A BRIEF ON EMBEDDED SOCIETAL SECURITY

Bengt SUNDELIUS

Abstract: The traditional dichotomy of security threats and responses cannot serve as a basis for developing national and international security arrangements and institutions in the Twenty First century. This article presents the concept of *societal security* and the notion of *intermestic* domain allowing to bridge state security and human safety challenges and to build trans-boundary linkages across domestic and international levels of response. Such holistic approach, that places societal security at the core, is manifested in the Solidarity Clause of the Constitution of the European Union. The implementation of the concept would provide for efficient development of security arrangements within the European Union, between European countries and the United States. Enhanced societal security across the Atlantic could become a core mission for the future work of NATO and the wider Partnership for Peace community.

Keywords: Security Risks, State Security, Human Safety, Crisis Management, Intermestic Domain, Solidarity Clause.

The twenty-five member states of the European Union, including Sweden, are now undergoing serious rethinking about security. In the Brussels focused networks, novel ideas are being presented and debated in a common search for better tools to deal with the security challenges of the future. Traditional fears are combined with revised notions of the consequences of living within a Risk Society. A Solidarity Clause has been included in the proposed Constitution of the European Union, as adopted by the European Council in June 2004. In this political pledge, the member states commit to give all necessary assistance to the other members in the case of a terrorist attack and in a natural or man-made disaster. In this holistic approach, procedures for war-like scenarios and peace-time emergencies merge, internal and external security are interlocked, and the ambitions of enhancing state security and providing citizen safety become blurred.

There is a paradigmatic shift in Europe from the national defence systems of the Cold War to the evolving notion of *embedded societal security*. The member states of the EU are developing novel practices for dealing with security challenges from abroad, at home and not least *within its intermestic sphere.* The latter domain becomes a primary playing field for the pursuit of embedded societal security in and by the Union. Several types of actor-focused and structurally-based threats can be faced in Europe in the foreseeable future. These developments will affect both the security challenges faced and our abilities to meet them in effective and legitimate ways.

This paper presents an overview of the types of threats and challenges that can be faced in Europe over the next ten years. This provides an important departure point for a discussion on the various instruments one may use to respond to these threatening situations. The conceptualisation of societal security, as opposed to territorial security, will be coined. Some trends of post-modern society and trans-national interconnectedness will be outlined. The EU is in the midst of developing novel practices for dealing with trans-boundary security challenges. In this paper a conceptual departure point is presented for such evolving practices across traditional concerns with state security and human safety.

Security Challenges Ahead

First, *actor focused threats* have to be considered. In classical security policy thinking, threats are actor focused and the classical threat is an armed attack by another state. This scenario constituted the essence of the East-West military confrontation. It is still part of the mission for NATO and for all nation states to plan and prepare for a military attack in this classical form. This contingency is now more urgent in other parts of the world than in Europe. Still, the 1990s were a tragic decade of armed conflicts among European national entities.

If one drops the notion of the state, one can focus on another actor focused threat: an armed attack by "another." September 11 was an example of an armed attack by "another." March 11 was another memorable example of this category. Another something is possible as a source of armed attacks and a network of terrorists is considered the most likely Other. What would be the most proper instruments to cope with that kind of challenge? Are the instruments that were developed to deal with military invasion, i.e. an armed attack by another state, also the most appropriate to deal with an armed attack by "another something?" Should such violent threats be framed as legitimate national defence concerns, as an area for criminal investigations and police authority, or as the evolving internal-external hybrid of societal security? The choice of framework will have consequences for the appropriate legalities and the instruments chosen to deal with this type of armed attack.

Europe has a legacy of violent terrorist attacks going back to the days of the multinational empires of Russia, Austria-Hungary, and Germany. In the 1960s, and particularly in the 1970s, a number of terrorist attacks were again experienced on this continent, including in Sweden.[1] In the United Kingdom, Spain and France terrorist bombings occur at regular intervals.[2] In many ways, armed attacks by “another” manifest traditional challenges to national and international security. This form of violent protest against the established political order will be with us for a long time.

A third actor focused threat is an attack by another state. Not all such attacks necessarily involve lethal means. Classical coercive instruments for threatening other parties are economic warfare, psychological warfare, etc. One can build on networks in trade, finance, energy, and so forth to manipulate other countries. There are many illustrations over the last 100 years of attacks by another state that are coercive, but not instantly deadly. How does one deal with these?

During the 1980s, the US pursued an economic warfare campaign against the Warsaw pact through the COCOM system.[3] This multilateral strategy involved the control of high technology exports in order to undercut the industrial and technological development of the Soviet Union and its allies. This was a form of attack by another state on certain countries. This coercive type is commonly pursued. It can be viewed as an indicator of superior might, as violence is not necessary to achieve a given policy objective. These types of non-military threats to national independence and even survival are very likely to be with us in the future as well.

Fourth and last of the actor focused threats is the attack by “another.” You have a non-violent attack, not pursued by another state but by another. It could be an isolated incident or event, e.g. an information operation. How can one know initially who or what controls an antagonistic information operation? Is it directed by another state, by a terrorist network, by a criminal syndicate, or by an individual hacker?[4] Is it, for example, a teenager in Germany who is merely interested in throwing havoc into the international information system, as in the Sasser incident? How do you know for sure, when you have to respond to such an attack under severe time pressure?

So far the discussion has been limited to actor focused threats, which is the traditional form of national security concerns. In security planning one traditionally thinks of the antagonistic Other: a person, a government, the enemy, be it a network or a foreign government, or an evil leader. The horizons can be further widened and include also the so called *structural threats*. Structural threats are not actor / agency focused in an antagonistic sense. Rather, consequential situations simply evolve without any intent to harm.

This challenge can be illustrated with two threatening types. The first is a collapse of neighbouring systems, where nobody is at fault in a direct sense. There is no culprit. There is no evil Other.[5] A nuclear plant is destroyed through malfunctions. Something serious goes wrong in Chernobyl or in Ignalina. Energy shortfalls or power blackouts, they just happen and they are with serious safety consequences. Deadly epidemics of various kinds may brake out and spread quickly. Consequences are often widespread and deadly like in violent attacks by some Other.

Within the EU there is an interest in the survival of the neighbouring countries. One needs to ensure in various ways that they do not collapse with grave consequences for themselves and for others. Collapses in the EU near abroad are likely to spill over into our own national security systems.[6] This has been a classic security concern and it was highlighted during the decade after the collapse of the Soviet Union and of the Yugoslavian Federation. This type of security challenge will remain on the agenda for the implementation of the EU security strategy.

In the second type of structural threat—a severe domestic disturbance—consequential events develop within our own societies. Serious accidents, disasters, infrastructure collapses, riots or epidemics spin out of control and have national security implications. They could lead to political up-scaling. Public authorities may enforce severe crisis management efforts that seem effective in dealing with the accident, with the riot or the emergency. Draconian measures also may undermine the legitimacy, the democratic values or the judicial system of society. Many countries search the balance between effectiveness in solving the particular problem, on the one hand, and not undermining over time values, interests and aspirations towards democracy, market economy and individual rights, on the other.[7] Enhancing security in a wider sense may be compromised for the sake of resolving the acute situation. Severe domestic disturbances in European societies could also be a form of structural threat that has to be coped with by public authorities.

One can note over time a shift away from a political focus on *the security of the territory*, a concern with keeping the geographical parameter intact in some fashion. That is the classical concern – the attack by another state. In the future, the political concern will be over *the security of critical functions of society*. It is not the territory that is at stake, but the ability of the government and civil society to function, critical infrastructures to be maintained, the democratic ability to govern, to manifest certain basic values and so forth.[8] This paradigmatic shift from a territorial to a societal security focus influences the thinking within the EU.

Trends Affecting Embedded Societal Security

What trends can be observed in the academic literature on societal developments that are significant for the future ability to enhance national and EU-based societal security? A number of enduring developments are significant within societies, in the relationship between society and the state, and, not least, among societies and governments. The aspects noted below have bearings on how governments can respond to and recover from those serious security threats reviewed above.

Geopolitical space is replaced by a time driven high pace logic of societal security challenges and countermeasures. Seemingly obscure developments in the health sector in a rural region of China in the winter of 2002 were rapidly transformed into a global concern over the rapidly spreading SARS epidemic. Draconian measures affecting individual rights and business practices were initiated in several East Asian nations. Far away Toronto was faced with its own public health crisis over how to cope with the new disease. Distances are not only determined by geography. Proximity can be measured by the time factor as continents and world cities are interconnected through easy air travel or by intercontinental missiles.[9]

In Europe an early warning sign of this trend was manifested in the 1986 Chernobyl disaster. A cloud of radiation was then transmitted by the high winds from the accident site in Ukraine across Central and Northern Europe. The fall-out caused considerable damage to human and animal health, farming and businesses along its way. The effects on the ground have endured over a decade. This early example of rapidly moving, trans-boundary threats to societal security originated in a technical accident. With the possibility of antagonistic threats striking vulnerable infrastructures, the real time character of these threats stand out even more.[10]

National governments need to be geared towards dealing with the security issues related to the critical functions of society and the requirements of governance. It is important when planning for national defence and international security not to build new vulnerabilities into infrastructures or into the fabrics of societies. Vulnerabilities can open up functional access points, channels of penetration for attacks by “another,” whatever that Other may be. Geopolitics and space used to be very important in strategic planning. With an ever more advanced information technology, it is not space but pace that is the important defining strategic element. The time dimension is also at the core for national security planning.

The technological complexities of modern society open for high-risk, tight couplings across sectors and across national borders. Infrastructure interconnectedness has become part of our daily lives as society depends on reliable systems for energy supply, robust communications, and functioning IT-networks. These spheres of activity are mutually dependent on each other. A breakdown in one system may give immediate effects in another. For example, without electricity there will be no IT-function and telephone services will be problematic. Similarly, with a breakdown of an IT-network, electricity supplies may be interrupted. The combination possibilities of system flaws are enormous with such interconnectedness.[11]

Naturally, antagonists wishing to inflict harm upon a society have interests in finding the critical points, where various infrastructures connect. A major task in planning for societal security is to transform potential vulnerabilities linked to this technological complexity into high reliability systems.[12] This is an open-ended process involving many societal sectors and numerous government agencies. It cannot be accomplished without the active participation of those that actually own and control most of these infrastructure networks, i.e. the private business sector.

The public expects good governance, but with less government. Over the last decade this trend has been clear in most societies. Public service functions have been placed in private hands, outsourced through contracting. National bureaucracies have been trimmed into lean, no slack machineries. Mandates for sector oversight rather than for delivery responsibilities have been prioritised. In the name of effective governing, parliaments have reduced the built-in redundancies often linked to previously-prioritised national defence concerns. One result of these efficiency reforms has been that public authorities in emergencies command fewer resources and less skilled manpower relevant to ensuring societal security.[13]

In the same way as industry during the Cold War was strongly motivated to support national defence in the face of an armed attack, one must now stimulate businesses to contribute to a hardening of those high-risk infrastructure complexities that are critical to the functionality of society. Efforts must be directed towards both preventive measures and preparedness to cope and recover, whenever various intentional or accidental hazards occur.[14]

Since many of the public services that can prove critical for societal security moved into private hands for reasons of more efficient government, questions arise regarding dependencies across the public-private gap. Can this interaction be seen as a relationship of mutually beneficial dependency? Or, do asymmetrical vulnerabilities exist that can form the basis for influence and manipulation by one of the parties? Private-public partnerships need to be developed in many sectors.[15] Societal security includes the ability to recover from a dramatic threat or a systemic breakdown. Questions of accountability must be clarified prior to a crisis resulting in the painful blame-game dynamics.[16] In this post-trauma phase the private sector is an important ally or foe to those with authority and responsibility to safeguard the security of the nation and its citizens.

Infrastructure failures, such as power outages, can directly cause considerable harm. In addition, they generate second and third order consequences of often even greater and enduring harm to society. In a blackout, like in New York in August 2003, numerous services were interrupted.[17] For this reason hospitals and other emergency installations keep backup systems. Still, most basic functions of society are not covered in this way due to cost limitations. Infectious diseases can spread across populations and demands for vaccinations, for isolating the infected, and for controlled hospital care often rise very quickly.[18] Cascading effects evolve in uncontrollable ways when some dormant risk contingency suddenly becomes a reality.

In an urban heat wave, as in Paris during the summer of 2003, thousands of very young and elderly people died due to inadequate planning for such a contingency.[19] This consequence generated widespread public criticism at the health services and indirectly at the public officials responsible for providing adequate services. Political accountability was being manifested for the human consequences of a lack of preparations for an extreme weather situation. The Spanish government was held responsible for its misdirected labelling of the culprits of the terrorist train bombings in March 2004 in the national elections. The consequences of this election victory for the social democratic opposition have so far been significant for Spain, for the war in Iraq, and for the evolving European Union. The effects of crises cascade beyond the events themselves in unpredictable ways.

It is not only how you act, but also the appearance of what you do or do not do that leaves an imprint in the public mind.[20] The importance of mass media has been widely highlighted in the processes of framing public issues, building expectations, placing blame, and in shaping composite images of leader success or failure in the face of security threats. George W. Bush became President after a narrow majority vote of the U.S. Supreme Court. He became the President of the American people in the shadow of his public leadership during the dramatic events of 9/11. The Spanish Prime Minister lost the parliamentary election immediately following the Madrid terrorist bombings. This political defeat was in part caused by the image of manipulation and misdirected blaming that the media transmitted to the Spanish public.

The presence of media increases pressures on high stakes decision-making, when facing threats to societal security. Deadlines for action are not only set by the situation at hand, but time parameters are equally determined by media demands for news at certain intervals. A lack of newsworthy information in a timely manner can lead to difficulties to handle media probes inside an organisation. Considerations of how to communicate actions or inactions through media become as important to success as calculations over what to do and what to avoid in certain consequential situations.[21]

Trans-national media coverage increases with advances in communications technology. Local events can blow up into global concerns, when for example CNN makes an editorial decision to focus its interest upon a given situation. Such up-scaling of attention may occur rapidly and add to the pressures of local authorities in an already difficult situation. Few national or local officials are prepared to deal with the demands of the international media corporations.[22]

Public expectations of government performance remain high in the face of a wide spectrum of threats to state security and to individual safety. At the same time, the available resources under the direct command of national public authority to meet such threats have been redefined and often reduced in scope and magnitude. This deficiency has not yet been compensated for by enhanced multinational capacities. In spite of a general awareness of the importance of pooling resources internationally when confronting trans-national threats, little added value in terms of tangible resources is yet generated from such cooperation. Statements of solidarity have been combined with ad hoc arrangements for mutual assistance when large-scale disruptions of societies have occurred. The governing structures for handling threats to embedded societal security are still national in focus. The potentially great resource mobilization possible through, for example, implementing the Solidarity Clause has so far been untapped.

The mental maps of European security elites were fixed by the Cold War and had to undergo a rather difficult and painful redirection over the last ten years. The mental scrap (not the metal scrap – it is also a problem) from the Cold War is still influencing security thinking in European and North American ministries. Unlearning of obsolete mindsets is needed in addition to some new learning about the types of security challenges reviewed above.[23]

It is important that the EU is not only inter-operative in technology and communications when assisting each other in emergencies. We need to be inter-operative when it comes to understandings and knowledge as well. We need shared bench marking for good performance, not so good performance, and best practices. One vital resource in that cumulative effort is expertise and organisational capacity. We should think about interoperability in terms of shared knowledge as well as a common training base for joint efforts.

Considerable research is conducted on the new security issues in many countries.[24] There is a wealth of observations, generalisations, and lessons. It is important that the understandings formed through this effort are being transferred from the ivory towers and think-tanks to facilitate organisational learning. A distinction can be made between organisational learning and individual learning. We can hopefully learn as individuals, but can public organisations learn? Or do government agencies merely change and adapt to circumstances? Can they learn in a cumulative way, i.e. that they add to their knowledge base and expand their repertoire? Learning is a complex matter when you move beyond individual learning to collective and organisational learning. This is a huge subject for academic debate and institutional design proposals.[25]

It is important to build knowledge about societal security in all EU countries, as an analytical underpinning for the implementation of the Solidarity Clause. New requirements are levied on think-tanks to develop such knowledge in partnership with policy agencies and operatives. One needs knowledge about security threats and strategies that is both based on scientific research and on practical experience. Such centres of knowledge production and transfer need to be linked in trans-national and co-operative networks. This knowledge-building enterprise should extend across the Atlantic as well as to other global centres.

Domains of Societal Security

How do governments organize their professional corps to meet the security challenges of the 21st century? Fundamental changes are underway throughout Europe as well as in North America. The prospects for policy diffusion, mutual learning, and institutional adaptation are very real. In the EU, one speaks of the Europeanization of national structures and procedures also in the area of defence and security.[26] Similarly, mutual learning or adaptation across the Atlantic is most likely.

Figure 1 gives the traditional two-track professional approach to state security and human safety. This format has been used in Sweden and in many other nations. Different parts of the government machinery have responsibility for and authority to enhance the security of the state and to protect the safety of citizens. A sharp dividing line has been upheld between these two spheres of authority in many countries. Distinct professions have developed with separate training programs, rules of engagement, and operational practices.

Objective	*Domain:*	
	Domestic Sphere	*International Sphere*
State Security	Law & Order	National Defence
Human Safety	Rescue Services	International Disaster Assistance

Figure 1: Concepts and Domains of European Security.

Similarly, a dividing line has been upheld between the concerns of the domestic sphere and the responsibilities focused toward the international setting. State security at home has been the responsibility of the criminal justice system and special counter-intelligence services. The defence sector has focused on mobilizing resources against overt external threats to state security. The Constitutions of many governments reinforce this separation between the spheres of enhancing state security from external threats and from domestic upheaval or penetrations. For the safety track, rescue services have been built at home. These national assets are also used for international disaster assistance. Such humanitarian operations are distinct from the international focus of the defence sector. In both tracks, collaboration with partners or allies abroad is well developed.

Figure 2 gives the more recently evolving Nordic three-track approach, where societal security becomes the core of the national mobilization of resources. Several elements that traditionally have been kept apart are becoming fused; procedures for war and peace merge, internal and external security are interlocked, and the ambitions of enhancing state security and providing citizen safety become blurred. This holistic approach, that places societal security at the core, is also manifested in the Solidarity Clause of the Constitution of the European Union as adopted by the European Council in June 2004.

Objective	*Domain*:	
	Domestic Sphere	*International Sphere*
State Security	Law & Order	National Defence
Societal Security	*CM Capacity*	*International CM Capacity*
Human Safety	Rescue Services	International Disaster Assistance

Figure 2: Concepts and Domains of Emerging European Societal Security.

Different parts of the EU machinery have primary responsibility for the six domains in Figure 2. The societal security track bridges the conceptual and professional gap between the high politics concern with security in terms of the Union as a state-writ-large, and, on the other hand, the more network-based focus on the safety of humans inside and outside of the Union. In this bridging perspective, priority tasks for a secure community of twenty-five would be to safeguard the functionality of civil societies and the capacity for democratic governance.

Without a holistic perspective on the totality of EU engagements on behalf of security and safety inside and outside the borders of the Union, the six distinct policy domains in Figure 2 would fragmentize into isolated spheres of professional, sector interests. Also, setting resource priorities across these operative spheres is only politically manageable with a holistic conceptualisation that spans across the domains into an overall societal security paradigm for the Union and its component member states.

In Figure 3 an additional EU domain is added in between the domestic sphere and the international setting. In the *intermestic sphere*, the necessary trans-boundary linkages across the domestic and the international levels are highlighted. Drawing on the discussion of trends affecting embedded societal security in the previous section, it is clear that this intermestic sphere is an important security domain for the Union. Its importance is symbolized in the Solidarity Clause of the proposed Constitution. In this statement of a common political commitment to embedded societal security, both a concern with state security and the requirements of human safety are included. The solidarity pledge cuts across these distinct professional tracks and it fuses the domestic-international nexus. The intermestic domain becomes a primary playing field for the pursuit of societal security in and by the Union.

Objective	*Domain:*		
	Domestic Sphere	*Intermestic Sphere*	*International Sphere*
State Security	Law & Order	*Counter- terrorism*	National Defence
Societal Security	*CM Capacity*	*Solidarity Clause*	*International CM Capacity*
Human Safety	Rescue Services	*Civil Protection*	International Disaster Assistance

Figure 3: Concepts and Domains of European Embedded Societal Security.

Embedded societal security has to be multi-sector. There has to be safety and security cooperation and preparation in and between, for example, the health, financial, food, or transportation sectors. It has to be multi-level. The consequences of various threats have to be managed and prepared for at all levels. Responsibilities range from the local, regional, national, and across borders to the European level. The shared perspective has to be multi-institutional and tri-pillar. The EU Commission (also among the directorates), the Council, the Parliament, and many autonomous EU agencies have to be involved and be able to cooperate. Societal security has to be conceived of as a multi-national concern. 25 member states plus the institutional complex in Brussels must develop a common outlook. Organisational relationships need to be designed and tested in support of a secure European Union.

Toward Embedded Societal Security across the Atlantic

Yet, preparations for European societal security cannot be conducted in splendid isolation. This demanding collaborative effort must be multi-continental in approach in order to be effective. The societal security paradigm must bridge across the Atlantic to the USA, as well as to other global partners. Steps can be taken to transform the existing, alliance based Atlantic security community into a secure trans-Atlantic Societal Security Community. The question remains how to link the novel European notion of embedded societal security with the US Homeland Security program?

European societal security, like Homeland Security in North America, concerns survival in several dimensions. In this high-stakes challenge, there is every reason to begin the difficult process of moving different conceptualizations of security closer to a more practically focused working partnership. When we know more about others' preferred arrangements, we also know better where we can find commonalities and where hard choices have to be made in order to reach a common good. It is hoped that this brief on the notion of embedded societal security can contribute to such a common outlook. The analytical work should now be initiated for drafting a concrete blueprint for the implementation of the novel ideas that were expressed through the political pledge of the EU Solidarity Clause, concerning security and safety at home, abroad and in-between.

The US Homeland Security program needs to be matched with the programs of numerous and distinct European national systems and, in addition, with the Brussels-based arrangements. All these parts are very much in a formative phase, even though their departure point has been the spectrum of security threats that was surveyed earlier in this brief. One trans-Atlantic vision could be an extended form of Homeland Security built on numerous bilateral arrangements, much like the negotiated deals for US military bases around the world. The Western intelligence regime is constructed through such bilateral links with Washington at the core of the information wheel. This US-led arrangement has worked well and discreetly for decades, for its defence related purpose.

Another vision would be a multilateral partnership between a US government that appreciates its "outland" vulnerabilities in matters of homeland security and a coherent EU policy for embedded societal security. The shared political agenda would then be to create several working-level multilateral processes to transform the existing Atlantic alliance into a secure Euro-Atlantic community. Practical measures towards this end should be undertaken at several levels and in many sectors. Working teams should be established to prepare for common outlooks among relevant officials. Policy pledges for enhanced partnerships must penetrate downstream into the operational settings of the many institutionalised stakeholders of the societal security sphere. Organisational and mental barriers must be overcome across jurisdictional, sector-based and professional boundaries.

One cost effective means to open up entrenched rigidities would be to plan and execute several interactive training workshops. Responsible policy makers and elected officials from several nations would in workshop settings deal intensively with some scenario-based trans-Atlantic threat situation. A shared contingency awareness and a mutual learning process would develop through such experiences with concrete decisional security dilemmas. An excellent example of such learning tool was the *Atlantic Storm* simulation that was conducted in Washington on January 14, 2005. The scenario-based game engaged prominent former statesmen and active policy shapers from a sample of European governments and from North America. The lessons learned from this exercise were widely noted in media.[27] The format was tested in March by members of the new House Homeland Security Committee of the US Congress. Similar multilateral workshops ought to be convened in Europe.

Enhanced societal security across the Atlantic could become a core mission for the future work of NATO and the wider Partnership for Peace community. The Nordic nations together with the USA could offer a lead in developing such a Partnership for Training within the PFP. Such a working agenda would serve to link together the rapidly evolving programs for societal security in and of the EU and the primarily inward looking dynamics of the massive US investment in institutions and policies for Homeland Security.

Notes:

[1] Dan Hansén and Ahn-Za Hagström, *I krisen prövas ordningsmakten* (Stockholm: Jure, 2004).

[2] Alex P. Schmid and Ronald D. Crelinsten, eds., *Western Responses to Terrorism* (London: Frank Cass, 1993).

[3] Ulrika Mörth and Bengt Sundelius, *Interdependens, konflikt och säkerhetspolitik: Sverige och den amerikanska teknikexportkontrollen* (Stockholm: Nerenius & Santérus, 1998).

[4] Michael Erbscholoe and John R. Vacca, *Information Warfare: Combat Hackers and Cyber Attackers* (Berkeley, California: Osborne McGraw-Hill, 2001); Chris C. Demchak, “New Security in Cyberspace: Emerging Intersection between Military and Civilian Contingencies,” *Journal of Contingencies and Crisis Management* 7, no. 4 (December 1999): 181-198.

[5] Barry Turner and Nick Pidgeon, *Man-made Disasters*, 2nd Edition (Oxford: Butterworth-Heinemann, 1997).

[6] Bengt Sundelius and Jesper Grönvall, “Strategic Dilemmas of Bio-security in the European Union,” *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science* 2, no. 1 (2004); Jesper Grönvall, *Managing Crisis in the European Union: The Commission and Mad Cow Disease*, Volume 10, Crismart, The Swedish Agency for Civil Emergency Planning (Karlstad: Tryckeri AB Knappen, 2000).

[7] Paul ‘t Hart “Symbols, Rituals and Power: The Lost Dimensions of Crisis Management,” *Journal of Contingencies and Crisis Management* 1, no. 1 (1993): 36-50.

[8] Barry Buzan, *People, States and Fear: The National Security Problem in International Relations* (Brighton: Wheatsheaf, 1983).

[9] The SARS Commission Interim Report – *SARS and Public Health in Ontario* (Ministry of Health and Long-Term Care, 15 April 2004), <http://www.fas.org/irp/threat/cbw/sars-ontario.pdf > (14 July 2005).

[10] Eric K. Stern, *Crisis Decision Making: A Cognitive Institutional Approach* (Stockholm: Försvarshögskolan, 2001); A. Libertore "Chernobyl Comes to Italy: The Reciprocal Relationships of Radiation Experts, Government Policies, and the Media," in *The Politics of Expert Advice: Creating, Using and Manipulating Scientific Knowledge for Public Policy,* ed. Anthony Barker and B. Guy Peters (Edinburgh: The University of Edinburgh Press, 1993), 33-48.

[11] Charles Perrow, *Normal Accidents: Living with High-Risks* (Princeton, NJ: Princeton University Press, 1999); Edward Deverell, *The 2001 Kista Blackout: Corporate Crisis and Urban Contingency* (Stockholm: Swedish National Defence College, 2003); Lindy Newlove, Eric K. Stern, and Lina Svedin, *Auckland Unplugged: Coping with Critical Infrastructure Failure* (Baltimore: Lexington Books, 2003).

[12] Scott D. Sagan, *The Limits of Safety: Organizations, Accidents and Nuclear Weapons* (Princeton: Princeton University Press, 1993); Philippe Boullé, Luc Vrolijks, and Elina Palm, "Vulnerability Reduction for Sustainable Urban Development," *Journal of Contingencies & Crisis Management* 5, no. 3 (1997): 179-188.

[13] Peter Aucoin, *The New Public Management: Canada in Comparative Perspective.* (Montreal, Quebec, Canada: Institute for Research on Public Policy, 1995); Lynn Ashburner, Ewan Ferlie, Louise Fitzgerald, and Andrew Pettigrew, *The New Public Management in Action* (Oxford: Oxford University Press, 1996); Jan-Erik Lane, *The New Public Management* (London: Routledge, 2000); Donald F. Kettl, "The Transformation of Governance: Globalization, Devolution, and the Role of Government," *Public Administration Review* 60, no. 6 (2000):488-97.

[14] Robert Agranoff and Michael McGuire, "Managing in Network Settings," *Policy Studies Review* 16, no. 1 (1999): 18-41; Myrna P. Mandell, "Collaboration through Network Structures for Community Building Efforts," *National Civic Review* 90, no. 3 (2001): 279-87.

[15] Akintola Akintoye, Matthias Beck, and Cliff Hardcastle, eds., *Public-private Partnerships: Managing Risks and Opportunities* (Oxford: Blackwell Science, 2003).

[16] Thomas Preston and Paul 't Hart, "Understanding and Evaluating Bureaucratic Politics: The Nexus Between Political Leaders and Advisory Systems," *Political Psychology* 20, no. 1 (1999): 49-98; Uriel Rosenthal, Paul 't Hart, and Alexander Kouzmin, "The Bureau-politics of Crisis Management," *Public Administration* 69, no. 2 (1991): 211-233.

[17] Interim Report: *Causes of the August 14th Blackout in the United States and Canada* (US-Canada Power Systems Outage Task Force, November 2003) <https://reports.energy.gov/814BlackoutReport.pdf> (15 July 2005).

[18] Thomas A. Glass and Monica Schoch-Spana, "Bioterrorism and the People: How to Vaccinate a City Against Panic," in *Clinical Infectious Diseases* 34, no. 2 (2002): 217-23.

[19] Abstract of the progress report – August 28th on the heatwave 2003 in France from the National Institute of Public Health Surveillance (InVS), Saint Maurice, France, <www.invs.sante.fr/publications/2003/chaleur_aout_2003/abstract_heatwave_280803.pdf> (15 July 2005).

[20] Murray J. Edelman, *Constructing the Political Spectacle* (Chicago: Chicago University Press, 1988).

[21] Patrick Lagadec, *Preventing Chaos in a Crisis. Strategies for Prevention, Control and Damage Limitation* (London: McGraw-Hill Book Company, 1991); Ardyth B. Sohn, Jan LeBlanc Wicks, Stephen Lacy, and George Sylvie, *Media Management: A Casebook Approach*, Second Edition (Mahwah, N.J.: Lawrence Erlbaum Associates, Inc., 1999).

[22] Rhona H. Flin and Kevin Arbuthnot, eds., *Incident Command: Tales from the Hot Seat* (Aldershot: Ashgate Publishing Company, 2002); Robert Heath, *Crisis Management for Managers and Executives* (London/San Francisco: Financial Times Pitman Publishing, 1998).

[23] Yaacov Y.I. Vertzberger, *The World in Their Minds: Information Processing, Cognition, and Perception in Foreign Policy Decision Making* (Stanford, California: Stanford University Press, 1990); James G. March, *A Primer on Decision Making. How Decisions Happen* (New York: The Free Press, 1994); Richard E. Neustadt and Ernest R. May, *Thinking in Time. The Uses of History for Decision-Makers* (New York: The Free Press, 1986).

[24] Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, Colorado : Lynne Rienner Publishers, 1998); Uriel Rosenthal, Arjen Boin, and Louise K. Comfort, eds., *Managing Crises: Threats, Dilemmas, Opportunities* (Springfield, Illinois, USA: Charles C. Thomas Publishers, 2001); Robert Mandel, *Deadly Transfers and the Global Playground: Transnational Security Threats in a Disorderly World* (London: Praeger Publishers, 1999); Simon Duke, *The EU and Crisis Management : Development and Prospects* (Maastricht : European Institute of Public Administration, 2002).

[25] Sander Dekker and Dan Hansén, “Learning under Pressure: The Effects of Politicization on Organizational Learning in Public Bureaucracies,” *Journal of Public Administration Research and Theory* 14, no. 2 (2004): 211-230; Eric K. Stern, “Crisis and Learning: A Conceptual Balance Sheet,” *Journal of Contingencies and Crisis Management* 5, no. 2 (1997):69-86.

[26] Magnus Ekengren, *The Time of European Governance* (Manchester: Manchester University Press, 2002); Alyson J.K. Bailes, ed., *The Nordic Countries and the European Security and Defence Policy* (Oxford: Oxford University Press, 2005).

[27] Daniel Hamilton and Tara O’Toole, “Facing up to the Bioterror Threat,” *International Herald Tribune*, 31 January 2005.

BENGT SUNDELIUS is Professor of Government at Uppsala University and the founding Director of the National Centre for Crisis Management Research and Training (CRISMART) of the Swedish National Defence College. He is Chief Scientist of the Swedish Emergency Management Agency promoting research in the area of homeland security. His most recent book is *The Politics of Crisis Management* (Cambridge University Press, 2005). *E-mail*: bengt.sundelius@fhs.mil.se.