies and crises on their own. Without government involvement, private actors will thus generally under invest in emergency preparedness and crisis management measures.

Imperfect information

A third reason why the market will be unable to provide the "appropriate" level of emergency preparedness for society as a whole is lack of perfect information. If information is not perfect, the market is incomplete and inefficient.[13]

---

[9] Goods are public if they are non-rival in consumption. National defense is a classic example of a public good because if the armed forces defend one citizen, no other citizen is less defended.
[10] If public goods are excludable, they will be underutilized. Przeworski 2003, p. 32.
[11] An externality is positive if the action of an actor increases the welfare of other individuals. An externality is negative if the action reduces the welfare of others.
[12] See Kunreuther and Heal 2003; Kunreuther, Heal, and Orszag 2002.
[13] Greenwald and Stiglitz 1986; Stiglitz 1994, chs. 3-4.

It is costly and extremely difficult to accurately evaluate emergency preparedness measures. To successfully do this would require active and consistent collection, analysis and dissemination of information of current and future risks. It would also require continuous assessment of current emergency preparedness levels in society as whole in order to stimulate and verify that implemented emergency preparedness measures lies within the "zone of adequacy". However, neither individuals nor individual companies have the resources or knowledge to evaluate the optimal level of emergency preparedness for major national crises. Arguably, only national governments have the resources to actively and consistently collect, analyze and disseminate information on current and future risks as well as the current security level in order to stimulate and verify that it lies within the "zone of adequacy". In a situation without any government regulation, or minimum standards, it is likely that private actors will under invest in emergency preparedness and crisis management measures.

Moral Hazard

A fourth reason why private actors will not provide "adequate" emergency preparedness measures is the existence of moral hazard. Many companies are unwilling to assume the costs for implementing necessary emergency preparedness measures since they expect the government to bail them out in case of a major emergency or crisis. There are numerous examples of governments picking up the bill of private industry after major crises. For example, government assistance has been extended to struggling banks in many countries and massive financial aid was given to the airline industry after the attacks on September 11, 2001. If the government is unable to credibly commit to not bailing out the private sector after a major crisis, it will create a moral hazard. If private firms expect the government to pick up the bill, they will under-provide emergency preparedness measures.

Moreover, bankruptcy laws limit individual and corporate financial liability for the effects of major crises. Thus, private actors have little incentive to prepare for large-scale emergencies and catastrophes. If a major crisis would lead to losses exceeding a private firm's net assets, and the government refuses to bail it out, the firm would simply declare bankruptcy. Since the outcome of a major crisis for a firm's owner does not vary beyond bankruptcy, the firm has little or no incentive to reduce the effects of the most severe kinds of crises by improving its emergency preparedness, even if the required steps were relatively inexpensive and would greatly benefit society as a whole.

The importance of each of these reasons may, of course, vary from case to case. However, the fact remains that in a deregulated economy, the market will in general under provide emergency preparedness measures. At the same time, uninterrupted energy supply, communication, transport, financial services and health care must be maintained in a modern society at all times.

The Role of Government

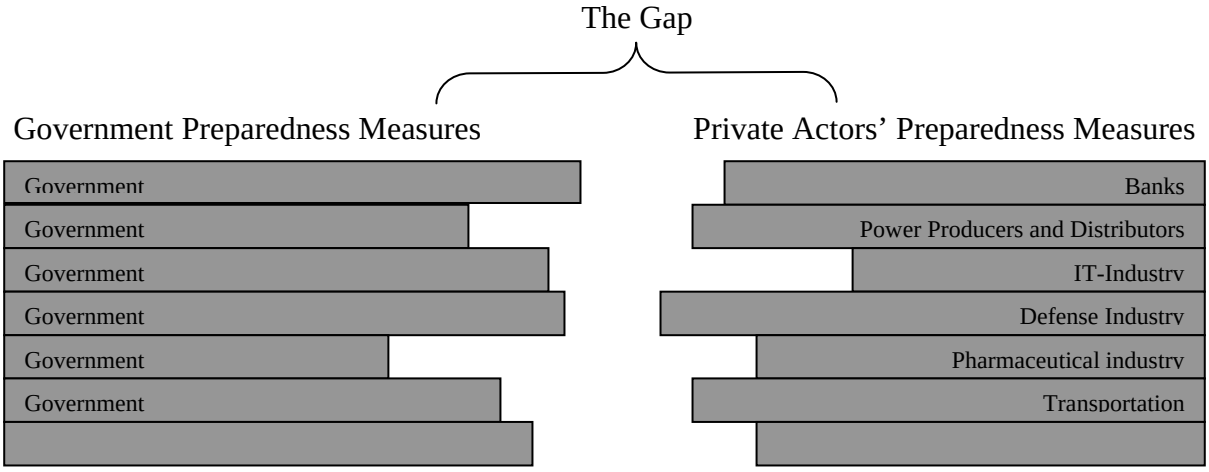
National Defense is the sole responsibility of the government, but who is responsible for "homeland defense"? In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing critical infrastructure systems and services to ensure societal security and public safety. It is more problematic assigning a clear responsibility for securing such systems and services in a liberalized economy where the majority of critical infrastructures is in private hands. Given the importance of the private sector in providing societal security and emergency management it is paramount to establish where and when private sector responsibility for societal security and public safety ends, and where and when government responsibility begins. Who should implement and pay for the protective measures that have to be taken to ensure societal security and public safety? Which measures should be the responsibility of national and local governments and which the responsibility of the private sector? Finally, how does the internationalization of markets and services affect these issues?

While liberalization of previously government controlled sectors and markets – such as energy, communications – in many cases has improved efficiency and productivity, it has also led to concerns regarding the accessibility, equality, reliability, and affordability of services. Moreover, the privatization of public monopolies, infrastructure networks, and the deregulation of service provision have important implications for national emergency preparedness and crisis management. While costs may have been reduced, redundancies and reserve capacity have also been reduced.[14] The government no longer has the reserve capabilities, resources, or manpower to manage major crises it once had and private companies are unable and unwilling to assume full responsibility.[15]

Market forces do provide some incentives to firms to avoid the direct financial costs of disruption of their operations due to crises and unforeseen events. All private firms are responsible to their shareholders for operational business risks and have to prepare for contingencies and emergencies. However, in general, market incentives are not compelling enough for private actors to provide the appropriate level of security for society as a whole. To survive in a market driven economy, companies need to minimize costs and maximize profits. Keeping reserve stock, maintaining redundant systems, and employing back-up staff all cost money. With pressure to cut costs less resources are available for contingencies and crisis management. Bankruptcy laws and moral hazard further limits the extent to which private actors are willing to extend their emergency preparedness and crisis management capabilities.

The diminishing role of the state in the provision of energy, communications, and financial services in combination with private companies need to minimize costs and maximize profits lead to a situation that we describe as a *gap* between government emergency preparedness measures (which, of course, varies across sectors), and private actors' lack of interest in providing sufficient such measures for society as a whole. This gap is illustrated in figure 1 below.

Figure 1: Minding the Gap



Source: Adapted from Andreas Malm, Klas Lindström, & J.J. Andersson, "Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art" [Resilience in the Financial Sector]. Report. Finansinspektionen 2003.

[14] See, for example, Boot et al 2003.
[15] Armed forces reductions in many countries have further diminished government capability for ensuring societal security, public safety, and emergency management.

The gap between government and private actors' emergency preparedness measures indicates that market incentives are not enough to provide sufficient societal security. Since the market is unlikely to close the gap by itself, the government must "help the market work" by altering the incentive structures to close the gap.[16] While market forces are potent, one must remember that over-reliance on markets is just as dangerous as over-reliance on the powers of direct regulations. In short, markets, by themselves, do not provide adequate incentives for private actors to invest in societal security at warranted levels.

In order to ensure appropriate emergency preparedness for major crises for society as a whole some form of government intervention will be necessary in certain markets. However, government intervention does not necessarily imply massive state-led intervention or government takeover of critical infrastructure. The need for some type of government intervention to ensure adequate levels of societal security and emergency preparedness for society as a whole does not determine how or in which situations the government should intervene.

Closing the Gap

In principle, there are three ways in which the gap in emergency preparedness between public and private actors could be closed. The first alternative is legislative regulation, the second alternative is to use economic policy instruments, and finally, the third alternative is to turn to PPPs. We will discuss each alternative in turn.

Direct Regulation

Knowing the tendency of private actors to under invest in emergency preparedness measures, the government could use its legislative power to close the gap by simply forcing the private sector to adhere to certain minimum standards. The government could, for example, impose direct regulation requiring private actors to adopt certain emergency preparedness features, such as back-up diesel powered generators and separate data- and telecommunication links, for example. Another regulatory option for the government would be to require private utility and service providers to carry insurance against major crises and catastrophic events. Such an insurance requirement would then lead insurance companies to provide incentives for utility operators and service providers to build more robust systems.

The argument for regulation is that it will provide a uniform level of emergency preparedness (assuming that the regulations are followed and enforced) across society as a whole. However, the benefit of regulation must be weighed against its potential costs.[17] A "perfect" government would certainly be able to improve societal security, public safety, and emergency preparedness by imposing the right kind of regulation to counteract negative externalities and moral hazard. In reality, however, it is less clear that governments would be able to do so. All regulators face the problem of imperfect information and must regulate under uncertainty. For example, how will we know that the mandated emergency preparedness measures are set at the "right" level for maximum social welfare?[18] Any form of regulation has distributional consequences with some gaining and some losing. Different interest groups will therefore seek to influence the government to regulate in their favor. Moreover, while regulation may motivate firms to meet the minimum mandated standards, there are no incentives to exceed them. Legislation may also impede innovation in finding new and less costly ways to improve emergency preparedness measures. Finally, the cost of these measures will, undoubtedly, be passed on to the customers/users.

[16] For a similar conclusion, see Orszag 2003.
[17] Laffont and Tirole 1994; Baron 1995; Spiller 1995.
[18] A standard for emergency preparedness suitable for, say, power grid operators could impose an excessively high standard (which would lead to unnecessary costs) or an excessively low standard (which would lead to insufficient protection) for society as a whole.

While careful attention to the design of any regulation may counteract many of the negative aspects of legislation, the potential for making regulatory mistakes is considerable, especially in innovative and rapidly changing sectors such as IT- and financial services.[19] The international dimension must also be considered. Internationalized markets and transnational information and communications networks pose considerable challenges to the autonomy and effectiveness of national governments to regulate domestic problems. Given the problems of imperfect information, distributional consequences, and international markets, it is unlikely that governments will choose regulation as their first choice in ensuring appropriate emergency preparedness across society as a whole. Private firms, in turn, will most likely consider regulation to be the *least* desirable form of market intervention to correct the undersupply of emergency preparedness.

Economic Policy Instruments

Rather than forcing the private sector by law, the government may use economic policy instruments to encourage the private sector to invest in emergency preparedness measures voluntarily. If designed appropriately, economic policy instruments – such as direct government subsidies or tax incentives – could affect firm behavior and improve emergency preparedness. It is likely that different types of incentives will be the first choice for private actors since it would allow them to improve their emergency preparedness measures on their own terms while avoiding both costs and government control.

However, in using economic policy instruments, the government faces a trade-off between inducing the firms to behave in the desired way and offering them some socially costly rewards, rents. In fact, economic policy instruments – such as direct subsidies and tax breaks – will likely be the least appealing alternative for governments. If the monetary incentives are too generous, it will encourage unnecessarily costly improvements and the government will pay for unnecessary security (gold plating). On the other hand, if the economic incentives are too small, the private sector will ignore the offer.[20] In short, the government will spend money (directly or by tax breaks) with little control over either process or outcome.

Public-Private Partnership

Given the problems of ensuring adequate levels of emergency preparedness in society by direct regulation or economic policy instruments, PPPs provide a solution that seems to satisfy both government and private actors. Arguably, PPP is an organizational principle that can successfully address the tension between market forces and non-market forces in the provision of societal security, public safety, and emergency management.

Public-private partnerships have a long history and tradition.[21] There are many definitions of PPPs and a growing literature exists on the subject.[22] In this paper, we adhere to the definition of PPPs as "voluntary cooperation between public and private actors on a common project."

PPPs are rapidly gaining popularity as a form of governance in many areas of society. There are several reasons for this development. Partnerships are seen by both public and private actors as the most effective way to reach their goals. The basis for any partnership is structural cooperation between equal parties in which both sides gain. For the government, PPP provides a mean to engage the private sector in public affairs and

[19] Malm, Softa, Andersson & Lindström 2003b.
[20] Another reason why the private sector may ignore such an offer is that the government often would want to renege on the promises it makes once the firms do what the government wants them to do. If the private sector suspects this, then the economic policy instruments are not credible. Przeworski 2003, p. 101.
[21] Davis 1986.
[22] Stiles and Williams 2000; Pierre 2000; Cars et al 2002; Mörth et al 2004; Sandebring 2004.

to achieve guidelines and standards without having to resort to regulatory means of "command and control." Public-private partnerships are also preferred to direct subsidies or tax incentives since certain control can be maintained. For private actors, PPPs offer a flexible way in which to meet government requirements while avoiding regulation.

However, despite the general consensus on the positive aspects of PPPs, we argue that it may be an unreliable and unpredictable solution to the problem of closing the gap in national emergency preparedness and crisis management in deregulated sectors of the economy. There are several reasons for this argument. It is difficult to achieve tangible results with PPP. The main problem lies in implementation. It is relatively easy for government and private actors in a PPP to agree on the existence of a problem and that something must be done about it. It is, however, much harder to agree on what should be done about it, who should be responsible for implementing it, who should assume legal responsibility for it, and who should bear the costs for the implementing it. To successfully close the gap in the provision of emergency preparedness measures requires clear guidelines and recommendations, consensus among actors, time, and money.

By refraining from imposing regulation and engaging in PPPs, the government pushes the responsibility for implementation and costs on to industry. Industry, in turn, will be reluctant to accept the responsibility and costs without clear guidance and economic compensation. Without clear guidance and money from the government, there is a distinct possibility that private actors simply participate in PPP as a means to deflect attention from insufficient emergency preparedness measures and to avert outright regulation. The preference ordering of the Government and the private sector of alternatives for closing the gap is illustrated in the figure below where, 1, indicates the most favored solution, 2, the second choice solution, and, 3, the least favored solution.

Figure 2: Closing the Gap

Actors	Direct Regulation	Economic Policy Instruments	Public-Private Partnership
Government	2	3	**1**
Private Sector	3	1	**2**

Alternatives

Source: Adapted from Jan Joel Andersson, "Public-Private Partnerships and Emergency Preparedness," paper presented at the conference on National Deregulation and European Reregulation, organized by the Stockholm Centre for Organisational Research, Stockholm, 27 February 2004, p. 8.

In the following sections, we will draw on some of our previous work on PPPs in the financial services and energy sectors to illustrate our argument.[23] In doing so we will compare and contrast our experience from Sweden with the work that has been undertaken by others in Britain and the United States.

[23] Malm, Lindström & Andersson 2003a, b, c; Malm, Softa, Andersson & Lindström 2003.

Cases: Financial services and Energy

Resilience in the Financial Sector

The importance of functioning financial systems cannot be overstated in today's global economy. The attacks on September 11 severely disrupted US financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market, but the risk of major operational disruption is not a new threat to financial systems.[24] Both naturally occurring and man made events over the last 30 years have clearly demonstrated the need for actors in the financial markets to plan for business continuity in case of major crises and disruptions. In comparison to other sectors, the financial market demonstrates a pattern of primarily market driven adjustments to credit-, market-, and operational risks.[25] While events such as the terrorist attacks of September 11 do not change the basic view in most countries that primary responsibility for managing operational disruption lie with the financial markets, the catastrophic nature of such events has led several governments to examine whether there is a need to modify existing policy instruments to mitigate the effects on society of operational disruption in the financial markets due to major crises.[26]

In order to analyze the appropriateness of any policy instruments it is necessary to first identify the key features of the market in which the policy instruments will be applied. Financial markets are characterized by some unique characteristics:

- Financial markets today are global in nature. Economic and technological interdependencies have created markets that exceed the scope of national sovereignty. For example, financial contracts increasingly straddle international borders and transactions often involve numerous jurisdictions. A business deal in London between a US and a UK bank could be carried out over the Amsterdam stock exchange, cleared through Clearnet in Paris, and settled in the Netherlands with payment made via a TARGET transfer.[27] Consequently, few financial market problems can be resolved by unilateral action by a single government and an attempt to assert public powers, which would bear on the single jurisdiction of a country, could in fact lead to more problems than it solves.
- Financial markets are large and complex. These facts suggest that those closest to the markets are likely to be in a better position to understand the impact that a decision in one area might have on others.[28]
- Financial markets are characterized by rapid structural change. A consequence of the rapidly changing structure is that any regulatory or statutory response from public authorities is at risk of becoming quickly outdated.
- Financial markets immediately react to events. In order to parry any market reactions, decisions have to be taken in a flexible manner.

Given the global nature, complexity, and uncertainty that characterize financial markets, British, American, and Swedish public authorities have concluded that although governments have an important role to play, the primary responsibility for dealing with operational disruptions should rest with the actors in the financial markets and the actors

[24] US General Accounting Office, GAO-03-251: Additional actions needed to better prepare critical financial market participants, 2003.
[25] In general terms, credit risk is the risk that a bank's customers will not repay their loans. Market risk is the risk that a bank suffers losses due to changes in exchange rates, interest rates, investment prices etc. Operational risk is the risk of unexpected financial losses, which arises from breaches in internal controls, processing errors, inadequate information systems, fraud, or unforeseen catastrophes.
[26] See for example: UK, Report of the Taskforce on Major Operational Disruption in the Financial System, Do we need new statutory powers?, December 2003.
[27] Even this relatively simple transaction involves interconnected contracts under the laws of a number of different countries.
[28] See for example, McKinsey & Company's Banking & Securities Practice - *Experiences from 9/11 terrorist attacks*, November 2001.

in the financial market have themselves supported this view.[29] In Britain and the United States, governments have concluded that no additional statutory powers are needed, as a consequence of September 11th, to safeguard the functioning of the financial markets in case of major crises.[30] In Sweden, the government has followed the Anglo-Saxon model and has refrained from imposing any new statutory powers to safeguard the functioning of financial markets in case of major crises.[31] However, the lack of new statutory powers does not imply that national governments do nothing. It simply means that other policy instruments have been employed.

The US government has, for example, adopted an Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System. This paper appears to have focused market infrastructures' attention on planning for wide-scale disruption.[32] In September 2003, the Securities and Exchange Commission (SEC) issued a policy statement suggesting that specific "business continuity planning principles" should be applied to certain trading markets.[33] On April 7, 2004, the Securities and Exchange Commission approved rules proposed by NASD and the New York Stock Exchange, which require NASD and NYSE members to develop business continuity plans that establish procedures relating to an emergency or significant business disruption.[34] Similar guidelines and rules have been devised in Britain and are under development in Sweden.[35] Such principles are also being discussed internationally in the G10 Central Bank Governors' Committee on Payment and Settlement Systems (CPSS) and within the European System of Central Banks (ESCB). For example, the CPSS' Core Principles for Systemically Important Payment Systems and the CPSS/IOSCO Recommendations for Securities Settlement Systems both address the importance of business continuity and the need for appropriate contingency arrangements. Furthermore, the principles for capital coverage of operational risks that will be introduced under the new Basel and EU Capital Adequacy Standards has strengthened and highlighted the importance of business continuity within financial firms.[36] The former case is particularly interesting since it ties risk management to annual accounts and thus forces firms to reconcile their accounts taking operational risks into their calculations.

However, in practically every case of direct regulation, individual firms and senior management remains responsible for developing business continuity plans and selecting and estimating those operational risks that will be financially covered, something that will prove to be a challenge for the supervisory role of authorities such as FSA, SEC, and Finansinspektionen.[37]

Although the primary responsibility for managing operational risk remains with the market, recent catastrophic events such as the terrorist attacks of September 11 have

---

[29] UK, Report of the Task Force on Major operational disruptions in the financial system, *Do we need new statutory powers*?, December 2003.
[30] IBID
[31] The Swedish government has not conducted the thorough investigations into the mater that the British and American authorities have.
[32] Pressrelease available at http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/default.htm, accessed on 21st April 21, 2004 4 pm.
[33] Policy statement available at http://www.sec.gov/rules/policy/34-48545.htm, accessed on 21st April 21, 2004 3 pm.
[34] File Nos. SR-NASD-2002-108 and SR NYSE-2002-35.
[35] See for example FSA handbooks on operational risks and business continuity such as the FSA Consultation Paper 142. Finansinspektionen is expected to release guidelines later this year (2004).
[36] Although the details of the accord, to be introduced by 2007 are still being worked out, central banks and banking sectors as a whole have commenced seminars and debates on the details of the accord as well as the impact it will have on banking in the future. Similar impact can be seen in the US Federal Trade Commission's (FTC) proposed regulation that will require financial service companies to protect their networks against "anticipated threats" and generally take measures to protect their information.
[37] For example, the Financial Services Authority (FSA) confirmed in 2003 that it will maintain its non-prescriptive approach to business continuity arrangements by financial firms as outlined in FSA Consultation Paper 142.

led the FSA, SEC, and Finansinspektionen to all elaborate on high level business continuity planning principles for firms critical to the functioning of the financial system in the specific areas of recovery times, and testing of business continuity arrangements and their preparedness for dealing with legal issues on major operational disruptions. This elaboration requires cooperation of market actors. Considering the problems associated with detailed direct regulation to provide appropriate emergency preparedness measures in the financial sector PPPs have emerged as a preferred solution for many governments.

In the financial sector, cooperation between public authorities and the private sector has traditionally been conducted on an informal basis primarily to facilitate the supervisory roles of authorities such as the Financial Services Authority (FSA) in Great Britain, the US Security and Exchange Commission (SEC), and the Swedish Financial Supervisory Authority (Finansinspektionen). Furthermore, in countries with antitrust laws less stringent than those in the US, such as Britain and Sweden, informal cooperation between private market actors on security issues has been highly developed and in some cases well organized for many years.[38] There are several reasons for this. Most important of these is the view among the key actors that security is not a factor to be used for competition purposes.[39] Among actors, recent major crises have also highlighted the need for a more developed cooperation and coordination of emergency preparedness and crisis management. For example, one clear lesson from the events of September 11 was that the "extraordinary levels of cooperation by market participants" helped overcome shortcomings in individual firms' business continuity planning.[40] The established cooperation between private market actors and between public authorities and market actors has, quite naturally, facilitated the development of private-public partnerships on issues related to security and emergency preparedness in the financial sector. Hence, there are several examples of PPPs under development throughout the countries under consideration.

In the US, the Financial and Banking Information Infrastructure Committee (FBIIC) is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership.[41] The FI-ISAC and the National BankNet under the OCC constitutes one form of an information sharing partnership launched as a result of the recent emphasis on homeland security.[42] In the UK, following the events of September 11, the Standing Committee (representatives from the UK's financial authorities: HM Treasury, the Bank of England and the Financial Services Authority) set up a sub-group on resilience and contingency planning to co-ordinate the work being done by the authorities and by other bodies in this area. Recognizing that the primary responsibility for contingency arrangements lies with the private sector, the authorities' aim was to share information and facilitate work to address any overlaps or gaps.[43] Furthermore in Britain and the US, market participants as well as public authorities are considering the establishment of a single organization that would become the focal point for both *ex-ante* preparations for major operational disruptions and *ex-post* responses. Although not developed into a "full-blown" PPP yet, Finansinspektionen in Sweden pushes for increased cooperation between market players and public authorities to improve resilience in the financial sector. At the international

[38] For example through organizations such as "Bankföreningen" and "Försäkringsförbundet" in Sweden.
[39] This trend appears to be shifting in terms of low-level security issues. Increasingly, client and transaction security is used competitively by key actors in financial markets.
[40] Federal Reserve, New York State Banking Department, Office of the comptroller of Currency, Securities and Exchange Commission, *Summary of 'lessons learned' and Implications for Business Continuity*, 13 February 2002.
[41] Done to a large extent in cooperation with the Federal Deposit Insurance Corporation (FDIC)
[42] The Office of the Comptroller of Currency (OCC) ensures "a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States."
[43] The Committee work under a Memorandum of Understanding (Financial Stability: Memorandum of Understanding), towards the common objective of financial stability. As set out in that MoU, there is a tripartite Standing Committee on financial stability, comprising senior representatives of the three authorities. This meets monthly to consider issues relevant to financial stability.

level, we note that much work is also being done in this area including, for example, the development within the EU of a Memorandum of Understanding on high-level principles of co-operation between banking supervisors and central banks in crisis management situations.

In short, work in the US, the UK as well as in Sweden points towards a more cooperative framework for dealing with business continuity in the financial markets, thus supporting our theoretical argument. Our experiences from working with emergency preparedness issues in the financial sector in Sweden also support the predictions of our model.

In Sweden, market actors demonstrate a growing interest in cooperation concerning high-level security issues, i.e. issues beyond the reach of separate financial institutions in terms of the existing risk management policies. In terms of national security issues, market participants want a single point of contact and guidelines. Furthermore, while all the major private actors in the Swedish financial market realize the importance of high levels of emergency preparedness and acknowledge that they have a certain responsibility for providing this preparedness, they resist direct and detailed government regulation, rules, and standards. The main arguments are that:

- Standards would be hard to keep up to date
- The specific circumstances of each infrastructure necessitates a flexibility
- It would be difficult to strike the balance between standards being either to prescriptive, or so vague as not to be worthwhile; and
- The standards would need to be extremely wide reaching to be effective, which would be difficult to achieve.

As an alternative to regulations, rules, and standards, market actors naturally find PPPs attractive and thus promote their development. However, we may already identify several difficulties in this developing PPP, such as:

- The sharing of information
- The supervisory vs. advisory role of the government
- The financing of market infrastructure improvements

On the basis of work in the US, Britain, and our experience from Sweden we may conclude that PPPs are being promoted by governments as a solution to “bridging the Gap” in the provision of emergency preparedness in the financial service sector. However, within the developing PPPs several key issues are outstanding. While the exact list of issues will vary from country to country, let us explore the ones mentioned above a bit further:

- The sharing of information. An effective PPP requires sharing of sensitive information. How can private actors be guaranteed that sensitive information regarding their emergency preparedness does not reach unauthorized users or competitors? In Sweden, for example, the Freedom of Information Act makes it difficult for government agencies to engage in an information sharing PPP with the financial sector.
- The advisory vs. supervisory role of the government. The dual role of the government as both advisor and supervisor makes for an unbalanced partnership.
- The sharing of cost for improving emergency preparedness. Who will foot the bill for agreed-upon emergency preparedness measures?

For PPPs to succeed in the financial service sector, these types of issues must be resolved.

Robustness in the Energy sector

The importance of energy, and in particular electricity, has been underlined by recent major black-outs in North America (Eastern Canada; North Eastern United States) and Europe (Italy; South Eastern England; Southern Sweden-Eastern Denmark). The costs to industry, commerce, and the individual of a failure of supply in electricity are difficult to fully estimate but are measured in billions of dollars of lost output.[44] The social consequences of any failure to supply are potentially even greater.[45] Ensuring the security of energy supply is a public interest consideration of central importance. It is crucial to underpinning economic performance and the quality of life.

The energy sector has recently been liberalized in several countries. When energy market liberalization gathered pace from the late 1980s, energy security still mattered, but seemed initially to need little attention – world fossil fuel markets were slack and there was substantial surplus capacity in the electricity and gas supply industries.[46] However, since the end of the 1990s, attention has focused sharply again on security of supply. Several highly publicized major blackouts (Auckland, Montreal) in combination with increasing international conflicts in important oil-producing regions (The Caspian Sea Region, Central Asia, and The Gulf Region) sparked new interest in energy supply and security issues.[47] Other important stimulants of this renewed interest were California's major power crisis and the "fuel protesters' " crisis in Britain which came close to shutting down the gasoline distribution network.[48] Moreover, the rise of international terrorism has drawn attention to the vulnerability of energy network infrastructures and production facilities.

There are a number of factors that are unique to the energy market, which must be taken into consideration, for instance:

- Electricity is difficult and expensive to store. To meet peak demand, an equivalent amount of generating capacity must exist, and in practice some extra to act as reserve in the event of breakdowns or exceptional levels of demand.
- Some energy markets are geographically circumscribed – for example the UK has relatively few international interconnections for gas and electricity supplies, limiting the ability of actors to respond quickly to a shortage by importing energy from abroad.
- An energy market is characterized by relatively low price elasticizes (meaning that in the short term very high prices might be necessary to balance supply and demand in response to a supply shortage; this effect was seen in the 1970s' oil crises)
- Long lead times and high capital intensity are typical of many energy development projects, which in turn constitute barriers to entry for new actors in an energy market.
- The concentration of world hydrocarbon resources, in particular, in certain countries, often enables some degree of market power to be exercised by those countries.

These are all reasons why, in view of the over-riding importance of energy security, national governments have a responsibility to ensure adequate levels of energy security. However, none of the governments in the US, the UK, and Sweden believe that these potential complications necessarily present an insuperable problem within a market framework. Quite on the contrary, these governments seem to believe that extensive

[44] UK Department of Trade and Industry Cm.5761, White Paper, *Our Energy Future – creating a low carbon economy*, February 2003
[45] Only imagine an extended loss of power during a severe winter in Northern Europe or North America.
[46] Priddle 2002.
[47].See for example Boot et al 2003 and Newlove et al 2003.
[48] See article in San Francisco Chronicle, available at http://www.sfgate.com/cgibin/article.cgi, accessed 6 April 2003.

direct and detailed regulation could hamper the policy objectives of security, efficiency, and environmental sustainability. They refer to several reasons, such as:

- Policies to control consumer costs, protect the environment, tax and subsidize industry, and maintain reliable service all interact. Hence, measures taken to solve one problem may worsen (or ameliorate) another problem: e.g., lowering oil use alone may increase global oil dependence by reducing oil prices. A clear and ongoing example, reflecting this complex relationship, is the debate on long-term contracts on gas supply within the EU.[49] First the Commission wanted to prohibit these contracts. Now the commission is expected to conclude that long-term contracts are indispensable for security of supply and that we therefore need a minimum percentage of long-term contracts in the directive on security of supply for gas. This confusion has lasted now for almost two years and as such has reduced the important predictability in the market.[50]
- Both within and across nations, consumers, industry, governments, and international organizations make interrelated choices. The fragmentation of power among localities, states, and the federal government, fragmentation of jurisdiction among agencies of the federal government, and perhaps even the constitutional legislative-administrative separation make it difficult to devise and implement integrated solutions to large-scale problems.
- Infrastructure resiliency improvements need not take a full generation, though substantial restructuring would. Significant reductions of oil dependence would take decades preceded by substantial public investments; costs accrue early, benefits later. In many cases the political system seems unable to address these large, long-term problems. Physical plants of any domestic energy infrastructure will only turn over in decades and there is a low public-political perception of need for change. Election cycles, changes of administration, and voter behavior do not reward continuity and long-term investment.
- Vulnerabilities vary across energy types. Event consequences may be local, regional, national, or international and therefore blur divisions of responsibilities.

Experience from regulatory initiatives clearly illustrates the intrinsic difficulties in direct regulation regardless of them being carried out on a national or supranational level. The EC directive and the debate on long contracts as well as the US experiences of price caps, with adverse consequences in California, clearly demonstrates these difficulties.[51]

In general therefore, governments look to markets, with appropriate economic incentive structures, to ensure that security of supply is maintained. The basic problem here centers on the issue of social costs not being internalized to the energy market (e.g. security, environmental costs of oil dependence, etc.). To the market, monetary costs of remedial measures is known better than intangible future benefits and in some cases such as industry, different customers may value security of supply differently. In broad terms, the costs of a failure to supply electricity may not be felt by the electricity supplier who fails to acquire the power; in the absence of appropriate arrangements and incentives, it may be spread over the industry more widely or borne by consumers. This could encourage some companies to try to free-ride, which could cause the industry collectively to take inadequate security of supply precautions. Indeed, there are a number of potential obstacles, which may make it difficult for markets to determine and deliver the appropriate level of security. Some of these have frequently been discussed in all of the three countries under consideration and they normally include obstacles such as:

[49] Long term contracts have traditionally provided the necessary incentive for new energy generation in many European Countries. However, the contracts have added inertia to the pricing mechanism.
[50] Boot et al. 2003
[51] Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003. The Economist, *How to keep the lights on*, August 23rd 2003, p 12.

- Economies of scale and natural monopoly effects
- Network effects (when a group of customers take their supply from a single pipe or wire)
- Transaction costs
- The fact that full competition in supply has not yet developed.

The impact of deregulation has sometimes been to provide no economic incentives for investments in restructuring for robustness or in taking precautions against attack.[52] In recognition of the obstacles mentioned, most Governments therefore wish to remove any potential barriers to the achievement of energy security; and to monitor developments in energy markets to determine whether in any way security is being put at risk.[53] Although it may be necessary in specific cases for regulators to set security standards or to take steps to remedy any inability of energy markets to provide satisfactory levels of security, experience point towards doing this through an internalization process. However, this approach has already demonstrated some weaknesses, due to the specific character of the energy market.

Differing strategies to liberalize home markets have resulted in a wide range of national market structures within not only the countries under consideration, but indeed the whole of Europe. The overall trend is that dominant and vertically integrated companies from relatively sheltered home markets expand abroad whilst companies in competitive markets merge at home. The latest developments (for instance the Eon/Ruhrgas merger) suggest an intensification of this trend: the dominant electricity companies are further increasing their level of vertical integration by taking over gas businesses.[54]

If energy markets proceed along this path, they run the risk of ultimately being characterized by a tight oligopolistic structure with large companies not competing within each others home markets and a high level of vertical integration.[55] In the case of EU, this might even be worse if some countries aim to stimulate this tendency, as seems to be the case nowadays.[56] In this context we need to take into consideration the specific characteristics of the electricity sector and electricity as a product, which make market power easy to abuse, hard to detect, and difficult to prove. Studies of the Californian energy crisis show that the risks in terms of price increases and reduced levels of security are significant.[57] Furthermore, today's competition authorities do not aim to engineer competition in markets, merely to companies from achieving dominant positions judging mergers and acquisitions. The tricky combination of a trend towards a high level of concentration in the electricity sector, the mentioned specific product characteristics, the inherent limitations of competition policy and the possibility of implicit objectives of some states are reasons for worrying about the levels of security within the energy market. Hence, although the governments under consideration believe that the protection of energy vulnerabilities will largely be accomplished through the private sector, there is a strong national coordinating and analytical role to be filled by governments.[58]

[52] See, for example, Karas 2003.
[53] "Though protecting our energy vulnerabilities will largely be accomplished through the private sector, there is a strong national coordinating and analytical role to be filled by the federal government." US FY 2004 Congressional budget.
[54] NERA 2003.
[55] Boot et al. 2003.
[56] In the US case, higher level of concentration is actually suggested as a potential solution to recent power failures. See for example the Economist, *Bring me your powerless masses*, August 23rd, 2003, p 20
[57] US General Accounting Office, report from period of May 2000 – February 2001
[58] See for example US FY 2004 Congressional budget, UK Department of Trade and Industry Cm.5761, White Paper, *Our Energy Future – creating a low carbon economy*, February 2003.

In the energy sector therefore, many governments consider public-private partnerships necessary to get around the difficulties imposed by private sector ownership of critical infrastructures.[59] The motivation for this is multifold:

- To create an information sharing framework for the public and private sectors to exchange information about threats and vulnerabilities affecting the nation's critical infrastructure.
- To define the appropriate level of security necessary to protect critical infrastructures, define the levels of security that markets will achieve, and define the role the government should play to close the gap between desired and market-achievable security.
- To review existing legislation, government capabilities, and private sector security requirements, at the federal, state, and local levels to ensure that (a) resources are adequate to support existing policy requirements, and (b) existing policy requirements contribute to improving economic security.

Governments, like the US, have even gone so far as to consider implementing a regulatory or legislative exemption to anti-trust rules that limit possibilities for PPPs, in order to permit improved security without adversely impacting consumers.[60] However, monitoring and analyzing present security levels is one thing, attempting to establish incentives through PPPs another, which of course, once again raises questions of how the public and private sectors should share the costs of any improving and correcting measures.[61]

To believe that only direct regulation raises questions on how the public and the private sectors should share the costs of achieving adequate levels of security is a pitfall. To a certain degree Governments' willingness to engage in a PPP with the private sector may open a window of opportunity for cost shifting. We are, in general, concerned about the potential for consumers and markets to place reliance on Government "rescue packages" in the event of perceived threats to security. If Governments hold out the prospect of intervention whenever "the going gets tough", markets may never be able to provide effective risk management. The interesting question then becomes whether PPPs, considered necessary for correcting imperfect information in the market and monitoring of risks and levels of security in general, in fact opens a window for government bailouts? Indeed, our experience from working with the energy market in Sweden points towards this dilemma.[62] In the face of the 'massive investment in energy production and transportation infrastructure' that will be needed over the coming decade it is naturally tempting for energy markets to shift costs to the Government.[63]

Indeed, there are further difficulties that complicate maters when trying to establish PPPs as a solution to the problem of the gap in the energy market. Let us just mention some of them:

- *The concrete nature of work on these issues*. There are underlying conflicts of interest between Politics/Markets and Micro-power and Mega-power, conflicts that will have to be resolved. Solutions to the security of supply problem may very well lie in market frameworks not promoted by incumbent market players, which naturally will lobby

[59] See for example section 1(b) of the October 16, 2001 Executive Order on Critical Infrastructure Protection (EO 13231) and UK Department of Trade and Industry Cm.5761, White Paper, *Our Energy Future – creating a low carbon economy*, February 2003 and work performed by "Nationella Styrgruppen för privat-offentlig samverkan" in Sweden

[60] Partnership for Critical Infrastructure Security, *Draft paper for critical infrastructure assurance*, 3 April 2002, available at http://www.pcis.org/index.cfm accessed April 21, 2004, 4 pm.

[61] Karas 2003.

[62] Malm et al 2003 c.

[63] OECD 2000.

against such solutions. Hence the concrete nature of work on these issues within a PPP may not be easy to outline.

- *Responsibilities*. Within a PPP issues of responsibilities may often be blurred in the face of consumers. Collective responsibility may often lead to no-one taking responsibility for the issues at stake.

Paradoxically thus, the transition to competitive markets seems to necessitate a greater, albeit carefully circumscribed, role for a regulator. This realization among governments has increased the interest in Public-private partnerships as a way forward and work in the US, the UK as well as in Sweden points towards a more cooperative framework for dealing with security issues in the energy markets, thus supporting our theoretical argument. However, experience demonstrates that Public-private partnerships have their own problems and difficulties that must be resolved to realize the long sought for security of supply in energy markets.

Conclusion

PPPs are rapidly gaining popularity as a form of governance in many areas of society. There are several reasons for this development. Partnerships are seen by both public and private actors as the most effective way to reach their goals. The basis for any successful partnership is structural cooperation between equal parties in which both sides gain. For the government, PPPs provides a means to engage the private sector in public affairs and to achieve guidelines and standards without having to resort to regulatory means of "command and control." PPPs are also preferred to direct subsidies or tax incentives since certain control can be maintained. For private actors, PPPs offer a flexible way in which to meet government requirements while avoiding regulation.

However, despite the general consensus on the positive aspects of PPPs, we have argued in this paper that such partnerships may be an unreliable and unpredictable solution to the problem of closing the gap when it comes to issues of national emergency preparedness and crisis management in deregulated sectors of the economy. Our conclusion is based on theoretical as well as empirical grounds. First, it is difficult to achieve tangible results with PPPs. The main problem lies in implementation. It is relatively easy for a government and private actors in a PPPs to agree that there is a problem and that something must be done to resolve it. It is much harder, however, to agree on what should be done, who should be responsible for doing it, and who should assume legal responsibility as well as the financial costs involved in implementing new measures. In order to successfully close the gap in the provision of emergency preparedness measures, clear guidelines and recommendations, consensus among actors, time, and money are necessary. In other words, governments and private actors must reconcile responsibilities and costs in the provision of societal security.

References

Akintoye, Akintola, Matthias Beck and Cliff Hardcastle, eds. 2003. *Public-Private Partnerships: Managing Risks and Opportunities*. Blackwell.

Andersson, Jan Joel. 2000. *States, markets and national autonomy*. Stockholm: ÖCB.

Andersson, Jan Joel. 2004. "Public-Private Partnerships and Emergency Preparedness," paper presented at the conference on National deregulation and European reregulation, organized by Stockholm Centre for Organisational Research, Stockholm, 27 February 2004.

Barnekov, Timothy, Robin Boyle, and Daniel Rich. 1989. *Privatism and Urban Policy in Britain and the United States*. New York: Oxford University Press.

Baron, David T. 1995. The Economics and Politics of Regulation: Perspectives, Agenda, and Approaches. In *Modern Political Economy,* edited by Jeffrey S. Banks and Eric A. Hanushek. Cambridge: Cambridge University Press.

Boot, P., et al. 2003. *European Energy Markets: Challenges for policy and research*. The Hague, the Netherlands: Ministry of Economic Affairs. .

Bozeman, Barry. 1987. All Organizations are Public: Bridging Public and Private Organizational Theories. Proquest Info & Learning.

Cerny, Philip J. 1995. Globalization and the Changing Logic of Collective Action. *International Organization* Vol 49:595-625.

Davis, P. 1986. *Public Private Partnerships – Improving Urban Life.* Academy of Political Sciences, USA.

Greenwald, Bruce C., and Joseph E. Stiglitz. 1986. Externaltities in Economies with Imperfect Information and Incomplete Markets. *Quarterly Journal of Economics.* Vol 101: 229-264.

Héretier, Adrienne. 2001. Market integration and social cohesion: the politics of public services in European integration. *Journal of European Public Policy.* Vol. 8(5): 825-852.

Héretier, Adrienne. 2002. Public-interest services revisited. *Journal of European Public Policy.* Vol 9(6): 995-1019.

Karas, Thomas H. 2003. 'Energy and National Security. SANDIA REPORT, SAND2003-3287, Unlimited Release. (September).

Knill, Christoph, and Dirk Lhemkuhl. 2002. Private Actors and the State: Internationalization and Changing Patterns of Governance. *Governance: An International Journal of Policy, Administration, and Institutions.* Vol. 15(1): 41-63.

Kunreuther, Howard, and Geoffrey Heal. 2003. Interdependent Security. *Journal of Risk and Uncertainty* Vol. 26: 231-249 (March/May)

Kunreuther, Howard, Geoffrey Heal, and Peter Orszag. 2002. Interdependent Security: Implications for Homeland Security Policy and Other Areas. Policy Bries #108. Brookings Institution, October.

Waltzer, N. and B. Jacobs, eds. *Public-Private Partnerships for Local Economic Development*. Praeger.

Lafont, Jean-Jacques and Jean Tirole. 1994. *A Theory of Incentives in Procurement and Regulation*. Cambridge, M.A.: MIT Press.

Malm, Andreas, Klas Lindström och Jan Joel Andersson. 2003a. Kritiska beroendeförhållanden i den nationella IT-infrastrukturen. Opublicerad rapport. KBM

Malm, Andreas, Klas Lindström och Jan Joel Andersson. 2003b. Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art [Resilience in the Financial Sector]. Report. Finansinspektionen.

Malm, Andreas, Klas Lindström, Jacob Henricson, Jan Softa and Jan Joel Andersson. 2003c. *Hel Projektet, Dokumentation från samverkansseminarium 23-24 oktober 2003*. Unpublished manuscript. Energimyndigheten

Malm, Andreas, Jan Softa, Jan Joel Andersson och Klas Lindström. 2003. *IT och sårbarhet - kritiska beroendeförhållanden i den nationella IT-infrastrukturen*. Temaserie 2003:5. Stockholm: KBM.

NERA, 2003. *Consolidation in the EU electricity sector*. London.

Newbury, David M. 1990. Missing Markets: Consequences and Remedies. In *The Economics of Missing Markets, Information and Games.* Oxford: Clarendon Press.

Newlove, Lindy, Eric Stern, and Lina Svedin. 2003. *Auckland Unplugged: Coping with Critical Infrastructure Failure*. Baltimore: Lexington Books.

O'Hanlon, Michael, et al. *Protecting the American Homeland. One Year On.* Washington, D.C.: Brookings Institution Press.

OECD. 2000. *World Energy Outlook 2000*. Paris: OECD.

Orszag, Peter R. 2003. Testimony before the National Commission of Terrorist Attacks Upon the United States, November 19, 2003.

Osborne, Stephen P. 2000. *Public-Private Partnerships : Theory and Practice in International Perspective*. Routledge.

Priddle, R. 2002. Security of Supply in Liberalized Electricity Markets, Eurelectric Annual Convention, Leipzig, 24-25 June.

Przeworski, Adam. 2003. *States and Markets*. Cambridge: Cambridge University Press.

Shuttleworth et al. 2003. Security of energy supply, Energy Regulation Brief. NERA, produced for Departement of Trade and Industry.

Spiller, Pablo T. 1995. Regulatory Commitments and Utilities' Privatization: Implications for Future Comparative Research. In *Modern Political Economy,* edited by Jeffrey S. Banks and Eric A. Hanushek. Cambridge: Cambridge University Press.

Stigler, George. 1975. *The Citizen and the State. Essays on Regulation.* Chicago: University of Chicago Press.

Stiglitz, Joseph E. 1994. *Whither Socialism?* Cambridge, M.A.: MIT Press.

Vaillancourt Rosenau, Pauline, ed. *Public-Private Policy Partnerships*. Cambridge, M.A.: MIT Press.

USA: "*Federalism / Regulatory Processes for CIP in the US compared to Europe"*

Ms Anne Dailey
George Mason University, USA

Federalism – Getting to the Roots

- John Locke, ca. 1683
  - "Men being, as has been said, by nature, all free, equal and independent, no one can be put out of his estate, and subjected to the political power of another, without his own consent. The only way by which anyone divests himself of his natural liberty, and puts on the bonds of civil society is by agreeing with other men to join and unite in a community, *for their comfortable, safe, and peaceable living one amongst another, in a secure enjoyment of their properties, and a greater security against any that are not of it."*

    --Two Treatises of Government, Ch. 8

What is federalism in the US?

We the people of the United States, in order to form a more perfect union, *establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare*, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America.

- In practice…
  - The federal government may only perform and execute those tasks delineated to it by the US Constitution – and no others.
    - (Although, through various clauses in the Constitution, this has been liberally construed.)
  - All other tasks are left to the states.
  - Each state is a sovereign entity, so it may create and execute laws within its borders.
  - Example:
    - Treaties are negotiated only by federal government, because the Constitution says it may do so (and that states may not).
    - Celebration of marriage (and the rules surrounding it) are left to the states.

What federalism issues arise out of Homeland Security?

- National regulators of critical infrastructures (FCC, FERC);
- State regulators of critical infrastructures (VA SCC);
- Federal agencies with an interest in CIP (DHS, FBI, Department of Energy, Transportation);
- State and local entities (police, emergency response, emergency planning)

…each level has an interest and (arguably) jurisdiction over critical infrastructures. How can they work together to promote CIP without overstepping boundaries?

What federalism issues arise out of Homeland Security?

- Who is really in charge?
- Overlap of (often redundant) information requests
- How do you get every level of jurisdiction (federal, state, local) to offer the same level of security? And, do they have to?
- Who pays

The EU and the US – A Federalist Comparison

- Striking differences between the EU and the US development
  - US
    - 13 original colonies with (essentially) one sovereign → 13 states with one primary sovereign
    - Additional states added at nascent levels of their development – separate culture, government, identity had not yet developed
    - Always understood that being a part of the US was being part of a single, federal entity – "Provide for the common defense"
  - EU
    - Various empires notwithstanding, modern Europe is many different, independent nations (with more developing)
    - EU was developed as an economic entity – it's not part of the original concept to "Provide for the common defense."

The EU and the US – A Regulatory Comparison

- US
  - Initial regulatory schemes developed as a result of the industrial revolution, with more since the 1930s
  - Almost all Critical Infrastructures have an element of their system (if not the entire system) that is based in the private sector
    - Thus, regulation (whether through direct or indirect means) is the primary way for the government to affect industry policy
  - Public-private partnership an essential element of government and industry relations
    - But hard to always know what this means
- EU
  - Until recently, most critical infrastructures were owned and operated by the governments (and still many are)
  - When owner and regulator are one in the same, MUCH easier to impose change

Back to where we started…

- *Salus populi suprema lex* [the people's safety is the supreme law], is certainly so just and fundamental a rule that he, who sincerely follows it, cannot dangerously err.

-- Two Treatises of Government, Ch. 13

USA: "*National Capital Region Modern-day Threat Planning Process*"

Ms Anne Dailey
George Mason University, USA

Regional vs. Local Threat Response: A 9/11 Case Study

- Twin Towers
  - Physically located in New York, NY
  - Owned and operated by the New York Port Authority
  - Responsibility fairly clear, right?
- Pentagon
  - Physically located in Arlington, VA
  - Owned and operated by the Federal Government
  - Housed operations for all four branches of government?
  - Which body is in charge of first responding? Of the clean-up? Of the rebuild?

What are some of the issues involved in regional threat planning?

- Sharing of assets across jurisdictional boundaries
- Sharing of information across jurisdictional boundaries
- Uniformity of services, training and security level for all areas – not just those who live in one state or another

National Capital Region – A Snapshot

- Includes Maryland, Virginia, and the District of Columbia (a federal district, not part of a state)
- Houses all three branches of the US government (executive, legislative, and judicial)
- 17 local government jurisdictions (counties, cities)
- 35 separate law enforcement bodies
- 2,100 non-profit entities (associations, other charities)
- Almost innumerable private sector interests
- And, most importantly, almost 4 million Americans

National Capital Region – Urban Area Security Initiative (UASI)

Overarching Objectives

- Enhance the capability and capacity of the National Capital Region to reduce vulnerability, minimize damage, and increase resiliency.
- Ensure vulnerability assessment processes are coordinated and appropriately integrated so that preparedness activities and planning mechanisms are consistent, non-duplicative, efficient and effective.
- Develop a sustainable, cost-feasible process for conducting infrastructure vulnerability assessments over time.

GMU Project Overview

- Act as the academic coordinator and assist the NCR Senior Policy Group (SPG) in assessing critical infrastructure practices and procedures in the National Capital Region
- Evaluate current vulnerability assessments and develop best practice process framework for conducting vulnerability assessments
- Work collaboratively with industry, government, and academia

Principal Activities

- Hurricane Isabel Study
- ***Phase 1: Evaluate publicly available recommended infrastructure vulnerability assessments procedures, processes, and tools***
- ***Phase 2: Conduct field work to obtain vulnerability assessment procedures, processes, and tools in use by government and industry***
- Phase 3: Capture best practice processes for vulnerability assessment procedures, processes, and tools
- Phase 4: Build a framework to ensure sustainability of infrastructure vulnerability assessments in the future
- Phase 5: Develop best business practices and policy issues/recommendations to implement the framework
- Phase 6: Develop recommendations for response and mitigation actions from the perspectives of public and private sectors

Critical Infrastructure Sectors to be Evaluated

- Banking and Finance
- Emergency Services
- Energy
- Health Services
- Postal and Shipping
- Telecommunications
- Transportation (to incorporate Hazardous Materials and Chemicals as related)
- Water (to incorporate Hazardous Materials and Chemicals as related)
- Analyze sectors to ensure alignment with National objectives:
  - *security*
  - *economic security*
  - *public health and safety*
  - *public trust and confidence*

Outreach: Framework – Tiered Approach

- Community of Practice
  - Infrastructure Owner-Operators
    - Individuals involved in the Community Research Associates effort, the Hurricane Isabel 45-Day Mitigation Study and other Regional Service Providers
- Community of Interest
  - Related trade and professional associations, academicians, sectoral actors, and national/regional coordinating bodies
- Policy Community
  - Business and government stakeholders

Outreach: Potential Pitfalls

- Many companies/organizations have already been approached with requests for information
  - Mitigate through cautious/strategic engagement and utilization of personal relationships
- Confidentiality concerns
  - Mitigate through NDAs, use of Virginia Code to protect information, CII Program at DHS
- Obtaining the right participation/avoiding insufficient/irrelevant information
- Unforeseen political consequences

Academic Partners

- **George Mason University** – Dr. Christopher Hill, Vice Provost for Research with representatives from the Schools of Public Policy, Law, Nursing, Information Technology and Engineering and Institute for Conflict Resolution
- **Virginia Tech** – Dr. Frederick Krimgold, Co-Director, World Institute for Disaster Risk Management
- **University of Maryland** – Dr. Gregory Baecher, Chairman, Department of Civil Engineering
- **University of Virginia** – Dr. Gregory B. Saathoff, M.D., Executive Director of the Critical Incidents Analysis Group
- **James Madison University** – Dr. George Baker, Department of Integrated Science and Technology
- **Howard University –** Dr. Kathleen Kaplan, Department of Systems and Computer Science

Activities to Date

- July – October 2003: Team building, convened team meetings
- December 2003: Convened Information Sharing Task Force meeting

Activities to Date – cont.

- October – November 2003: Conducted assessment of Hurricane Isabel's impact

- January – March 2004: Inaugurated Project Coordination Team
  - Conducted review of VA processes
  - Began development of Flexible Data Model
  - Developed Outreach Strategy
  - Solidified Project Management structure

Hurricane Isabel – September 18, 2003

- Major storm hit the East Coast of the US – called a "100-year" storm
- Affected major systems for several days:
  - Electricity
    - 4.85 million people without power (Maryland, the District, Virginia, and North Carolina)
  - Telecommunications
  - Transportation
  - Water
- Provided another "case study" for regional threat planning

Hurricane Isabel – Planning Stages

- Virginia regulator (SCC) requires electric utilities to provide disaster relief plans on yearly basis
  - Plans include such information as restoration priorities, contingency plans, and communications plans
- Specific planning began on Monday, September 14th
  - SCC met with electric utilities to discuss disaster plans; prepared to act as communications link between utilities and VA Department of Emergency Management
  - Localities (counties, cities) set up Emergency Operation Centers, and planned to have utility representatives either present, or available via telephone
  - Conference phone bridge for key NCR personnel tested
  - Utilities solicited help from workers in other states, so clean-up could begin as soon as the storm was over

Hurricane Isabel – The Aftermath

- Initial Response
  - Utilities were slow to act when power lines went down – primarily for safety reasons
- After the Storm
  - Utility repair priorities were not always aligned with those of emergency personnel – repairing a system that the state thought was critical was not always first on the utilities' list
  - So many people were without power, for so long, that the interdependencies escalated
  - Trouble with communications
    - Between the utility and the state
    - Between the utility and localities
    - Between the utility and the public

Hurricane Isabel – Lessons Learned

- Preparation and Planning
  - Government didn't include privately owned critical infrastructures in their planning
  - Redundancies weren't sufficient – back-up generation only lasted for hours, not days
  - Alternative forms of public were not established (i.e. using radio instead of television, print media instead of the Internet.)
- Initial Response
  - No central mechanism for coordinating triage between sectors
  - Coordination between state and local government, and the privately-owned utilities was strained
  - Consumer problems: lack of information, and the information given was inaccurate
- Infrastructure Interdependencies
  - Loss of electric power affected almost every critical sector: water treatment plants shut down, traffic lights were down, cellular towers experienced intermittent service disruption. These were the immediate, direct consequences of power loss.
  - The longer a service was out, the further the interdependencies cascaded. For example, hospitals had to consider moving patients because the hospitals could not clean their dirtied bed linens. The linens could not be cleaned because the laundry facilities had no water. And lack of water was due to lack of power at a pumping station.
- Recommended Remediation
  - The most prevalent suggestion going forward from Isabel, voiced by representatives of almost every sector, is centralization of emergency coordination on the local and state level. The communications challenges that each sector faced during the hurricane could have been addressed if representatives from each sector had been working together in a central office. The EOC (Emergency Operations Center) concept touches this, but should be developed further to include industry as well as government.

Conclusions

- In order to have a robust regional system for emergency response, all jurisdictions must work together – cannot have "free riders"
- Traditional, vertical organization of response (with the state at the top) will have to be traded for a newer, more horizontal model; efficiency over hierarchy
- Lines of communication must be open
  - Between jurisdictions
  - Between critical sectors
  - Between sectors and the government
  - Between sectors, the government, and the public

Norway: *"The Shift of Responsibilities within Government and Society"*

Mr Stein Henriksen
Norwegian Directorate for Civil Protection and Emergency Planning, Norway

What I am about to say, may be obvious to some of you; if so, I apologise in advance. However, it is my distinct impression that some aspects of what follows have yet to sink in, certainly within government circles. I am going to say something about major societal trends, their impact on our security, and our attempts to adapt to them.

Our societies are now changing rapidly and probably in a more fundamental way than has been seen since the ascendancy of the nation state after the Peace of Westphalia and the political, economic, industrial, and scientific revolutions that followed. The Westphalian System established the nation state as the dominant level of integration of society, subjugating, but not removing, previous local, regional, or confessional political levels of organisation. This system has lasted until our own time and dominates international law and international political institutions, with a few exceptions, notably the European Union as an evolving supernational entity.

However, the new paradigm of Globalisation is now upon us. The conceptual breakthrough of this paradigm is recent. The concept of globalisation as such is however not new. It started with the European expansion from the 16th century onwards, then taking the form of "Europeanisation", later to some extent continuing as "Americanisation" or "Multinationalisation". Phenomena such as multinational corporations and multinational political organisations are also well known. In some cases the links between such organisations and the nation state are tenuous. The most radically globalised arena of all is probably the Internet, which belongs to and is controlled by no nation.

This development predictably creates new arenas for conflict and new security issues. Globalisation has today caused societies that do not share the same values to face each other more acutely than ever before. As a consequence, a new, violent struggle for pre-eminence on the global arena has been brought up, notably by Islamic fundamentalism in the shape of Al Qaeda and successor organisations. The composition of this organisation is unusual in not being national, and the aims are not national. This organisation wants to take over the world, violently if necessary, and impose its values on it. It does not totally reject globalisation but takes advantage of its means. Al Qaeda as a highly connected global terrorist network uses the means of globalisation not to fight globalisation itself but Western values, such as human rights, liberal democracy, market economy, open, pluralistic societies. It will therefore potentially attack everything that

gets in their way. This threat represents a global-scale security challenge, which ultimately cannot be addressed by any single nation state, only by global organisation.

There are now many global trends that in various ways may challenge the security of our societies, even without external threats like Al Qaeda. Most of the challenges we face are internal to the dynamics our own societies. I have mentioned the emergence of the Internet, which while being global makes huge amounts of information available to the determined individual. This will empower the individual, both for respectable political purposes, but also potentially for creating mischief. In more general terms, the nation state is loosing some of the control it had over its citizens, and for some of those citizens the temptations that this entails will be too great. Rapidly changing societies will erode some of their social capital as institutions fail to keep pace and develop. Delinquency and anomic behaviour is a familiar result. The Internet is a new and powerful tool for the delinquent. The aging of populations, shifting patterns of distribution of income, the permanent and rapid development of knowledge, and other general developments, add to the picture.

One of the most significant security-related global trends, however, is probably the deregulation and to a considerable extent the privatisation of what used to be called public utilities, such as electric power, telecommunications, water supply, and railways. To varying extents these are being removed from direct governmental control, with the implication that they have to be self-financing, i.e. the taxman no longer finances them, and they have to make a profit. Almost invariably, this has led to a security challenge. As public utilities, these were required to be nearly 100% reliable and available. This is not economically viable in the market economy, but the requirements are still there and, if anything, have increased in significance. Old security measures are allowed to wither. Systems that previously had wide safety margins are now operating on the edge of their capacities, as funds for investments and maintenance have dried up. This was partially an intended result of deregulation, as this came about to prune over-capitalised systems. The net result, however, is that there is now little margin for error. There is no margin at all to handle extraordinary situations or crises and there are no mechanisms to make funds available for building such margins. Public utilities have thus become critical infrastructures.

———

From an organisational point of view, we are observing the hesitant beginnings of adaptive change. These organisational adaptions do, not surprisingly, differ from nation state to nation state and also have repercussions on the international arena.

Within nations one may observe:

- Increased co-operation and exchange of information between the key ministries: Ministry of Foreign Affairs, Ministry of Defence, Ministry of the Interior, and Ministry of Justice. In the past, these ministries have often led their own lives. They still do, but to a lesser extent.
- Increased intelligence co-ordination, often bridging a constitutional chasm between exterior intelligence and internal security and counterintelligence. Interpretation, presentation, and perception of intelligence and the relations between the intelligence community and the users of intelligence have probably improved somewhat in the present situation, but remain a major issue.
- A certain approximation and adjustment between some of the responsibilities of the Ministry of Foreign Affairs and the Ministry of Defence, occasioned by the internationalisation and militarisation of counter terrorism (“International War on Terrorism”). In some cases, this visibly leads to “turf wars” between ministries, particularly were the seeds of this already exist. Notably, the “International War on Terrorism” is at least as expensive as any military situation that preceded it, and thus might leave less funding for other security measures.

- Given that the treat of terrorism has increased, and given that most governments will prefer to legally label terrorism as criminal activity rather than as a form of warfare, the responsibility for the national and territorial aspects of security is drifting towards the Ministry of the Interior and/or the Ministry of Justice and the conventional police structures. In some cases, this movement is gradual and not the result of a deliberate strategy or learning process. Unfortunately, this tends to lead to underfunding and inadequate measures as the ministry tries to "make do" within existing structures and budgets. In other cases, notably, the USA and Canada, this has led to the creation of what are effectively powerful ministries of internal security. Both nations have federal type organisations, and this to some extent entails the creation of structures that did not previously exist at the national level.
- The responsibilities for the security of critical infrastructures have apparently and to a significant extent devolved from government to parastatal or private actors. This is usually an unintended result of deregulation. A major problem is that government, generally through ignorance, has almost invariably failed to inform the new owners that they have such responsibilities, what the nature of these responsibilities are, and what the legal and financial implications are. This is echoed in the deregulating legislation, where security concerns tend to be absent. As a result, security against incidents that are out of the ordinary is not funded, and at best rests on a legacy of security measures from a by-gone age. In the Norwegian case, important power supply installations remain heavily fortified because of this legacy. Belatedly, governments are now trying to force security legislation onto infrastructure operators. Predictably, the reception is at best lukewarm. It is easily argued that this was not part of the original deal and will jeopardise profitability.

Between nations one may observe:

- That the security challenges that are emerging are too great to be managed by any single nation alone.
- That international security measures and organisations developed to manage or fight conflicts between nation states are sometimes poorly adapted to managing or fighting resourceful non-state, asymmetric actors that have a global vision. NATO is not an organisation with either a global vision or a global mission, neither is the EU. The only organisation currently available with that kind of scope is the UN, but the UN has not been equipped by its members to handle this.
- The emergence of ad hoc "coalitions" under the leadership of the USA in order to handle the military aspects of the problem and which are limited in scope and time. This is not a lasting solution. Eventually, even the most enthusiastic coalition partner will tire of being regarded as a component part of a "tool box". This became very obvious in the latest conflict, the war on Iraq, where several European countries refrained from supporting a war that was initiated by unilateral decision and was additionally perceived to violate international law.
- There is increasing exchange among nations about generalised and specific security challenges (this kind of workshop is an example), but this exchange is to some degree hampered by the residual need of the nation state to filter knowledge about its own vulnerabilities.

In summary some of the more important points:

- We are in the middle of the most radical societal change that has happened for centuries, including the key factors of globalisation and deregulation, both reducing the power of the nation state
- Security has become global and too big for the nation state, however there are no adequate global solutions
- Military defence forces have become expeditionary forces in support of foreign policy

- Within the nation state, responsibility for national security is moving towards the justice and police structures
- Significant security concerns are being privatised
- Communication of changing responsibilities and allocation of funding are both inadequate and untimely

On a positive note, many previous conflict arenas concerning the proper levels of integration of our societies, such as local vs. central, nation vs. nation, religious and ideological conflicts, while remaining, are now increasingly being regulated in peaceful and co-operative institutions, and are no longer the serious security concerns that they were.

Sweden: "*Risk Finance"*

Mr Per Åkenes
Aakenes Advisory Services, Sweden

Risk management is about the future, uncertainty, and how we manage uncertainty. Risk management consists of

- Risk identity
- Risk assessment
- Risk treatment
- Risk financing
- Risk audit

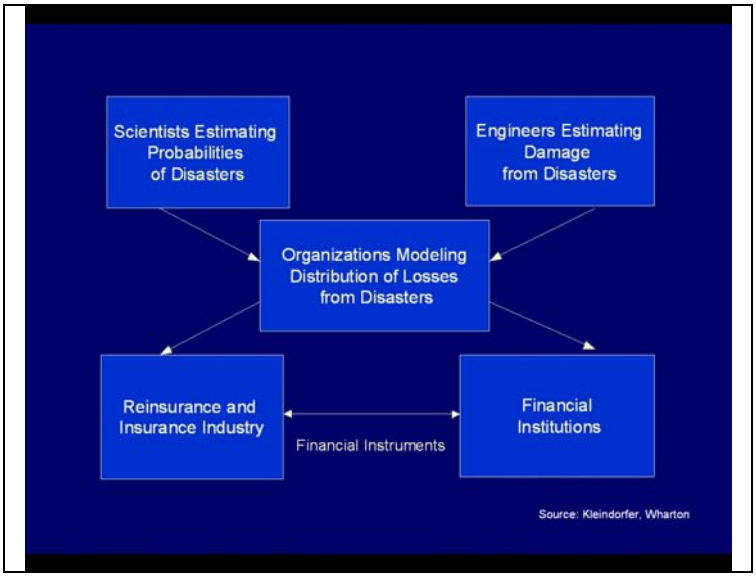
The focus of this presentation is on insurance and risk financing.

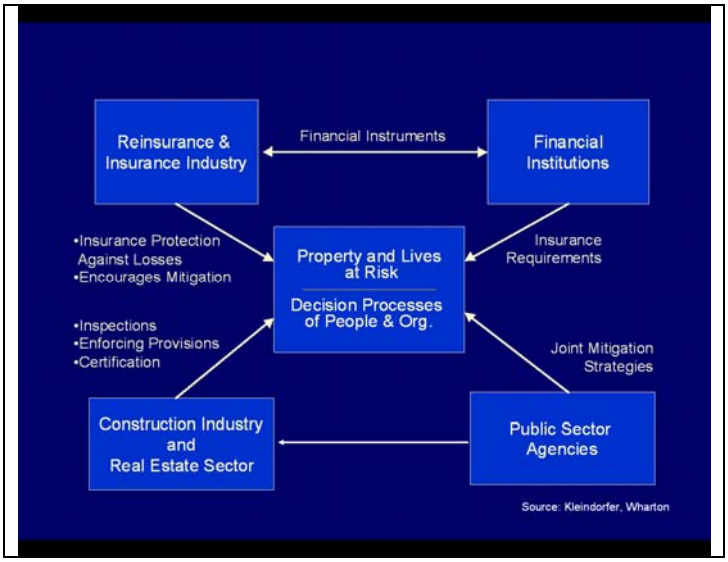
Example:
The case of the twin towers of the World Trade Center (WTC), destroyed in the 11 September 2001 terrorist attacks, is an interesting and tricky example of risk finance. The insurance cover for the WTC was US$3.5 billion. As both buildings were hit at more or less the same time in the same manner by terrorists belonging to the same group, the question needed to be clarified as to whether the attacks constituted one or two occurrences – that is, would the insurance companies have to pay once or twice. After a two-and-a-half year trial, Swiss Re received a favorable verdict in the declaratory relief action against Silverstein Properties, the master leaseholder of the World Trade Center. The argument was that the parties were bound by the language of the WilProp Form, which defines the loss of the twin towers as one event, i.e. an "occurrence or series of occurrences". A similar case was the attack on Pearl Harbor during World War II. Here the same question of whether the attack constituted one or several occurrences arose.

The lessons that can be learnt from these events are:

- Risk financing and insurance is intimately linked to risk management (insuring infrastructure against crises).
- The scope of insurance has decreased significantly since 11 September. Indeed, this scope has been gradually declining since the 1990s. In true risk management, from an insurance perspective, every loss is preventable (barring acts of God).
- Insurance is very important in society. The insurance mechanism gets people thinking about risk management and the literal value of protection.
- Mind the gap. Who is going to fill the gap in post-disaster situations? (see example Silverstein or Swiss Re)

The following two figures illustrate the connection between risk assessment, financial institutions and the insurance industry, people and organizations, the public sector, and private industries.





We have to understand that to handle risks and uncertainty better, there have to be auditable risk management processes in place that clarify and distribute authority, responsibility, and accountability. Further, pre-loss and post-loss risk financing has to be addressed, where an assessment of the financial consequences of various worst-case scenarios is performed and where the loss-financing abilities of all actors involved are determined, that is, who can pay and who will pay for loss and recovery? This concerns:

- Individuals, homeowners
- Trade and industry
- Municipalities and counties
- Insurers
- Financial institutions
- NGOs
- State financing.

Switzerland: *"KATAPLAN – Risk-Based Emergency Planning"*

Mr Jürg Balmer
Swiss Federal Office for Civil Protection, Switzerland

Main message: Things should be settled at home first. This means that emergency planning has to be done locally, according to uniform criteria.

The world and society are threatened to varying degrees by very different natural and man-made hazards such as floods, avalanches, nuclear accidents, earthquakes, riots, and many other hazards. As many of these risks cannot be controlled, they have to be managed. The Swiss Federal Office for Civil Protection issued the first report "Disasters and Emergencies in Switzerland" the KATANOS report, in 1995. An updated version, KATARISK, on risk assessment from a civil protection perspective was published in 2003. The office is now working on a project, KATAPLAN, that looks at the methods and procedures that deal with the principles of risk-based planning for local and regional use. The following table gives an overview of the dangers relevant to civil protection in Switzerland.

	Scope of dangers which are relevant for civil protection			
Everyday incidents	**Disasters**	**Emergencies**	**Violence below the threshold of war**	**Armed conflicts**
Limited incidents Major incidents	Natural disasters (e. g. earth-quake) Man-made disasters (e. g. nuclear accident)	Wide-scale health hazard Massive influx of refugees Breakdown of big parts of the information infrastructure (e. g. computer break-down)	Blackmail of Switzerland from abroad Extremism, terrorism	War in neighboring countries with or without use of weapons of mass destruction Armed conflicts in Switzerland
No or short warning time				**Warning time = several years**

The KATARISK report covers the dangers in the left part of the table (in gray):

- Everyday limited and major incidents
- Disasters such as natural catastrophes (e.g. earthquakes) and artificial disasters like nuclear accidents
- Emergencies related to wide-scale health hazards or a massive influx of refugees.

A comparative view of disasters and emergencies, as well as everyday incidents, shows that both groups currently represent approximately 50 per cent of all risks relevant to Switzerland. How is this comparative view obtained? First, a risk analysis is performed where the extent of damage is described by the same five indicators:

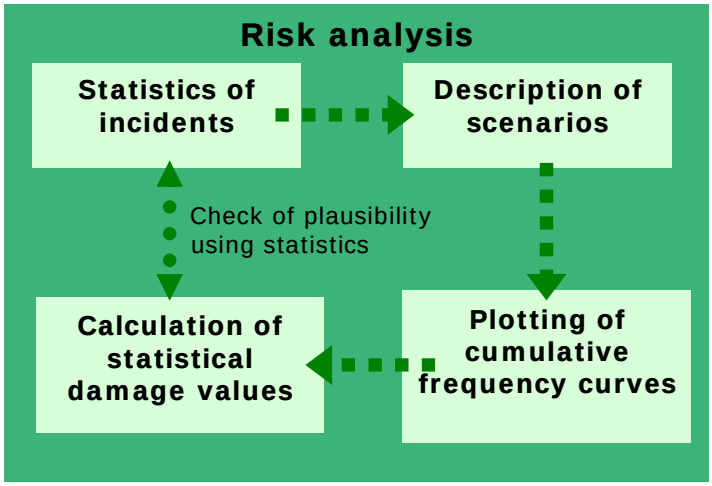
- Number of victims (fatalities, injured, sick)
- Number of evacuees
- Number of those in need of relief (homeless, persons in need of care)
- Damage to the environment (km^2)
- Property damage (reconstruction costs)

Thus, incidents become comparable.

Approach

A systematic investigation of all selected hazards in a two-stage procedure was used:

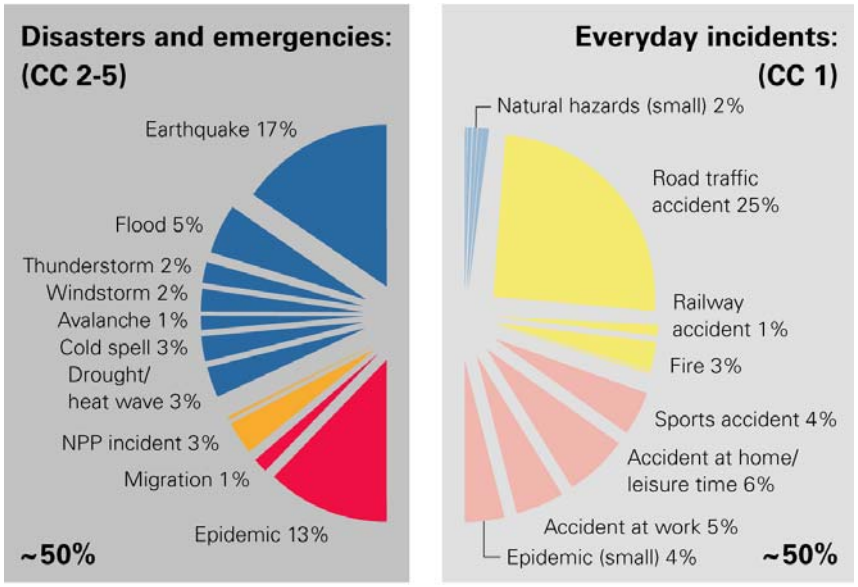
Risk analysis, based on damage indicators, describes and quantifies the hazards in relation to their frequency and the expected extent of damage



Risk evaluation considers society's readiness to pay to prevent damages (marginal costs) and risk aversion relative to large-scale and rare and unknown incidents.

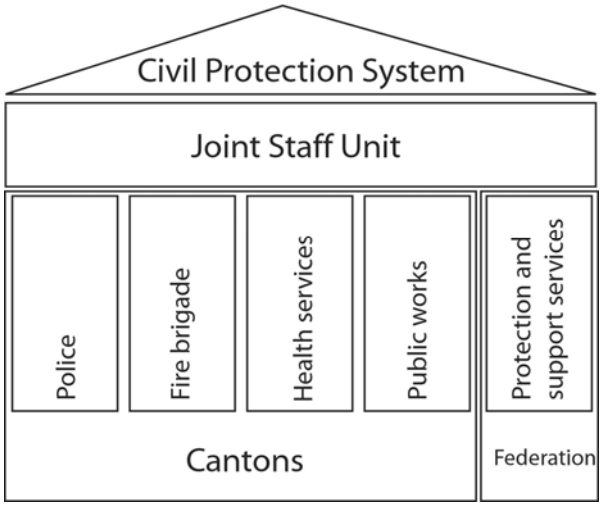
Risk evaluation		
Monetary terms of statistical damage values (marginal costs)	→	**Weighting** by consideration of aversion against large-scale incidents

Based on this evaluation, the risks are compared. The largest share of disaster and emergency-related risk goes to strong earthquakes, widespread epidemics, and large-scale flooding. Traffic and sports-related accidents and accidents at work, in the home, and during leisure time represent the largest part of risks related to everyday incidents.

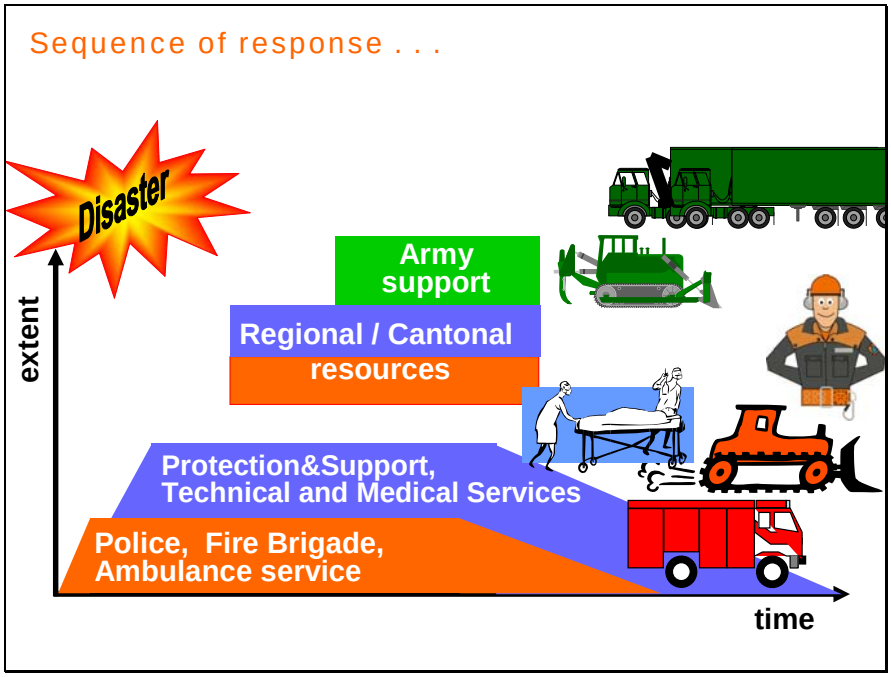


Responsibilities

The civil protection security policy mandate is to protect the population and the nation's vital resources during disasters and emergencies and in the event of an armed conflict. Civil protection builds up day-to-day resources and guarantees the coordination and cooperation of the five partner organizations working together to master a catastrophe. The civil protection system combines cantonal and federal bodies, directed by a joint staff unit (commando).



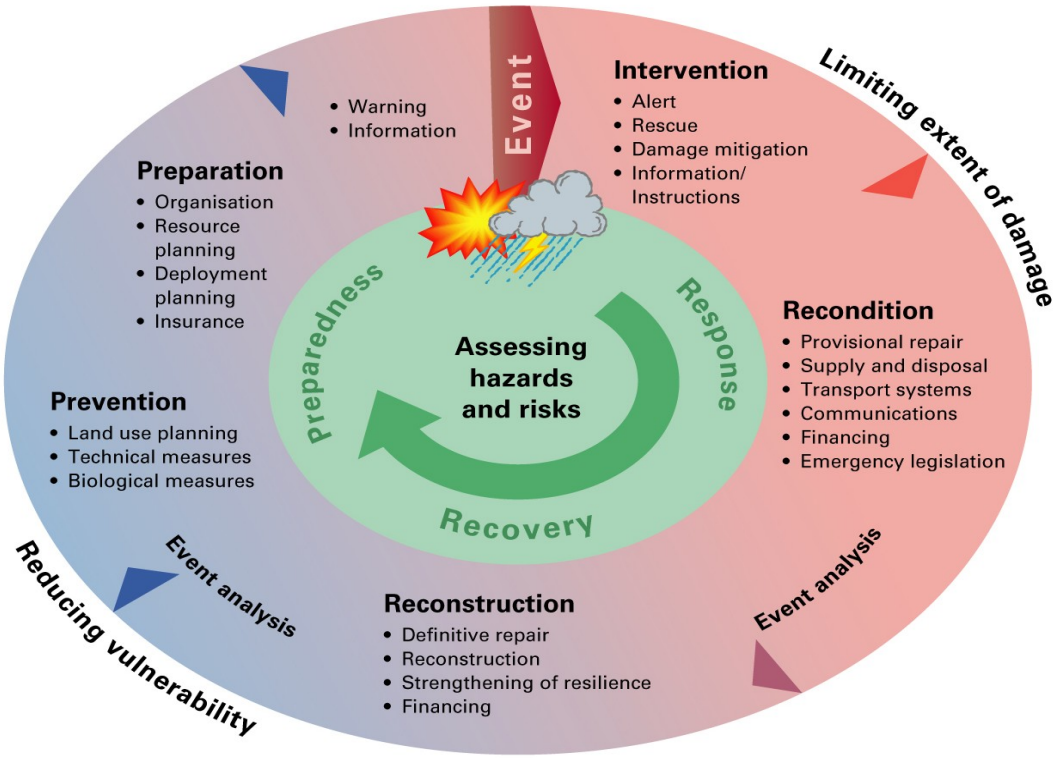
The joint staff unit directs the response in case of an emergency. The resources used depend on the duration of the catastrophe (time) and the extent of damages. Military resources can be engaged to top up other means, if necessary.



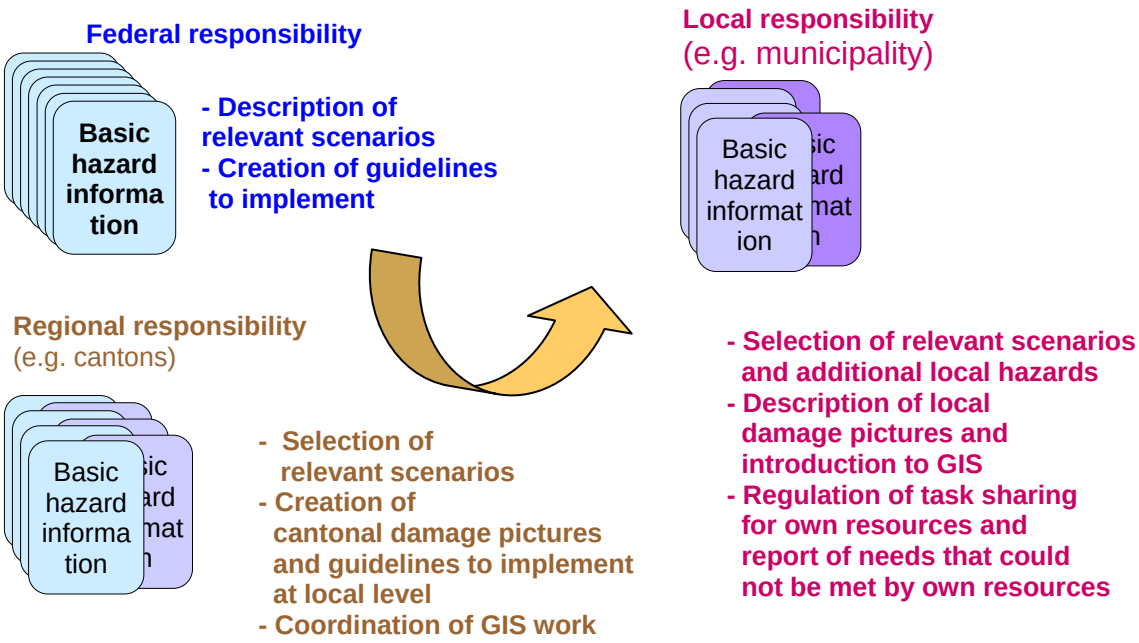
Small, everyday incidents will be dealt with at the local level, larger incidents at the regional level, and incidents relevant to the whole country at the national level. Local incidents include traffic accidents and regional incidents include various small natural events. National incidents are, for example, strong earthquakes and storms.

Risk management and risk-based planning

Risk management consists of various elements that affect each other and are thus part of an integrated process (see next slide):



The following slide gives an overview of who in Switzerland should be responsible for what, when it comes to risk assessment.



For emergency planning, several points have to be considered:

- Hazards and the resulting risks have a different relevance for different communities
  - Risks have to be assessed in relation to the community concerned (locally, regionally, nationally)
- The resources of the community concerned have to be prepared for a best possible response
  - Not everybody must be able to cover everything

Risk-based emergency planning for a specific community requires:

- Identification and evaluation of risks (risk assessment)
- Identification of the need for assistance, based on risks
- Preparation of the community's own resources for the best response
- Planning of external assistance
  - Available resources (the community's own and external ones) can be best prepared for response actions
  - Resources can be planned according to real needs based on assessed risks

Various categories of risks and the corresponding method for risk management can be presented as shown below (based on O. Renn[64]).

[64] O. Renn, *Das Vorsorgeprinzip - eine Gratwanderung zwischen Willkür und Zukunftsicherung*', Presentation held at Zurich University of Applied Sciences Winterthur, Switzerland, 2.10.2003

Routine risks	**Complex risks**		**Uncertain risks**		**Ambiguous risks**
Everyday incidents	**Disasters**	**Emergencies**	**Violence below the threshold of war**	**Armed conflict**	**?**
- Traffic accident - Fire - Accident at work - …	e.g. KATARISK ambitious but calculable		- Cyber war - Climate Change - New epidemics … No statistics Many assumptions Side effects		- Genetic engineering - Implementation of biochips - … Disputed Chance or risk?
RISK MANAGEMENT:					
Standard procedure	Relationship between costs and benefit		Precaution, setting of limiting values		Discussion, political decision

Whenever we discuss how to deal with a specific risk, we have to first look back (statistics, experience) and then have to try to design a suitable scenario for describing the risk as comprehensively as possible.

Working group results

Panel I
The challenge of security threats and emergencies in modern society

Core questions for Panel I:

- What is the specific content of the emerging security panorama in regard to the nation state's responsibilities?
- What challenges do the management of threats and vulnerabilities in modern society create?
- What are the objectives and rationale behind the security concepts? How applicable are they?

Question 1: What is the specific content of the emerging security panorama in regard to the nation state's responsibilities?

The state is responsible for the survival of the country and its citizens. It thus has to support the welfare of the population and the continuity of the system through trust and accountability and the protection of

- Critical infrastructures
- Health of the population
- The environment
- The cultural characteristics
- The economy
- The basic values of Western modern society

It has to provide for education and political and legal institutions to safeguard law and order/rule of law.

Various risks and threats can prevent the state from providing security. It is not possible to protect the state and its citizens against everything. Nevertheless, the state has to keep an eye on all possible threats, try to understand them, and deal with them in a sensible manner. Thus, risk analysts and politicians have to work together to move ahead in the process of sensible risk management. This will also help to continuously develop methods of how to deal with future threats. The creation of scenarios is one way of analyzing future risks. As risks might nevertheless develop differently from what has been predicted, one has to continuously evaluate and adapt the scenarios and thus the long-range planning. Trend analyses and imagination help to foresee future risks.

Question 2: What challenges do the management of threats and vulnerabilities in modern society create?

We have to expect the unexpected and be prepared as well as possible and feasible against the risks we face today. We can do this by applying preventive measures and by enhancing the capability of recovery after damage. To be able to adapt more easily to new developments and changing environments, the state and private industries have to develop organizations that are flexible and dynamic. Politicians have to be made aware of

the long-term results of short-term politics. Negligence of long-term risks will cause serious damage in the future.

It is neither possible nor sensible to deal with all risks in the same manner. Thus risks need to be prioritized, and resources and means have to be allocated accordingly. An important question is which measures are acceptable and which are not. What is possible and what is not? What is the legal aspect of these measures? The speed in which for example laws can be adapted will have an influence on the response. However, there has to be a balance between adaptability and rigidity of laws for the protection of right. We also have to determine how much we expect the state to do for us. Do we want the government to maintain control over private entities, to the extent that these private entities provide critical services?

Public expectations need to be managed for the benefit of each citizen and for the country's neighbors.

Question3: What are the objectives and rationale behind the security concepts? How applicable are they?

Security concepts are constantly being challenged, as they are tied to the perceived threats. We thus have to ask ourselves whether our security policy or concept is adequate for meeting the threats we perceive. Also, what purpose do they serve? What is their function? The concept of neutrality or armed neutrality, for example, can be a source of safety or it can be a smokescreen. After a time of transparency and openness, the traditional understanding of security concepts from Cold War times has become more prevalent lately. Thus, the question arises whether it is at all possible to have comprehensive security or whether traditional, state centered security will take over again. Concepts also do not always fulfill what they promise. The solidarity clause, for example, worked well within NATO; within the EU, however, it (currently) does not have any substance behind it.

Panel 2
Distribution of responsibilities and funding when dealing with societal security, public safety, and emergency management

Core questions for Panel II:

- How can vertical and horizontal security and safety cooperation be optimized?
- Who should set preventive priorities and define security standards?
- Who pays for and who will benefit from dealing with vulnerabilities?

Catchphrases: communication – cooperation – trust – responsibility - accountability

Question 1: How can vertical and horizontal security and safety cooperation be optimized?

For optimization of vertical and horizontal security and safety cooperation a better risk management culture is needed. The experts have to assess risks and should also provide the information to politicians in such a way that politicians can understand how the findings of a risk analysis should be incorporated into security policy. A major problem is, however, the ambivalent way in which politicians perceive risk analyses. While on the one hand risk analyses provide them with essential and relevant information on the risks their country faces, on the other hand, they perceive risk analyses as potentially constraining their freedom to act. The key is to find a balance that leaves politicians the freedom to act but still allows them to recognize that certain threat-specific countermeasures must be taken. For this, governments must maintain a continuous dialog with scientific institutes and the private industry. The creation of inter-agency coordination groups (taskforce) would be very helpful to vertical and horizontal communication and cooperation.

How can the state bring security to the individual? This process has to start from two sides: Individuals have to clearly voice their expectations and needs, which strongly depend on the political systems we live in, our culture, and other factors. Expectations usually become greater, the more security is already provided. We have to be aware, however, that there will eventually be an end to this chain, as total safety can never be provided.

The responsible actors in the government have to agree on targets and strategies of how to best fulfill the safety demands and how to tailor their approaches to the specific needs at the various levels. They also have to agree on who is responsible for what and to what extent (also financially). It is important, though, that the government always remains the central actor who instructs and guides the other players (industry, various agencies, civilians)

Question 2: Who should set preventive priorities and define security standards?

The ultimate responsibility to protect the people and the country has to lie in the hands of the government. The government has to be aware of risks and vulnerabilities. The threats, however, have to be defined by society as a whole. Society must state what it wants and at which price – financially and in other ways. Businesses as part of public-private partnerships can increase a nation's and people's security, but for these partnerships to function, the government has to give something in return and has to share the information it has. Information has to flow vertically as well as horizontally, and this could be fostered through platforms for risk communication. Besides the private

industry, IOs and NGOs – for example, the OECD in the IT sector – are setting security standards that everybody can benefit from. The state also has to take advantage of the knowledge of local actors, as they are closest to potential problems in their environment. While some responsibility has to be shared, it cannot completely been forced on to individuals and companies, who are also very hesitant to accept and often unable to take the responsibility. Another aspect concerns the enforceability of responsibility. To achieve it on all levels, some legal pressure might be required.

Question 3: Who pays for and who will benefit from dealing with vulnerabilities?

Today's general understanding is that we are more or less protected against any harm, and if we should nevertheless experience harm or loss, we will be reimbursed. But this has never been true, and it will never be true. We have to understand that sometimes sacrifices have to be made. But are we ready to share risks and misery? To prepare the people for what they might face, they have to be informed about risks, safety, and security, and the government has to set standards, regulations, and guidelines. However, dealing with vulnerabilities has become profitable, while safety is often understood as not paying off. Thus prevention is often neglected, and a stronger focus is placed on repair and recovery. Various examples, e.g., when dealing with floods, show, however, that if there is a valid reason to believe that a specific event will happen, that is, if there is a moderate to high risk, then prevention pays off very well. For businesses, the right risk management can be essential, as some companies will not survive specific events, while governments usually do. The blame, however, will not only be placed with the business that failed but also with the government for not having foreseen and prevented the damage.

As already mentioned several times during this discussion, the right communication is important and challenging. Often, various sectors know too little about each other, the vocabulary they use differs, and cultural differences enhance a different understanding of vulnerabilities. These problems need to be overcome.

And what about solidarity? What can we expect from the community? Various case studies have shown that during disasters, solidarity is very high. Help within the community is usually also the most important, as it represents help on the spot. Community thus somehow represents an untapped resource. But as it is not paid for, it cannot be demanded. However, one can at least appeal to the pioneering spirit and to self-help, which is a question of political and personal will.

And finally, who will pay for safety and security? In the end, it is always the consumer who will pay and benefit, either as a consumer or as a tax payer.

Summary

The challenge of security threats and emergencies in modern society

During the Cold War, security was mainly defined by the bipolar system that held the whole of Europe and much of the world in its grip. The Cold War was characterized primarily by nuclear deterrence between the East and the West. Thus, the security thinking followed the lines of traditional state-centric military security. However, with the end of the Cold War, the traditional military and state-centric security concept was placed more and more in question. This was the result of various developments: military threats gave way to "new" threats and risks, and global security concerns gave way to regional and local security matters. Among the advanced industrial democracies, political means of conflict resolution replaced military means. Today's *Comprehensive security* describes the broadening of the notion of what security is away from purely military issues into the fields of politics (insofar as these had not been included so far), economy, ecology, and society. *Comprehensive security* moves away from state-centricity and national security towards the security of people, either as individuals or as a group.

The attacks of 11 September 2001 brought about another turning point in security matters. The emergence of threats like global terrorism could be described as a kind of anti-globalization movement against Western values, such as human rights, liberal democracy, market economy, freedom, tolerance, and open and pluralistic societies. These issues are addressed in the new fields of societal security and homeland security, which are meant to bridge the gap between state security (law and order) and human safety (rescue services) to not only protect the sovereignty of the state but also its people, values, and functions (Sundelius, this report). To do so adequately, the institutions, organizations, and methods that deal with today's threats have to be adapted to today's security issues. New security strategies have to be developed to enhance a country's crisis management capability, with a special focus on peacetime crises.

The security of a country, however, is no longer only a national task. Many risks and threats, for example, natural catastrophes, economic crises, and migration, are not geographically limited or constrained to one nation but are highly transnational. Thus, these also have to be addressed on not only a national level but on an international level; national and international networks and task forces have to be created and maintained; information must be shared; and domestic and external security and safety have to be linked at the international level. Sundelius (this report) calls this link between the international and domestic sphere the *intermestic* sphere. The EU is one of the international organizations that has to operate in this intermestic sphere. However, differences in, for example, culture, values, and needs pose problems, as they lead to different perceptions about what should be safeguarded and why. Every country also has its "own" vulnerabilities and thus requires different measures for prevention, protection, crisis management, and recovery from crises. All these differences bring about the potential of a crisis within the EU. This has to be prevented, though, as does the possibility that a potential crisis within the EU could lead to a crisis for the EU.

To make things even more complex and challenging but also more thorough and complete, Hamilton argues in this report that we have to look beyond the EU, think globally, and aim to bring about a healthy transatlantic relationship. Due to the many connections between countries and continents, the EU and the US cannot operate alone. Differences between the EU and the US are not insuperable; certainly there are issues that make consensuses difficult. But the EU and the US also have a lot in common, including the many threats they face. Terrorism, for example, is not solely a US problem. The terrorist attacks of 11 March 2004 in Madrid have shown that the new terrorism has also reached Europe. The US and the EU have to work together to counter terrorism and other threats. The different viewpoints and approaches that the two continents have

might make cooperation difficult at times. Also, the US model of civil security is still not "transatlantic" enough, while European jurisdiction is too confusing for the US. However, these problems need to be addressed and a solution found. Homeland or societal security does not end at a country's border: Security is an international task. Thus, it has to be safeguarded not only by each individual country but also by the international community.

Ensuring security is a major task. In establishing various security measures, local, regional, national, or supranational sovereignties may be encroached upon. Also civil liberty issues might be challenged, when privacy issues are balanced against security. It is thus most important to open up the public discourse and to involve the people in the discussion about today's threats and potential countermeasures in order to define the extent to which they are prepared to go to defend their basic values.

However, to begin with, a sensible and dynamic risk analysis has to be performed, so those involved know the short- and long-term risks we face. This requires that we expect the unexpected and understand the risks we face, prioritize them, and allocate the means accordingly. This lies mainly in the hands of governments, but increasingly private industries have to be mobilized and become involved. SEMA is an example of a new crisis management system that promotes this interaction between the public and the business sector in the field of emergency management.

To summarize, the Cold War security concept is no longer viable for protecting today's society and its individuals. An overall security concept has to be found that can handle the broad spectrum of threats and risks to which society and its individuals are exposed. The realization of security will require multi-sector, multi-level, multi-institutional, multi-national, and multi-continental cooperation.

Distribution of responsibilities and funding when dealing with societal security, public safety, and emergency management

One part of homeland and societal security is an effective emergency preparedness and crisis management. In the past, this was comparatively easy to achieve, as the responsibility and services were in the hands of the government. In recent years, however, public monopolies, infrastructure networks, and services (energy supply, transportation, health care) have been increasingly liberalized through deregulation and privatization. This has had many positive effects, like increased efficiency and productivity, but it has also had drawbacks, for example, with regard to the accessibility, reliability, and affordability of services. However, the questions arise: Who is responsible when services are no longer available? Who has to pay to avoid a loss or interruption of services? Who has to pay for the consequences of a service failure and for repairs? In times of liberalization, the answer is not easily found, as it is no longer the government alone who runs various services but also businesses – and both have different standards, means, and policies. This can cause serious problems, as some of the systems and services concerned are critical for a state to function. Thus, the responsibilities have to be clearly assigned to those involved to ensure a well functioning state and society.

How is this done? In the end, the government will always be responsible, and private companies will generally be reluctant and often also unable to assume full responsibility. This is due to the fact that private industries follow different rules, namely those of the market economy. They have to keep costs low and maximize profit, which usually leaves only few resources for crisis management.

To fill the gap, as Andersson and Malm call it (this report), between government emergency preparedness measures and private actors' lack of interest in providing such measures, some option were discussed at the workshop. One option concerns legislative regulations, another the deployment of financial incentives for industries, and a third the

creation of public-private partnerships (PPPs). The third alternative seems to be the favorite option for both governments and industry, and it is already widely employed. This is so because through PPPs the government has some influence on the private sector, while the private sector can thus avoid strict regulations.

Whether PPPs will be able to successfully engage in the field of emergency management remains questionable, however. Still many obstacles have to be overcome. Appropriate emergency management measures will require clear guidelines and recommendations, as well as consensus among actors, time, and money. Some government intervention and regulations will probably be necessary.

Here are some suggestions for ensuring security despite liberalization. Coordination of these should remain with the government:

- Information should be shared continuously, both horizontally and vertically (industry, government, academia). Sensitive information has to remain classified. Good communication facilitates good cooperation. All have to work together.
- Minimum standards for security should be defined, and those involved must determine who is responsible for what. Actors must be informed about their responsibilities and about the legal and financial implications.
- Industry, governments, and academics must learn from one another.
- The risks and threats to a country and its society must be defined and analyzed. People must be informed about risks, safety, and security.
- Experts should find out the degree of protection the people want and at what prize – financially and legally.
- The various parties must define and agree upon what is to be protected, by whom, and to what degree. The government has to assure that the required protection is guaranteed.
- Dealing with vulnerabilities has become profitable, while safety is often understood as not paying off. The various actors must be convinced of the contrary, and solutions that all can agree upon must be found.
- People at all levels (local, regional, national) must be involved. They should be allowed to take their share of the responsibility (and financing) to reduce vulnerability, minimize damage, and increase resiliency. In the end it is always the consumer who will pay and benefit anyway, either as a consumer or as a taxpayer, so all should be encouraged to become involved at an early stage.
- Preparedness activities and planning mechanisms must be consistent, not duplicated, efficient, and effective. Privately owned critical infrastructures must not be forgotten, and interdependencies between critical infrastructures must be kept in mind.
- Recommendations for response and mitigation actions from the perspectives of the public and private sectors must be developed.
- Emergency coordination at the local and state level must be centralized.
- Funding must be made available for all threats and not weighted towards one or two individual threats (e.g., the war on terrorism).
- Pre-loss and post-loss risk financing must be addressed, the financial consequences of various worst-case scenarios must be assessed, and the loss-financing abilities of all the actors involved must be determined, that is, who can pay, and who will pay for loss and recovery?
- New ways of funding must be found, for example, taxes, fees, and voluntary financing.
- Precise measures must be defined, decisions must be made, and responsibilities must be allocated.
- And:

DON’T

BUT DO

(Schliessen Sie Ihre Lücken. – Fill the gaps.)

Acknowledgements

I wish to thank Mr Stein Henriksen, Prof Jan Hovden, Dr Jan Joel Andersson, and Mr Andreas Malm for providing me with written versions of their presentations. I would also like to thank the other authors for reviewing the summaries of their presentations. The two texts by Dr Daniel S. Hamilton and Mr Per Åkenes have not been reviewed and I am thus solely responsible for the summary of these presentations. The full and sole responsibility for all other content of this publication also lies with me and not with the Swedish Emergency Management Agency and the CRN.

I would further like to thank Dr Stephanie Buus and Jesper Grönvall from the Swedish National Defense College for providing me with their notes of the workshop presentations. I also thank Dr Michelle Norgate for editing the report.

Programme

Thursday, April 22, 2004

Arrival of participants

19:30 **Informal evening reception at SEMA (the Swedish Emergency Management Agency), Kungsgatan 53**
Welcoming address by the Head of Department, ***Mr Staffan Karlsson***

Friday, April 23, 2004

07:00- 08:20 Breakfast

08:30-08:40 Opening
Official opening of the workshop by the Deputy Director General, ***Mr Lars Hedström***, SEMA

08:40-08:50 Goals of the workshop and general information
Workshop chairman, ***Mr Jan Lundberg***, Senior Analyst, SEMA

08:50-09:00 CRN introduction and outlook
Dr Jan Metzger, Senior Researcher, Center for Securtiy Studies, ETH Zurich, Switzerland

09:00-09:45 Keynote speech
"Transatlantic Homeland Security and Societal Security",
Dr Daniel S. Hamilton, Johns Hopkins University, USA

09:45-10:15 Coffee break

10:15-10:45 Introductory speech for Panel I
"The Challenge of Security Threats and Emergencies in Modern Society",
Prof. Bengt Sundelius, National Defence College, Sweden

10:45-12:15 Panel I: The challenge of security threats and emergencies in modern society
Moderator: ***Capt Ernst M. Felberbauer***, Bureau for Security Policy, Austria

Presentations (15 min.)

- Sweden: *"A New Security Strategy"* ***Mr Michael Mohr***, Swedish Defence Commission, Sweden
- Austria: "*Comprehensive Security"* ***Dr Henriette Riegler***, Austrian Institute for International Affairs, Austria
- Norway: *"Risk and Uncertainty Management Strategies"* ***Prof. Jan Hovden***, Norwegian Technical and Natural Sciences University, Norway

12:15-13:15 Lunch

13:15-14:45 Working groups
Introduction to the working groups Capt Ernst M. Felberbauer, Austria

14:45-15:15 Working group results Moderator: ***Capt Ernst M. Felberbauer***, Austria

15:15-15:30 Final remarks on Panel I *Panelists of Panel I*

15:30-16:00 Coffee Break

16:00-16:45 Introductory speech for Panel II
Mr Andreas Malm and ***Dr Jan Joel Andersson***, 4C Strategies, Sweden
"Distribution of Responsibilities and Money in Dealing with Societal Security, Public Safety and Emergency Management"

16:45-17:00 Round-up session and dinner instructions
Workshop chairman, ***Mr Jan Lundberg***, Sweden

18:40 Departure from hotel by coach

19.00 Dinner at the Cavalry Mess, Life Guards' Regiment, hosted by SEMA
(Dress code "formal" i.e. dark suit)

Saturday, April 24, 2004

07:00- 08:20 Breakfast

08:30-10:30 Panel II: Distribution of responsibilities and funding when dealing with societal security, public safety and emergency management
Moderator: ***Mr Roger Steen***, Norwegian Directorate for Civil Protection and Emergency Planning, Norway (conf.)
Presentations (15 min.)

- USA: "*Federalism/Regulatory Processes for CIP in the US compared to Europe"*
  and
  USA: "*National Capital Region Modern-day Threat Planning Process"* ***Ms Anne Dailey***, Critical Infrastructure Project, National Center for Technology and Law, George Mason University, USA
- Norway: "The Shift of Responsibilities within Government and Society" ***Mr Stein Henriksen***, Norwegian Directorate for Civil Protection and Emergency Planning, Norway
- Sweden: "*Risk Finance"* ***Mr Per Åkenes***, Aakenes Advisory Services, Sweden
- Switzerland: "KATAPLAN – Risk-Based Emergency Planning**"** ***Mr Jürg Balmer***, Swiss Federal Office for Civil Protection, Switzerland

10:30-11:00 Coffee break

11:00-12:30 Working groups
Introduction to the working groups *Mr Roger Steen*, Norway

12:30-13:30 Lunch

13:30-14:00 Working group results Moderator: ***Mr Roger Steen***, Norway

14:00-14:25 Final remarks on Panel II *Panelists of Panel II*

14:25-14:45 Conclusions and Final remarks *Dr Jan Metzger*, Switzerland

14:45-15:00 Round-up session – What's next?
Workshop chairman: ***Mr Jan Lundberg***, Sweden

15:00 End of workshop *A chance to do some serious shopping*

Sunday, April 25, 2004

07:00-10:00 Breakfast

Departure of participants

List of participants

Switzerland

	Family name	First name	Title	Country	Organization	E-mail
R	Dunn	Myriam	lic phil	Switzerland	Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)	dunn@sipo.gess.ethz.ch
R	Guery	Michael	Dr	Switzerland	Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)	guery@sipo.gess.ethz.ch
R	Kastrup	Ulrike	Dr	Switzerland	Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)	kastrup@sipo.gess.ethz.ch, ulrike@kastrup.net
R	Mauer	Victor	Dr	Switzerland	Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)	mauer@sipo.gess.ethz.ch
R	Metzger	Jan	Dr	Switzerland	Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)	metzger@sipo.gess.ethz.ch
R	Maridor	François D.		Switzerland	Directorate for Security Policy	francois.Maridor@dsp.admin.ch
R	Balmer	Jürg	Ing HTL	Switzerland	Federal Office for Civil Protection (FOCP)	Juerg.Balmer@babs.admin.ch
R	Brem	Stefan	Dr des	Switzerland	Ministry of Foreign Affairs	stefan.brem@eda.admin.ch stefan.brem@switzerland.org

Sweden

	Family name	First name	Title	Country	Organization	E-mail
R	Engelhart	Monica	Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	monica.engelhart@krisberedskapsmyndigheten.se
R	Hansson	Oskar	Principal Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	oskar.hansson@krisberedskapsmyndigheten.se
R	Hedström	Lars	Deputy Director General	Sweden	Swedish Emergency Management Agency (SEMA)	lars.hedstrom@krisberedskapsmyndigheten.se
R	Jennerholm	Mattias	Principal Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	mattias.jennerholm@krisberedskapsmyndigheten.se
R	Karlsson	Staffan	Head of Depart-ment	Sweden	Swedish Emergency Management Agency (SEMA)	staffan.karlsson@krisberedskapsmyndigheten.se
R	Lundberg	Jan	Principal Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	jan.lundberg@krisberedskapsmyndigheten.se

	SWEDEN *cont.*					
R	Måwe	Karin	Principal Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	karin.mawe@krisberedskapsmyndigheten.se
R	Myrdal	Sara	Principal Admini-strative Officer	Sweden	Swedish Emergency Management Agency (SEMA)	sara.myrdal@krisbredskapsmyndigheten.se
R	Stern	Peter	Dr	Sweden	Swedish Emergency Management Agency (SEMA)	peter.stern@krisberedskapsmyndigheten.se
R	Åkenes	Per	Risk Manager	Sweden	Aakenes Consulting AB	per@aakenes.se
R	Andersson	Jan-Joel	Dr	Sweden	4C Strategies AB	jan.joel.andersson@4cstrategies.com
R	Malm	Andreas	Manager	Sweden	4C Strategies AB	andreas.malm@4cstrategies.com
R	Mohr	Michael	Main Secre-tary	Sweden	Swedish Defence Commission	michael.mohr@defence.ministry.se
R	Molin	Staffan	Head of Depart-ment	Sweden	Swedish Defence Research Agency	staffan.molin@foi.se
R	Buus	Stephanie	Dr	Sweden	Swedish National Defence College	stephanie.buus@fhs.mil.se
R	Grönvall	Jesper	Senior Analyst	Sweden	Swedish National Defence College	jesper.gronvall@fhs.mil.se
R	Sundelius	Bengt	Prof	Sweden	Swedish National Defence College	bengt.sundelius@fhs.mil.se
R	Eriksson	Johan	Assoc Prof	Sweden	Södertörns University College	Johan.eriksson@sh.se

Austria

	Family name	**First name**	**Title**	**Country**	***Organization***	**E-mail**
R	Felberbauer	Ernst M.	Capt	Austria	Ministry of Defence, Bureau for Security Policy	ernst.felberbauer@bmlv.gv.at e.felberbauer@dcaf.ch
R	Pankratz	Thomas	Dr	Austria	Ministry of Defence, Bureau for Security Policy	thomas.pankratz@bmlv.gv.at
R	Riegler	Henriette	Dr	Austria	Austrian Institute for International Affairs	hriegler@oiip.at

Canada

	Family name	**First name**	**Title**	**Country**	**Organization**	**E-mail**
R	Grenier	Jaques	Senior Advisor	Canada	Public Safety and Emergency Preparedness Canada	jacques.grenier@psepc-sppcc.gc.ca
R	Smith	George D. (Tim)	Dr	Canada	Canadian Security Intelligence Service, Government of Canada	smithtim@smtp.gc.ca
R	Wong	Suki	Director	Canada	Public Safety and Emergency Preparedness Canada	suki.wong@psepc-sppcc.gc.ca

Germany

	Family name	First name	Title	Country	Organization	E-mail
R	Maskow	Mark	Specia-list	Germany	Academy for Crisis Management, Civil Emergency Planning and Civil Protection	mark.maskow@bva.bund.de MarkMaskow@aol.com

Luxemburg

	Family name	First name	Title	Country	Organization	E-mail
R	Lenz	Guy	Colonel hon., Haut-Commis-saire	Luxemburg	Ministère d'Etat, Haut-Commissariat à la Protection Nationale	guy.lenz@hcpn.etat.lu secretariat@hcpn.etat.lu
R	Welter	Isabelle	Attaché de Gouver-nement	Luxemburg	Ministère d'Etat, Haut-Commissariat à la Protection Nationale	isabelle.welter@hcpn.etat.lu

Norway

	Family name	First name	Title	Country	Organization	E-mail
R	Henriksen	Stein	Senior Adviser	Norway	Directorate for Civil Protection and Emergency Planning	stein.henriksen@dsb.no
R	Steen	Roger	Senior Advisor	Norway	Directorate for Civil Protection and Emergency Planning	roger.steen@dsb.no
R	Hovden	Jan	Prof	Norway	Norwegian University of Science and Technology	jan.hovden@iot.ntnu.no

USA

	Family name	First name	Title	Country	Organization	E-mail
R	Dailey	Anne	Senior Legal Research Associate	USA	Critical Infrastructure Project, National Center for Technology and Law, George Mason University	amitche2@gmu.edu, adailey_74@yahoo.com
R	Hamilton	Daniel S.	Dr, Director	USA	Center for Transatlantic Relations, Johns Hopkins University	dhamilt5@jhu.edu
R	Stewart	Stephen H.	Prof	USA	College of Integrated Science and Technology James Madison University	stewarsh@jmu.edu

This report presents the findings of the 6th International Expert Workshop on "Societal Security and Crisis Management in the 21st Century", held in Stockholm, Sweden, on April 22–24, 2004. The report documents the changes in national security concepts and provides new models and concepts for redistributing responsibilities and funding for dealing with the challenges of the 21st century.

The Center for Security Studies of the ETH Zurich

The Center for Security Studies of the ETH Zurich (Swiss Federal Institute of Technology) was founded in 1986 and specializes in the fields of international relations and security policy. The Center for Security Studies is a member of the Center for Comparative and International Studies (CIS), which is a joint initiative between the ETH Zurich and the University of Zurich that specializes in the fields of comparative politics and international relations.

The Comprehensive Risk Analysis and Management Network (CRN)

The Comprehensive Risk Analysis and Management Network (CRN) is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness. Originally launched as a Swiss-Swedish Initiative, the partner network today consists of partners from four different countries: the Swedish Emergency Management Agency (SEMA), Sweden; the Directorate General for Security Policy at the Federal Ministry of Defence, Austria; the Directorate for Civil Protection and Emergency Planning (DSB), Norway; the Federal Office for National Economic Supply (NES), Federal Departement of Economic Affairs, Switzerland and the Swiss Federal Department of Defense, Civil Protection and Sports (DDPS), Switzerland.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.isn.ethz.ch/crn)