Transforming Homeland Security: U.S. and European Approaches

Esther Brimmer, Editor

Brimmer, Esther, editor. *Transforming Homeland Security: U.S. and European Approaches* (Washington, DC: Center for Transatlantic Relations, 2006).

© Center for Transatlantic Relations, 2006

Center for Transatlantic Relations
The Paul H. Nitze School of Advanced International Studies
The Johns Hopkins University
1717 Massachusetts Ave., NW, Suite 525
Washington, D.C. 20036
Tel: 202-663-5880
Fax: 202-663-5879
Email: transatlantic@jhu.edu
http://transatlantic.sais-jhu.edu

ISBN 0-9766434-4-8

Cover photograph: "Pristina Sport Palace on Fire—COMKFOR Gen. Reinhardt and U.N. Fire Chief Robert Triozzi." KFOR Photos. Available at http://www.nato.int/kfor/multimedia/photos/2000/lr/pic00024_lr.jpg

Table of Contents

Acknowledgements v

Preface vii
Esther Brimmer

Introduction: Transforming Homeland Security: A Road Map for the Transatlantic Alliance ix
Daniel S. Hamilton

Implications of Homeland Security for Rethinking Transatlantic Security

Chapter 1
Homeland Security and Transformation: Why It Is Essential to Bring Together Both Agendas 3
Heiko Borchert

Chapter 2
From Territorial Security to Societal Security: Implications for the Transatlantic Strategic Outlook 23
Esther Brimmer

Chapter 3
Transatlantic Homeland Security and the Challenge of Diverging Risk Perceptions 43
Gerd Föhrenbach

Transatlantic Cooperation on Homeland Security: What Do We Need to Do? What Do We Need to Do Together?

Chapter 4
The Concept of Homeland Security in the European Union and in Austria—A challenge for the Austrian EU presidency 59
Gustav Gustenau

Chapter 5
What Does the United States Need to Do? The United States and Homeland Security 81
Lawrence J. Korb

Chapter 6
Structures and Cultures—Civil Military Cooperation in Homeland Security: The Danish Case 95
Anja Dalgaard-Nielsen

Chapter 7
The EU's Approach to Homeland Security: Balancing Safety and European Ideals 115
Gustav Lindstrom

Connecting Key Capacities

Chapter 8
Defending Critical Infrastructure and Systems 133
Sandra J. Bell

Chapter 9
Intelligence Cooperation and Homeland Security 153
Yves Boyer

Chapter 10
Homeland Security and the Role of Business 163
Pauline Neville-Jones and Neil Fisher

About the Authors 171

Acknowledgements

This book results from collaboration among the Center for Transatlantic Relations at the Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (CTR), the Politisch-Militärische Gesellschaft (PMG), and the Danish Institute for International Studies (DIIS). CTR would like to thank its partners for their support and dynamic and effective cooperation throughout the project. In particular, we would like to thank Col. Ralph Thiele, Dr. Heiko Borchert, and Dr. Anja Dalgaard-Nielsen. We convened two meetings of the authors and other experts, one in Berlin in September 2005 and one in Washington, DC, in November 2005. We would like to thank Katrien Maes and Jeanette Murphy at the Center for Transatlantic Relations and Anna Sturm at the Politisch-Militärische Gesellschaft for their help organizing the authors' meetings and Carrie Schenkel and Medlir Mema, also of CTR, for their help with the text and charts. The project was kindly supported by the Transatlantic Program of the Federal Republic of Germany with funds of the European Recovery Program of the Federal Ministry of Economics and Technology (BMWI). We also want to acknowledge support from the European Commission and the EU Center of Excellence Washington DC.

The Center for Transatlantic Relations will continue to address these issues as part of the newly formed Johns Hopkins University-led National Center for the Study of Preparedness and Catastrophic Event Response (PACER), a research consortium created by the United States Department of Homeland Security.

Each author writes in his or her personal capacity. The views expressed are their own and not those of their institutions.

Esther Brimmer

Preface

Many countries are considering how to reorganize civilian and military resources to meet the challenges of "homeland security." The issues raised are diverse and complex, ranging from infrastructure protection to social cohesion to the role of the military in a democratic society. This book was conceived as an examination of various approaches to these topics. The project took on added urgency as authors wrote in the aftermath of Hurricane Katrina, which struck the United States in August 2005.

Esther Brimmer

Introduction: Transforming Homeland Security: A Road Map for the Transatlantic Alliance

Daniel S. Hamilton

This volume addresses the need for the United States and Europe to transform their respective approaches to homeland security in ways that are more attuned to 21st century challenges. Effective homeland security may begin at home, but in an age of catastrophic terrorism no nation is home alone. If Europeans and Americans are to be safer than they are today, individual national efforts must be aligned with more effective transatlantic cooperation.

While there has been no effort to force consensus among the authors in this volume, a basic theme does connect the various contributions: if the U.S. and its partners are to protect their societies more effectively, they must go beyond piecemeal extensions of current policies. They must better understand and seek to bridge differing approaches on each side of the Atlantic; better understand what they are protecting; transform public-private and civil-military relationships; adopt network-centric approaches; and include homeland security as a high profile mission of key institutions and transatlantic mechanisms. This chapter seeks to extract from the various contributions lessons of relevance to policymakers and practitioners on both sides of the Atlantic.

Overcoming Some Hurdles

If Europe and the United States are to "transform" their respective approaches to homeland security and chart some type of common path together, they first need to understand better the different paths each has been on until now. Six issues have consistently plagued transatlantic cooperation.

Definitional debates

Just as the American term "homeland security" is largely unfamiliar to many Europeans, most Americans are unfamiliar with European concepts such as "resilience" or "societal security," or with experiences Europeans have gained from combating domestic terrorism. Americans tend to focus on the anti-terrorist elements of "homeland security," whereas Europeans tend to focus on the civilian emergency response or law enforcement elements of "societal security." Over the past few years each side has become more attuned to the concerns of the other, but when Europeans and Americans meet they still tend to get lost in definitional debates.

Homeland security has been advanced in the United States as a systematic attempt to reduce society's vulnerabilities and to build capabilities to deal with massive terrorist strikes, should they occur. Although U.S. emergency planners have experience with "all-hazard" approaches to threat and risk, between September 2001 and September 2005 homeland security came to be associated more narrowly with the anti-terrorist campaign. Homeland security is even defined in the U.S. National Strategy for Homeland Security as "a concerted national effort to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[1] In sum, American homeland security is widely conceived as a broad-based effort to prevent, protect, respond and recover from terror—an effort involving multiple actors, covering numerous societal sectors and professions, and many levels of government.

In September 2005, Hurricane Katrina demonstrated forcefully that not all homeland security challenges stem from terrorism, and exposed dysfunctional response and recovery systems at every level of government. It remains unclear, however, whether the failure to cope with the devastation wrought by this natural disaster will prompt an adequate retooling of homeland security approaches.

In Europe there is no generally accepted definition of the term homeland security. Whereas U.S. homeland security has been driven by the counterterrorist agenda, European efforts to protect society

[1] *National Strategy for Homeland Security*, Office of Homeland Security, Washington, DC July 2003, p. 2.

have derived largely from civilian emergency response communities working with domestic law enforcement agencies. In this volume, Gustav Gustenau attempts a "European" definition of homeland security. He describes it as an interagency approach to protecting society that integrates public and private participants and is based on a comprehensive concept of security encompassing naturally occurring dangers as well as the threat of terrorism. He identifies various homeland security areas and tasks, all of which would resonate with Americans, such as intelligence services and early warning; security of borders and transport; anti-terror measures, including defense against catastrophic terrorist attacks; protection of critical infrastructure; and reaction and aid in the case of natural disasters.

There is as yet no Europe-wide consensus on such a "homeland security" definition, however, much less a common agenda. Nonetheless, some individual European nations have developed frameworks for societal protection that could serve as useful references for U.S. efforts, and perhaps offer a basis for more effective transatlantic cooperation. These are discussed later in this chapter.

Differences in risk perception

Different understandings of tasks are compounded by different perceptions of risks. As Gerd Föhrenbach explains, most Europeans feel significantly less threatened than Americans—despite incontrovertible evidence that Europe is both a base for and a target of international terrorism. Risk perceptions also vary within Europe itself. Many in Europe and not a few in the United States view the 9/11 attacks as isolated incidents. Some in Europe also see terrorism as principally America's problem, one they believe the Bush Administration has exacerbated through its own actions, particularly the war in Iraq. Some see the subsequent Madrid and London attacks through the same perspective—nations were attacked that joined the Americans in the Iraqi war. It is important to note that European governments promptly rejected Osama bin Laden's offer of immunity to any country that would pull its troops out of the Middle East, and that Europe and the United States are working closely to deal with terrorism. But there is still appeal in policies that demonstrate distance from Washington. These divergent risk perceptions tear at both transatlantic partnership and EU solidarity.

War and peace or crime and justice?

Whereas U.S. efforts represent a radical break with traditional American approaches to security and reflect a tendency to characterize the issue as one of war and peace, initial European efforts represented an extension of previous efforts to combat terrorism and reflect a tendency to characterize the issue as one of crime and justice.

During the 20th century Americans thought of "national" security as something to be advanced far from American shores. The United States invested massively to project power quickly and decisively to any point on the globe, and invested meagerly to protect Americans at home. September 11 shattered that perspective. Now, Americans share a strange sense that they are both uniquely powerful and uniquely vulnerable. Partisan divisions within the United States are fierce, but they obscure a deeper consensus that the threat of WMD terrorism warrants a reframing of U.S. foreign and domestic policies. Americans disagree intensely whether the U.S. should have invaded Iraq. They disagree over the degree to which public security efforts may intrude on personal liberties. But most agree that America is engaged in a global war on terrorism. And most are willing to project American power abroad to "win" that war.[2] They are far more receptive to radical breaks with traditional thinking, far more inclined to support crash efforts to protect the homeland, and far less concerned with breaking diplomatic crockery along the way.

In the name of this "war" on terror the Bush Administration has justified a number of extraordinary actions, including spying on U.S. citizens without court warrants, the practice of rendition, and detaining terrorist suspects as "enemy combatants" beyond the jurisdiction of domestic or international law. These are controversial in the United States as well as abroad, and have hampered international cooperation even with America's closest allies.

Just as Americans have sought to understand the consequences of September 11 within the context of their own national experience, European views have been colored by the kind of domestic terrorism

[2] For more on these developments, see Daniel S. Hamilton, "Transatlantic Societal Security: A new paradigm for a new era," in Anja Dalgaard-Nielsen and Daniel S. Hamilton, *Transatlantic Homeland Security* (London: Routledge, 2006), pp. 172-196; "One nation after all," *The Economist*, September 11, 2004, p. 32.

that has confronted them for the past three decades. During that period, more than 5,000 lives were lost to terrorism in Britain, Ireland, and Spain alone. Whereas U.S. officials are suddenly haunted by the prospect of further—and perhaps even more catastrophic—attacks, European officials have long been taunted by domestic terrorists, who have argued that a government's own zeal to apprehend terrorists would lead it to subvert the very rules of the open society it sought to protect. A number of European countries have adopted laws to confront domestic terrorism while preserving civil liberties. Of course, there are differences within Europe as well, which make generalizations difficult. Recent British anti-terror laws, for instance, go even further than some U.S. efforts.

These perspectives influence the way in which each side has addressed the threat. Whereas the homeland security effort in the U.S. has been waged with the rhetoric of war, such efforts in Europe have been viewed largely through the perspective of crime. Most Europeans view terrorism itself as a tactic rather than an enemy. These differing perspectives complicate transatlantic cooperation: American critics charge Europeans with complacency, while European critics accuse Americans of extremism.

"Pushing borders out" or pulling together at home?

Activist U.S. efforts to "externalize" homeland security have often overwhelmed European partners, who are concerned about the legal ramifications of such approaches or are focused primarily on issues of internal coordination

Despite the impact of September 11 on the United States, the natural instinct in a nation bounded by two oceans is still to fight one's enemies abroad so one doesn't need to fight them at home. Washington's "forward defense" mentality, which exerts such a pervasive influence over the U.S. military, is also being applied to homeland security. The result has been a series of U.S. efforts to "externalize" homeland security by "pushing borders out"—essentially to move the focus of the anti-terrorism campaign abroad.

Aspects of this effort are controversial and problematic for transatlantic relations, for instance the Bush Administration's attempts to justify its war in Iraq through its war on terrorism; the notion enshrined

in the Patriot Act that non-citizens have fewer rights to privacy and due process than U.S. citizens; or the "Guantanomo" practice of holding non-citizens indefinitely outside the jurisdiction of U.S. courts and without status in either domestic or international law. Tremendous European goodwill towards the U.S. after 9/11 has essentially been squandered by various manifestations of the externalization policy. It is important to note that much of the Guantanamo system remains controversial in the U.S. itself, and is currently under review by the courts.

Other "externalization" initiatives have simply caught European partners flatfooted, since such initiatives either require greater coherence among EU member states than they have been able to muster on such issues as customs, or collide with prevailing European regulations, for instance regarding data privacy.

Despite these difficulties, in select areas "externalization" has formed the basis for practical transatlantic agreements. Such U.S.-led initiatives as the Proliferation Security Initiative, the Container Security Initiative, Operation Safe Commerce or the Customs-Trade Partnership Against Terrorism (C-TPAT)[3] are all examples of "pushing borders out" in ways that have included European partners. The basic premise should be acceptable: it is safer to interdict potentially nasty people or items before they ever reach one's territory rather than trying to find them once they've arrived, even while safeguarding the free flow of people, goods and ideas upon which open societies depend. But "pushing borders out" will require unprecedented international cooperation tied to a major transformation of national cus-

[3] For details on the Proliferation Security Initiative, see the U.S. Department of State fact sheet at http://www.state.gov/t/np/rls/other/46858.htm. For information on C-TPAT see http://www.customs.treas.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf. For a description of the Container Security Initiative, see http://en.wikipedia.org/wiki/Container_Security_Initiative. Operation Safe Commerce builds on C-TPAT and CSI by (1) building a greater understanding of vulnerabilities within global supply chains, and (2) ensuring that new technologies and business practices designed to enhance container security are both commercially viable and successful. For a critique of some of these efforts, see Stephen Flynn, "Addressing the Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative," Testimony before a hearing of the Permanent Sub-Committee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate May 26, 2005, available at http://www.cfr.org/publication/8141/addressing_the_shortcomings_of_the_customstrade_partnership_against_terrorism_ctpat_and_the_container_security_initiative.html

toms and immigration agencies into the equivalent of diplomatic services. The resource implications are serious, and as indicated there is potential for abuse—such as conflating anti-terrorist efforts with immigration control efforts in ways that might lead to serious violations of human rights; or paying inadequate attention to the international legal ramifications of extraterritorial initiatives.[4] Moreover, such efforts may be self-defeating unless they establish a level playing field for all stakeholders. But the core principle offers important insights into new forms of international collaboration.

Organizational incoherence

Neither the United States nor Europe is yet well organized to advance an effective homeland security effort. The different "homeland security" mechanisms set in place in Europe and the United States have each complicated transatlantic cooperation.

The Bush Administration's immediate homeland security response—a scattershot burst of urgent domestic initiatives, with little effort at prioritization or consideration of their international impact—has given way to the most extensive reorganization of federal agencies since the end of World War II. Much effort has been consumed by bureaucratic turf wars. The Department of Homeland Security lacks the type of authority over U.S. intelligence agencies that would enable it to help shape intelligence collection priorities, the international dimension of its activities continues to be weak, and its relationship with the Defense Department remains murky. Hurricane Katrina exposed major weaknesses in the Department's prevention, response and recovery capabilities. The Bush Administration's approach to homeland security has represented little more an aggregation of discrete elements, ranging from counterterrorist intelligence, border security, risk management and cargo screening to health and other issues. The sum is less than the parts, and many parts are still moving to their own beat. For most of these missions, the bipartisan 9/11 Commission Public Discourse Project in December 2005 gave the Administration failing grades.[5]

---

[4] For a critique, see Tom Barry, "Pushing Our Borders Out," http://americas.irc-online.org/pdf/briefs/0502immigration.pdf

[5] 9/11 Public Discourse Project, *Final Report on 9/11 Commission Recommendations*, December 2005, available at www.9-11pdp.org.

U.S. efforts are matched by a byzantine collection of efforts on the other side of the Atlantic. The European Union, having expanded to twenty-five nations, must now address the domestic security needs of 456 million people, with more to come in the next few years. But as Gustav Lindstrom and Gustav Gustenau explain, the EU is not a federal state and its powers cannot be compared directly to those of the United States. Preventive and protective efforts still consist of a patchwork of contributions by the EU, its member states, and individual ministries, agencies, and services within those states. Links to non-EU members are uneven. Civil protection remains primarily the preserve of member states, and there are major turf wars between the European Commission and the European Council. There is no European "Minister for Homeland Security" available to the U.S. Secretary of Homeland Security. The EU Coordinator for Counterterrorism, appointed for the first time in the spring of 2004, has neither line authority over Commission bureaucrats or member state agencies, nor a significant budget to promote harmonization of policies, procedures, standards, or equipment, which vary widely across member states. He cannot prescribe; he can only persuade. He reports to the High Representative for Foreign and Security Policy in the European Council, and thus is of a lower level than the U.S. Secretary, and works out of the European Council rather than the European Commission, and so only has a small staff at his disposal. In the meantime, the EU suffers gaps in intelligence sharing, and interoperability between the police, judicial and intelligence services is questionable. SitCen, the center for intelligence in the Council Secretariat, analyzes information, but operational work remains the exclusive competence of the national security and intelligence services. Gustav Lindstrom notes a growing realization that pan-European homeland security is increasingly important. But some of the competencies and most capabilities needed for an effective effort are still lagging. The Union simply has a long way to go, particularly with regard to networking civilian and military capabilities, civil protection and safeguarding critical infrastructure.

In short, both sides face serious organizational challenges. And the interaction between these unwieldy, multi-jurisdictional approaches on each side of the Atlantic has complicated efforts to boost transatlantic and broader international cooperation.

All of these difficulties were exacerbated by the negative spillover from a host of other transatlantic disagreements

Finally, over the past few years transatlantic cooperation in areas related to homeland security was rendered particularly difficult due to policy differences over a host of other issues, including but not limited to the Iraq war. Transatlantic squabbles ranged from European criticism of the Bush Administration's handling of terrorist suspects to its refusal to participate in a series of international agreements. The Adminstration's supporters retorted that Europeans seemed eager to lecture Americans about U.S. failings but appeared less willing to spend the money necessary to make European troops effective, were too absorbed with the details of deeper and wider European integration to recognize the dangers posed by terrorists wielding weapons of mass destruction, and were eager to trumpet "noble" multilateralist instincts in contrast to America's "retrograde" unilateralism—except when it came to international rules that did not support EU preferences. These shrill exchanges sucked the political oxygen out of any possible high-profile transatlantic initiatives to protect European and American societies.

Finding Common Ground

Although some of these differences are likely to persist, much has been done on both sides of the Atlantic to make life safer for ordinary citizens. In recent years a considerable number of cooperative intra-European and transatlantic arrangements have been set in place covering such issues as border security, air transport and container traffic to judicial, law enforcement, and intelligence cooperation.

Within Europe, the EU has created an European Arrest Warrant and started joint investigation teams for criminal investigation. It created a common judicial space, named "Eurojust," to improve the coordination of member states' law enforcement activities, to help with assistance and extradition requests and to support investigations. The EU has adopted legislation on terrorist financing and beefed up laws against money laundering. Europol is collecting, sharing and analyzing information about international terrorism and assessing EU member state performance. National legislation was tightened by key EU member states. Following the March 11 attacks the EU adopted a sol-

idarity clause that commits member states to help each other to prevent and protect against terrorist attacks and to assist each other in case an attack happens. Moreover, European nations have agreed to develop an integrated threat analysis capability at the EU level. FRONTEX, the European Borders Agency, has become operational.[6]

The U.S. and the EU have also stepped up their cooperation. Mutual legal assistance and extradition agreements have been signed. Intelligence sharing has improved, especially information about specific individuals suspected of ties to terrorism. The U.S. and EU have signed agreements to improve container security, expand customs cooperation, improve public-private partnerships to ensure transportation security, and transfer passenger name record (PNR) data. They have agreed to enhance information exchange to target and interdict maritime threats, work more closely through Interpol to deal with lost and stolen passports and other border issues, incorporate interoperable biometric identifiers into travel documentation, enhance their policy dialogue on border and transport security, and start a dialogue on improving capabilities to respond to terrorist attacks involving chemical, biological, radiological or nuclear weapons.

A number of these initiatives are also interesting for broader reasons. First, transatlantic efforts have helped to advance deeper European integration. The creation of the European arrest warrant and the formation of Eurojust, for example, would scarcely have come about without intense U.S. pressure.

Second, the U.S. is gradually accepting the EU as a bilateral partner in issues of societal protection. The U.S.- EU mutual extradition and legal assistance treaties represent a significant expansion of traditional bilateral cooperation in law enforcement and modify transatlantic legal assistance in combating transnational crime in twenty-six countries. They were the first of their kind to be successfully negotiated between the EU and a third party. Given the divergences in European and U.S. legal systems concerning the death penalty, as well as standards in sentencing and for the protection of personal data, these agreements would have been a political impossibility before September 11.

[6] The European Council provides six-month updates of its efforts in this area. See http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/87254.pdf

Third, the U.S. is grudgingly accepting EU standards on issues of vital national importance. U.S. cooperation with Europol, for instance, enables the U.S. to share in the EU's growing development of databases and capabilities, based on the EU's own standards for data protection and privacy.

Fourth, transatlantic cooperation on container security, PNR data transfer and biometric passports is very significant because it requires acceptance of mutual constraints on a broad range of state action in the area of border control—one of the defining aspects of territorial sovereignty. The Container Security Initiative, for instance, is reciprocal, meaning not only that U.S. customs officials can operate in such ports as Rotterdam, Le Havre, Hamburg and Algeciras, but European inspectors could be stationed in Boston, Houston, Long Beach or Shreveport. Such a program is perhaps but the harbinger of a coming revolution in border affairs that creates "virtual" borders far from a nation's territory.

Moreover, such efforts are not starting from scratch. Even though terrorism became the overriding focus of transatlantic security discussions after September 11, 2001, a growing substructure of cooperative efforts to combat criminal and financial threats had already developed among the U.S. and the EU, the G-7, and other OECD countries through the 1990's. These initiatives provided a solid platform on which additional counter-terrorism activities could be based.

In short, despite practical, conceptual and political obstacles to deeper transatlantic cooperation in the area of homeland security, both sides have recognized that deeper collaboration is essential if either side of the Atlantic is to be more secure, and are breaking new ground in their efforts to advance their common security. Taken together, the growing array of U.S.-European cooperative ventures provides ample evidence for a rethinking of homeland security to span the transatlantic space. These agreements underscore the resilience of transatlantic partnership even in the face of serious disagreements.

This is important, because there is still much to be done. Compartmentalized approaches to security remain powerful on both sides of the Atlantic. Transatlantic arrangements have largely been ad hoc achievements rather than integrated elements of a more comprehensive approach.

The premise of this book is that these scattered efforts must now be incorporated into a systematic, high profile effort to "transform" homeland security in all of its many dimensions. In a globalized world no nation is home alone; effective homeland security must also include an international dimension. Without systematic pan-European and transatlantic coordination, each side of the Atlantic is at greater risk of attack. If the transatlantic allies cannot find common ground, there will be little hope for broader global efforts. Moreover, given tight public budgets, security management must become more effective and more efficient. Comprehensive threat assessments and vulnerability analyses are needed to set priorities. Failure to transform civil-military approaches and public-private partnerships, in turn, could further exacerbate problems of transatlantic interoperability. Finally, both sides have expressed a desire to move beyond the tensions of the first Bush Administration. The political climate may therefore be more conducive to cooperation.

"Transforming" Homeland Security: First Principles

In short, a systematic, high-profile effort to transform homeland security is necessary, desirable—and now perhaps more possible. A systematic approach to "transatlantic" homeland security could be guided by a few basic propositions that integrate homeland security and national security.

Understand what we are protecting

Al-Qaeda and related terrorist groupings are lethal networks, often with global reach. Such networks can be flexible and agile, constantly able to reconfigure themselves to address new challenges and seize new opportunities. They are networks that prey on other networks—the interconnected arteries and nodes of vulnerability that accompany the free flow of people, ideas, goods and services, and the complex interdependent systems on which free societies depend. These range from global electronic financial networks, networked information systems, "just-in-time" food supply chains and business systems, air, sea and land transportation to flows of fossil fuels or nuclear energy. It is our complete reliance on such networks, matched with their susceptibility to catastrophic disruption, that make them such tempting tar-

gets for terrorists.[7] In the 21st century, what we are defending is our connectedness.

Globalization is causing a shift in conceptions of power and vulnerability from those that are state-centric and territorial-based to those that are stateless and network-based.[8] A transformative approach to homeland security would supplement the traditional focus on *the security of the territory* with a clearer focus on the *security of critical functions of society*. Terrorists wielding weapons of mass destruction or mass disruption are less intent on seizing and holding our territory than they are on destroying or disrupting the ability of our societies to function. Pauline Neville-Jones uses the example of the September 2000 UK trucking industry strike, which essentially shut down the country, to demonstrate that events other than terrorism could also offer serious threats to national livelihood. "The task," she argues, "is to maintain the connectivity of a networked society."

Antagonists wishing to inflict harm upon a society want to find the key nodes where critical infrastructures connect. When Al-Qaeda destroyed the World Trade Center towers, it engaged simultaneously in attacks on the global securities markets through simultaneous market manipulation, demonstrating that terrorists understand how interconnected, and vulnerable, the world's collective infrastructures are to attack.[9]

Natural disasters, however, may also threaten our connectedness. Hurricane Katrina, for instance, disrupted key energy supply lines between the Gulf coast states and other regions of the United States. The 2004 Pacific tsunami became a world-class homeland security disaster for distant Sweden because of the major tourist networks Swedish citizens had established in recent decades.

---

[7] See Steven Flynn, *America the Vulnerable: How Our Government is Failing to Protect us from Terrorism* (New York: HarperCollins, 2004), p. 86.

[8] See Jean-Marie Guehenno, *The End of the Nation-State* (Minneapolis: University of Minnesota Press, 2000)

[9] See Jonathan Winer, *The Role of Economic Sanctions in Combating International Terrorism (and Its Place in the Trans-Atlantic Alliance)* (Washington, DC: American Institute for Contemporary German Studies, 2001), available at www.aicgs.org/Publications/PDF/Winer.pdf

A security system focused on protecting the connective tissue of modern society would seek to protect critical nodes of activity while attacking the critical nodes of those networks that would do us harm. It would integrate security considerations into the design and daily operations of such systems—from oversight of food production to the guarding of airport perimeters to the tracking and checking of ships. It would identify potential vulnerabilities linked to the technological complexity of the modern world and seek to transform them into high reliability systems. In would seek to anticipate and prevent possible "cascading effects" of a breakdown or collapse of any particular node of activity. It would ensure that "connectiveness vulnerabilities" are not built into future systems. It would engage the active participation of the private sector, which actually owns and controls most of these networks.[10]

Incorporate potentially "transformational" concepts

Given the complexity of risks to be addressed, missions to be accomplished, actors to be coordinated, and effects to be monitored, transformational homeland security requires a comprehensive conceptual framework. This does not mean a one-size-fits-all approach, but it does mean incorporating innovations derived from military and business "transformation" and such security concepts as "resilience," "total defense" and "societal security."

A number of European countries developed a "total defense" concept with roots going back to World War II and its immediate aftermath. This concept was originally geared to the physical survival of the nation and its people in the case of major war, and was premised on the notion of territorial integrity. Total defense focused on comprehensive mobilization of society's resources to support the military in case of a traditional conflict with a foreign enemy.[11]

[10] Some corporate leaders may resist, but many realize that safety makes sense for the bottom line. The 24-hour manifest rule in the cargo industry, for instance, has actually increased productivity. Remarks by Eugene Pendimonti, Vice President of Maersk Sealand, to the Center for Transatlantic Relations, September 13, 2004.

[11] For details and case studies, see Daniel S. Hamilton, Bengt Sundelius and Jesper Grönvall, eds., *Protecting the Homeland: European Approaches to Societal Security—Implications for the United States* (Washington, DC: Center for Transatlantic Relations, 2005).

The modern concept of "societal security" retains the core principle of total defense—the need for a comprehensive societal effort—while widening the notion to embrace a broader, all-hazards approach to risks and threats. Instead of mobilizing civil society to assist the military in the face of external attack, the military is now one element to be mobilized as part of an overall response to major societal disruptions, including—but not limited to—terrorism. Societal security is a comprehensive effort by all levels of government, engaging closely with each other and the public, to prevent, respond to and recover from severe strains on society—whether those strains are unleashed by thinking enemies, natural cataclysms or systemic breakdowns. The strong social weave—Esther Brimmer refers to "cohesion"—that emerges from these vertical and horizontal partnerships enhances national credibility and boosts the chances of preventing and withstanding such strains.

The United Kingdom operates under the different but analogous concept of societal "resilience." The British government established a Civil Contingencies Secretariat in the Cabinet Office shortly before the September 11 attacks to improve the UK's resilience against disruptive challenges. Resilience is defined as the ability at national, regional and local levels to detect, prevent and if necessary handle disruptive challenges. These could range from floods, through outbreaks of human or animal disease, to terrorist attacks.[12] Pauline Neville-Jones portrays resilience in practice through her description of the British response to the July 2005 attacks in London. Even if prevention fails, she argues, resilience must work.

Esther Brimmer suggests how such notions may both frame and focus a "transformed" homeland security agenda. She argues that homeland security is an important subset of the larger notion of societal security, which should not only address issues of physical protection, but also take account of societal cohesion. By cohesion she refers to those values and qualities that bind a community together and are relevant to security—democracy, the rule of law and civil liberties, education, welfare, and pluralism. She adds that concepts of "human security," which focus on the individual rather than the state as the entity to be safeguarded, offer connections between personal safety

[12] For basic information, see the CCS website, www.ukresilience.info/home.htm

and national security of direct relevance to a transformed notion of homeland security. Similarly, notions of "common security" and "human needs" acknowledge that the well-being of society requires sustainable societal networks (provision of food, maintenance of health, etc.). The new security agenda, she suggests, is about "protecting the rich connections that sustain modern life."

Heiko Borchert argues that homeland security can also benefit from the "transformation" agenda developed to advance the effectiveness of U.S. and European militaries. For those unfamiliar with the term, as practiced in the United States it is the process of creating and harnessing the revolution in military affairs that is "transforming" the entire way the U.S. military organizes and trains for warfare, even how it thinks about it. U.S. military services are shifting from force-oriented to capability-oriented approaches to defense planning; from attrition-based force on force warfare to effects-based operations; from terrain-based to time-based capabilities; and from segmented land, sea and air services to shared awareness and coordination across all military services. They are focusing more on countering asymmetric threats, on developing capabilities to synchronize and "leverage" the capabilities of the entire force, and on technologies and practices that can save manpower and increase lethality and survivability.[13] Borchert argues that "transformation" can provide important conceptual and operational tools to align homeland security concepts, capabilities, processes, and structures with changes in the security environment. He describes how key building blocks behind "transformation"—effects-based and network-centric operations, the use of concept development and experimentation, and the establishment of joint command and control instruments, such as the Common Relevant Operational Picture—could offer added value to homeland security. He proposes a "transatlantic homeland security transformation agenda" to harmonize different national and international activities.

[13] For more detail on military transformation and what it may mean for the transatlantic Alliance, see Daniel S. Hamilton, ed., *Transatlantic Transformations: Equipping NATO for the 21st Century* (Washington, DC: Center for Transatlantic Relations, 2004); Hans Binnendijk, ed., *Transforming America's Military* (Washington, DC: National Defense University, 2002).

It takes a network to beat a network

Repositioning existing structures will be important. But traditional alliance mechanisms or government-to-government relationships are inadequate to the challenge of globally networked terrorism. It will take a network to beat a network. A key premise of transformed homeland security is networked defense: traditional structures must be supplemented by an overlay of informal networks that offer a denser web of preventive efforts. Since most of the critical infrastructures that terrorists might want to destroy or disrupt are linked to global networks, it is vital to include citizens and companies in any new regime.[14] This will require governments to define national security more in societal than statist terms and to move beyond traditional "public diplomacy" and "outreach" activities for NGOs toward more effective public-private networks. Traditional alliance mechanisms may be the densest weave in the web, but other connections will be needed to make the overall effort more effective.

During the 1980s and 1990s, military planners moved defense establishments into network-centric warfare, while business executives moved away from vertical hierarchies to flat structures and networked operations. Foreign ministries and other agencies of government, however, remain caught in state-centric approaches and organizational stovepipes. They need to undergo the same type of network-centric reforms; the need for more effective homeland security can both frame and spark such new thinking.

The 9/11 Commission has proposed unifying the many participants in the U.S. domestic counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional bureaucratic boundaries. An international dimension to such an effort would also be essential, and if it were to be launched it would most likely begin with America's closest allies.

Of course, governments are not starting from scratch. In a number of areas relevant to societal security the rigid trappings of state-to-state diplomacy have been giving way, gradually and unevenly, to new forms of interaction among state and non-state actors. Beyond the media glare on transatlantic squabbles the United States and its

[14] Flynn provides a variety of proposals, *op. cit.*, p. 166.

European allies have been forming their own complex, almost invisible and somewhat unconventional networks of cooperation that have become the foundation of joint efforts to freeze terrorist funds, toughen financial transparency measures, and bring aggressive threats of sanctions to those not cooperating. National governments are linking with their regulatory counterparts and the private sector across the globe to tackle thorny transnational issues such as money laundering, securities fraud, and drug trafficking. Governments are finding that such networks can be fast, flexible, cheap, and effective. They can lower the cost of collective action and enable large and disparate groups to organize and influence events faster and better than before. They can build capacities without building bureaucracies.

Transformational homeland security will depend increasingly upon new forms of cooperation among state and non-state actors. In the international sphere, such efforts have been led almost entirely by institutions that are neither nation states, regional unions, multilateral organizations, or international organizations, but rather informal networks of law enforcement agencies, regulators, and the private sector. Such "international non-organizations" such as the Financial Action Task Force (FATF), the Egmont group or the Lyon Group can make a difference by setting standards and attacking nodes of terrorist or criminal activity. These structures developed in response to particular crises in the global financial system, as stakeholders came to realize from painful experience that transborder financial crime, including money laundering, terrorist finance, the theft and sequestration of national patrimonies by corrupt officials, stock market and investment fraud, contributed to such serious domestic problems as drug trafficking, immigrant smuggling, insurance crime and terrorism. By naming and shaming miscreants and threatening to block their access to the world's two most important markets, the Europeans and North Americans at the core of such networks began to produce practical results.[15] Such groups might offer models for similar networked cooperation in related fields.

Such networks aim to protect the critical nodes of activity that connect modern societies while attacking the critical nodes of those net-

[15] See Jonathan Winer, "Cops across borders: the evolution of transatlantic law enforcement and judicial cooperation," in Dalgaard-Nielsen and Hamilton, *op. cit.*, pp. 106-125.

works that would do us harm. Nodal strategies give higher priority to creating an environment hostile to all antagonists than to invest inordinate resources in chasing any particular offender. In each relevant sector the ultimate objective must be to create a loose, agile but muscular public-private network capable of responding to the terrorists' own transnational networks. Heiko Borchert argues that homeland security "should embrace the logic of network centricity in order to create a comprehensive "system of systems" that includes law enforcement, police, fire fighters, emergency medical services, hospitals and other emergency responders, armed forces, intelligence services, research institutes, and the corporate sector.[16]

Include the military in integrated responses to "severe strains on society."

As was discussed earlier, traditional approaches to total defense focused on mobilizing a society's resources to support the military in case of a traditional conflict with a foreign enemy. Today's challenge is the reverse: instead of mobilizing civil society to support the the military in the face of external attack, the military is now one element to be mobilized as part of an overall response to major societal disruptions, including terrorism. Anja Dalgaard-Nielsen argues that civil-military collaboration is essential to prepare a nation for peacetime crises in ways that may also benefit preparedness for catastrophic attack by a thinking enemy. She argues that civilian and military authorities must work more closely together to develop common planning scenarios, common planning goals, and a common understanding of appropriate military tasks.[17]

Gerd Föhrenbach explains that positions among EU members vary considerably with regard to the use of military forces for homeland

[16] For similar proposals, see: James Jay Carafano, "Preparing Responders to Respond. The Challenges to Emergency Preparedness in the 21st Century," Heritage Lectures No. 812, (Washington, DC:The Heritage Foundation, 2003); Lex Bubbers, *Transforming Homeland Defense Through Network Centric Operations. Establishing Event-Driven, Cross-Agency Task Forces. An Executive Brief* (New York: IBM Global Services, 2005).

[17] As she notes in her chapter, there is some movement in this area: the U.S. Department of Defense has issued a Strategy for Homeland Defense and Civil Support; NORTHCOM has drafted plans and scenarios for the military's role in homeland security; and European military research institutes have begun to address some of the same questions.

security purposes. While countries like France and Italy have a history of cooperation between the police and the military, others such as Germany have been very cautious in that respect for historic reasons. Spain and Poland put certain constraints on the domestic use of the armed forces, whereas the legal codes of Denmark, Belgium and the Netherlands do not restrict homeland security missions of their national armed forces.

Yves Boyer would prefer that the military be deployed domestically only for "high threshold" events. But this difference should not obscure a central point of agreement: while a "transformational" approach to homeland security recognizes that military threats represent only one dimension of the threat landscape, it also recognizes that a nation's military must be prepared to respond as part of an integrated national response to "severe strains on society."

This has direct implications for the U.S. debate about the appropriate role of the armed forces in U.S. homeland security. Hurricane Katrina has opened a debate in the United States about the need to modify the Posse Comitatus Act[18] so the President could use the military whenever a major national catastrophe is declared and many lives are at risk. Such a situation would only arise when neither local first responders nor the National Guard would be able to respond quickly or effectively. Lawrence Korb notes, however, that Department of Homeland Security response plans lack detail on how the Pentagon and other federal agencies should assist local leaders in the event of natural or man-made disaster.

Esther Brimmer agrees that the military should have a role in coordinating with the Department of Homeland Security on infrastructure protection, natural disaster relief, and aspects of anti-terrorism. She argues, however, that military support for disaster relief should be expressed by equipping the National Guard with special homeland security units. Lawrence Korb also calls for the creation of specialized National Guard units devoted to incident management and not

[18] The Posse Comitatus Act, written in 1878 to prevent former Union soldiers from mistreating former Confederates, prohibits the U.S. armed forces or U.S. National Guard from engaging in domestic law enforcement tasks within the United States. Exemptions include insurrection, crimes involving nuclear materials or emergencies involving chemical arms or biological pathogens. For one view, see Michael O'Hanlon, "Let Military Keep Order in Disasters," *The Baltimore Sun*, October 6, 2005.

deployed overseas except in times of extreme national emergency. I believe consideration should be given to new types of "homeland security" partnerships across the Atlantic. Partnerships already exist between U.S. state National Guards and various European nations, for example, but they have focused on traditional emergency response. Such partnerships might usefully be extended and focused on best-practice exchange on prevention, response and recovery to catastrophic events, natural or man-made. Had such relationships been in place, the United States may have been better able to utilize European offers of assistance in the wake of Hurricane Katrina.

Effective 'transformation' is not just about building the right structures but cultivating the right culture for networked cooperation

Forging appropriate mechanisms among government agencies and across societal sectors is important, but not sufficient, for transformed homeland security. Success also means cultivating a culture of cooperation across very different organizations. In her case study of Denmark, Anja Dalgaard Nielsen illustrates how turf battles and differences in bureaucratic cultures have complicated efforts to forge more systematic approaches to homeland security planning in a country where the tradition for cross-governmental cooperation is strong, where the military has long carried out or supported a variety of tasks at home, and where political pressure for a coordinated civil-military efforts is high. She suggests that a culture of cross-governmental cooperation should be actively promoted by assigning higher priority to joint education and training.

Transform public-private relationships for homeland security

A related need is a transformed homeland security relationship between the public and private sectors. Pauline Neville-Jones demonstrates how privatization, global sourcing and digital technologies have deprived governments of traditional levers of control over critical elements of their economies at a time when the threat environment forces government and the private sector to take closer account of each other. Since "the task is to maintain the connectivity of a networked society," she argues that governments must forge new rela-

tionships with the private sector that owns and operates critical infrastructure, just as private sector owners must incorporate considerations of public interest into their business planning and daily operations. Heiko Borchert adds that private operators of critical infrastructure and services, supply chain managers, and corporate security managers can provide valuable information to governments, and that public-private interface will be critical to the success of a "common relevant operational picture" for homeland security. Sandra Bell points to possible synergies between various U.S. and European initiatives involving public and private actors. Such public-private mechanisms are still in their infancy, and are likely to encounter similar issues of cultural dissonance and competing goals. For instance, whereas the business community is typically focused on efficiencies, the security community is often focused on redundancies—layers of defense that reinforce their overall deterrent value. Nonetheless, there is a need to forge new patterns of interaction.

Don't destroy what you are trying to protect

Esther Brimmer notes that "Homeland security includes not only preventing an attack, physical protection of assets, and consequence management, but also respect for the character of the society that it seeks to defend." She argues that "societal security" must encompass the values and qualities that bind a community together, and must not degrade those features which make democratic society worth defending in the first place.

European experience offers a cautionary tale. Thirty years ago, the Baader-Meinhoff terrorist gang goaded German authorities to hit back at them in ways they believed would break the law and undermine Germany's hard-won democracy. They reasoned that the quickest way to wound the German government would be to force it to break its own rules, corrupt its own nature and generate mistrust between the government and the governed. German leaders had to find the difficult balance. The anti-terrorist legislation that resulted sought to find this balance.[19]

[19] For a review of German efforts to confront terrorism then and now, see Oliver Lepsius, *The Relationship between Security and Civil Liberties in the Federal Republic of Germany After September 11* (Washington, DC: American Institute for Contemporary German Studies, 2001), available at http://www.aicgs.org/Publications/PDF/lepsiusenglish.pdf

This challenge is perhaps of even more relevance to democratic governments fighting international terrorism today. A number of the measures introduced to combat terrorism raise serious civil liberties concerns. In addition, abuses at Abu Ghraib and Guantanamo have undermined confidence in the U.S. Administration and international support for the anti-terrorism campaign. If the campaign is not perceived to be legitimate, it is unlikely to be effective. If efforts to protect our societies from catastrophic disruption are not aligned with the freedoms of those societies, we endanger that which we are trying to protect.

At the same time, the U.S. is finding that judicial cooperation is particularly important for dealing with terrorism. The unique nature of terrorism means that maintaining the appearance of justice and democratic legitimacy will be much more important than in normal wars or struggles. Ad-hoc anti-terrorist measures that have little basis in societal values and defined legal procedures provide little long-term bases for the necessary cooperation with other countries.

The U.S. and Europe can each learn from each other's experience with mechanisms that seek to advance security and liberty, such as sunset clauses and provisions for legislative oversight and judicial review. If the U.S. and Europe can help each other live up to their own standards, together they can help set human rights standards for the broader anti-terrorist campaign. On the other hand, if concerns about civil liberties are widespread even in the West's most sophisticated and oldest democracies, how much worse are they likely be in countries without such strong traditions who are also cracking down on suspects? Failure to advance security with liberty has the potential to subvert other key priorities, such as transformation of the Broader Middle East, where the overall trend throughout the Arab world has been a decline in social, political and cultural freedoms in the name of greater security against terrorism.[20]

Transforming Institutions and Mechanisms

Taken together, our authors present a comprehensive "transformational homeland security" agenda to be advanced on multiple tracks.

[20] See Alyson Bailes, "Have the Terrorists Already Won?" Speaking Notes, Scanbus Conference, Riga, September 14, 2004.

National efforts

Lawrence Korb calls for an exhaustive set of initiatives in the U.S., from improving the FBI's counterterrorism capabilities, establishing Homeland Security Operations Centers across the nation, and increasing pharmaceutical and vaccine stockpiles and distribution systems to replacing the current color-coded public alert scheme and creating a reinsurance corporation capitalized by the private sector and backed by the government.

In Europe, ultimate responsibility for "transformed" homeland security rests with individual nations. European societies are inextricably intertwined, however, in mutually dependent networks of information and finance, transportation and power generation, food production and health. These networks can only be protected successfully on a transnational basis. Gustav Lindstrom and Gustav Gustenau argue that the EU can and should develop an "added-value" role. They propose a raft of new initiatives at EU level, ranging from new data retention procedures and sunset clauses to intensified intelligence cooperation, formation of national civilian-military homeland security units, and use of 'variable geometry" subsets of EU member states as test beds for EU level homeland security policies in selected areas. Gustenau makes the important point that if the European homeland remains as unprotected as it is, fear of reprisals at home will hamper more ambitious EU missions in hostile environments abroad.

Bilateral efforts

Bilateral cooperation between the U.S. and individual European nations will remain important despite more ambitious EU efforts, because even within the EU most of the instruments and competences in the fight against terrorism remain in the hands of member states. Although the EU can do a lot to help national authorities work together internationally, the hard work of tracking down potential terrorists, preventing attacks and bringing suspects to justice remains the preserve of national authorities. Operational decisions are still national decisions. Boyer argues that intelligence cooperation against diverse terrorist networks has to be advanced at three levels of "operation:" synchronizing and pooling intelligence products efficiently among different national services; coping with different judicial proce-

dures and legal systems, and managing the risks of intelligence sharing, at both the European and transatlantic level; and global cooperation regarding terrorism and organized crime.

U.S.-EU cooperation

The U.S. can work not only with individual European nations but with at EU level as well. The depth of that cooperation depends in part on the nature of the EU's own competencies in this area. U.S.-EU cooperative mechanisms are likely to evolve as the EU itself evolves. Transatlantic efforts in law enforcement, intelligence and other areas that operate at the member state level need to be coordinated with efforts at infrastructure protection, health security and other areas that are gradually beginning to be coordinated at the Community level. Information sharing will remain a critical yet difficult issue, given different legal regimes and political perspectives. As in so many other fields of policy, the key is to keep each other informed at an early stage of new policy proposals which might have an impact on the other so that potential differences can be resolved before legislation is enacted. The U.S.-EU Policy Dialogue on Border and Transport Security could perhaps be supplemented, as Heiko Borchart suggests, by a Transatlantic Homeland Security Dialogue that includes various agencies.

More can be done together, however, not only to protect European and American societies directly, but to help third countries in their fight against terrorism—in essence to "project resilience" to neighboring countries. Europeans and Americans could engage more effectively together in security sector reform in third countries, and better coordinate external assistance to address conditions in which terrorism can grow. A strong homeland security system in one country may mean little if neighboring systems are weak. Terrorists in Europe, for example, have shown themselves to be far more pan-European than most of Europe's security agencies. They plan attacks in one country and execute them in the next.[21] Health issues, to take another example, have become integral elements of national security. Developed countries are only as secure as the world's weakest public health system.

[21] See John L. Clarke, "European Homeland Security: Promises, Progress and Pitfalls," in Bertelsmann Stiftung, (ed.), *Securing the European homeland: The EU, terrorism and homeland security* (Gütersloh, August 2005).

NATO and the Partnership for Peace/Euro-Atlantic Partnership Council

In past years NATO reforms have focused on projecting force and coping with threats beyond the NATO area. But NATO's nations—and their partners—must be prepared not only to project power beyond Europe but also to prevent, deter and, if necessary, cope with the consequences of WMD attacks on their societies—from any source. Territorial defense in the Cold War sense of protecting sealanes from Soviet submarines or guarding the Fulda Gap from Soviet tanks must give way to a new common conception of societal protection from WMD attacks from any source. If Alliance governments fail to defend their societies from a major terrorist attack, potentially involving weapons of mass destruction, the Alliance will have failed in its most fundamental task. It will be marginalized and the security of Europe and North America will be further diminished.[22]

In most countries these issues are primarily civilian, national and local priorities. But NATO has a role to play, particularly in civil-military planning capabilities, security sector reform, intelligence-sharing, political consultations and consideration of missile defense. NATO's civilian disaster response efforts are still largely geared to natural disasters rather than intentional attacks, and remain very low priority. It is time to ramp up these efforts to address intentional WMD attacks on NATO territory, to develop more serious transatlantic efforts to protect critical infrastructure, to work with partners such as Russia to develop new capabilities and procedures for collaboration with civilian authorities, and to tap the expertise of partners who have had decades of experience with "total defense."

In fact, the area of "transatlantic societal security" could be an attractive new mission for a rejuvenated Partnership for Peace and its political umbrella, the Euro-Atlantic Partnership Council. A bioterrorist attack of contagious disease, for instance, will not distinguish between "allies" and "partners," and a number of partners have more experience mobilizing for societal security than do many allies.

[22] See Daniel S. Hamilton, "Renewing Transatlantic Partnership: Why and How, Testimony to the House Committee on International Relations, European Subcommittee, June 11, 2003; and Daniel S. Hamilton, *Transatlantic Transformations*, *op. cit.*

Following the last round of NATO enlargement the Partnership for Peace is a strange mix of prosperous, non-aligned Western countries such as Sweden, Finland, Austria, Ireland and Switzerland, and a number of Central Asian nations. It is precisely some of these non-aligned countries, however, which have decades of experience with approaches to societal defense, and it is precisely the area of Central Asia in which forward defense, security sector reform and preventive efforts against WMD threats are critical. NATO's special partnerships with Russia and Ukraine could also be utilized to good effect in this area.

Joint work on societal security could also infuse NATO-EU relations with a new sense of common purpose and lend substance to the "strategic partnership" each has declared yet neither has achieved. While both organizations are exploring how to strengthen their cooperation, they have little to show for it except for some successes in the Balkans. A joint focus on societal security, including consequence management, could inject new energy into their efforts, and both organizations have tools to offer.

New mechanisms and approaches

Heiko Borchert suggests the need for various mechanisms that are not necessarily the "preserve" of any single institution, for instance a collaborative homeland security "concept and development experimentation" environment drawing on "transformational" lessons; a transatlantic homeland security clearing house and training program; a transatlantic Common Relevant Operational Picture (CROP); or a homeland security science and technology program.

Moreover, to take another example, the world is on the cusp of exponential change in challenges posed by pathogens and their accessibility to state and non-state actors. These challenges require actions beyond piecemeal extensions of current policies. They require something more holistic than disease-specific stockpiles of medicines or vaccine. They require us to integrate public health and national security communities in ways that allow us to deal with an unprecedented challenge. Key multilateral frameworks such as NATO and the EU are limited in their ability to cope with the unique challenges posed by a bioweapon-induced spread of epidemic disease. Would a bioweapon attack that threatens a nation's health rather than its territory warrant

a collective response under NATO's mutual defense clause or the EU's "solidarity clause?" What might such a response entail, and is either institution equipped for such action? Joint planning for traditional international security contingencies has occurred in NATO for decades. Planning with that degree of rigor and strategic and operational detail, but now for international response to epidemics, is but one example of what is needed to cope with potential threats to the European or North American homelands.

Looking ahead

During the late 1940s and early 1950s Europeans and American responded together to the challenges facing their generation. The potential of catastrophic terrorism now challenges a new generation of Europeans and North Americans to reshape and reposition existing structures, and to devise new approaches that can help us respond more effectively. Given the nature and scope of the threat, many solutions will ultimately have to be global. Any "global" solution, however, must be built by a coalition of nations committed to the effort. The core of any effective coalition on homeland security issues, as on security challenges of the past, is most likely to be the transatlantic community.

Implications of Homeland Security for Rethinking Transatlantic Security

Chapter 1

Homeland Security and Transformation: Why It Is Essential to Bring Together Both Agendas

Heiko Borchert

Contemporary security challenges such as terrorism, organized crime, the proliferation of weapons of mass destruction, cyber risks, or mass migration have one thing in common: they challenge the capability and the capacity of our security institutions to deal with them. The key problem is that the diverse, network-centric, and interrelated character of today's security risks has hardly led to adequate organizational and behavioral reforms in the security sector. Four issues can be singled-out as most important:

First, contemporary security risks are transnational, originate within or beyond states, and involve non-state actors that are ready to use force. The new nature of the risks thus requires concerted efforts to bring into play all public and private instruments of power to address the sources and the consequences of risks. This in turn demands a new quality of interagency interaction for planning, implementing, and evaluating the necessary strategies. Second, because of the general shortage of public funds, security management must become more effective and more efficient. In the future, joint operations involving all instruments of power and the deliberate creation of common pools of capabilities will become the norm. Third, the seamless interaction between various actors at home and abroad puts a premium on improving interoperability and cooperability with regard to concepts, doctrines, processes, structures, and materiel used. Finally, the need to accelerate decision-making has greatly increased—a trend that is underlined, for example, by the deployment requirements of the NATO Response Force and the EU Battle Groups, which were cut to a few days, or the military sensor-to-shooter cycle that has been compressed to a few minutes. As a consequence, the added value of each level of the command echelon has to be reassessed and new instruments are required to improve joint situational awareness and understanding and to facilitate joint command and control.

While some of these issues have been addressed, what is still lacking is a comprehensive approach to realign security tasks, responsibilities, and capabilities as well as structures and processes of all relevant actors in line with the new risk environment. This is a serious problem, because it could lead to a dual asymmetry: adapting civilian security instruments and ministries lags behind most recent military reform initiatives aimed at improving the effectiveness, deployability, and flexibility of the armed forces, and diverging views about the possible homeland security role of armed forces could worsen already existing problems affecting transatlantic interoperability and cooperability.

This chapter argues that the overall approach needed to address comprehensively all of these issues can be found in the concept of transformation. Transformation provides a new philosophy and the building blocks continuously to adapt concepts, capabilities, processes, and structures of the security apparatus in line with changes in the security environment. It emphasizes the need for effects-based and network-centric operations, the use of concept development and experimentation, and the establishment of joint command and control instruments, such as the Common Relevant Operational Picture. As will be shown, each of these building blocks provides much needed added value to improve homeland security. The chapter concludes by proposing a transatlantic homeland security transformation agenda to help facilitate the harmonization of different national and international activities.

Why Transformation is Relevant for Homeland Security[1]

Homeland security is a concerted all-government effort that involves all available public and private security capabilities aimed at

- preventing symmetric and asymmetric risks from arising,
- protecting people, democratic institutions, critical infrastructure and services, and security forces (i.e., armed forces, emergency responders, and others)

[1] Portions of this section build on: Heiko Borchert and Thomas Pankratz, "Homeland Security aus europäischer Perspektive," [Homeland Security: A European Perspective] in *Weniger Souveränität—Mehr Sicherheit. Schutz der Heim]at im Informationszeitalter und die Rolle der Streitkräfte [Trading Sovereignty for Security. Homeland Security in the Information Age and the Role of Armed Forces]*, ed. Heiko Borchert (Hamburg: Verlag E.S. Mittler & Sohn, 2004), pp. 21-30.

- containing the impacts/effects of a catastrophic event, managing its consequences, recovering, and facilitating the return to pre-crisis conditions.

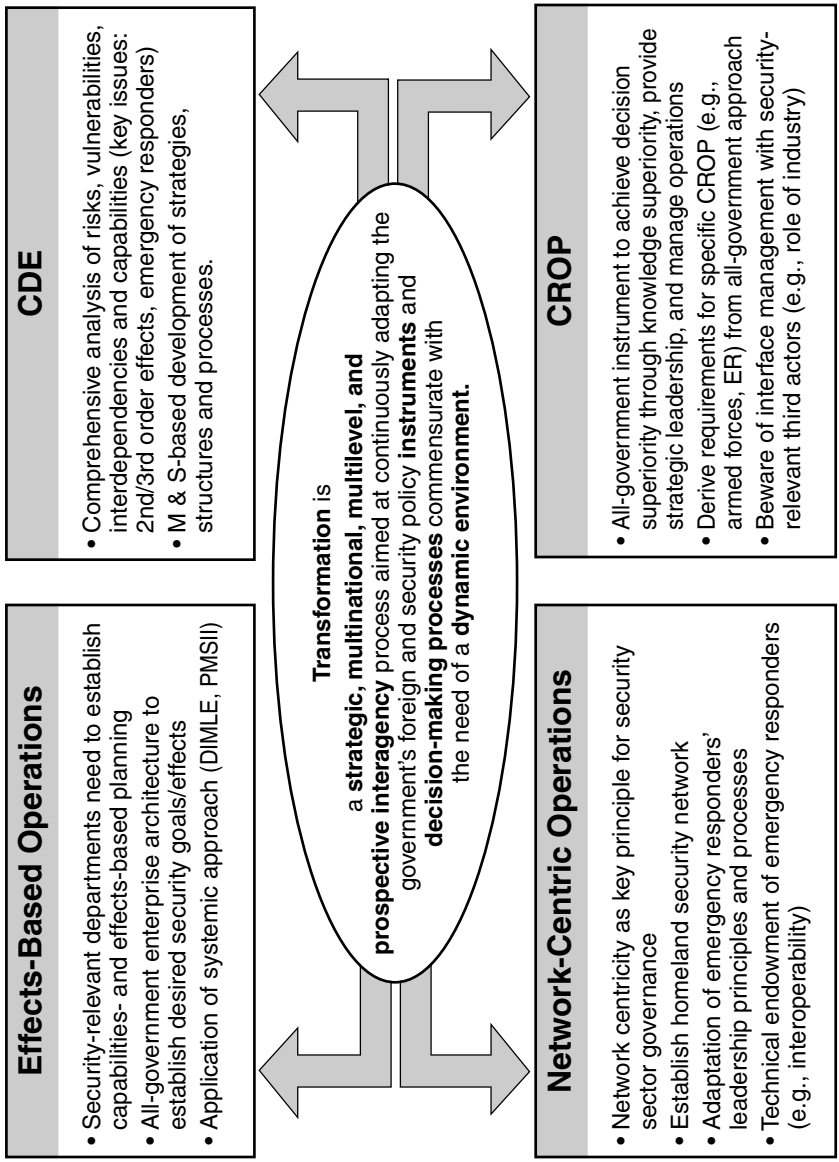
The novelty of this approach is threefold. Rather than focusing on a territorial definition of the origin of risks, the definition looks at their effects. This helps overcome the traditional distinction between "domestic" and "foreign" security concerns, which are becoming increasingly blurred. By focusing on the effects, the definition advances a functional understanding of the missions to be executed. In doing so, a continuum of operations ranging from crisis prevention to crisis management and post-crisis stabilization can be defined that provides the general framework for contingencies at home and abroad. This continuum can be interpreted as a value chain along which each instrument of power can make specific contributions based on individual core competencies, thus providing an intertwined delivery of military and non-military capabilities. Finally, the logic of the value chain gives rise to a process-based and network-centric organization of interagency interaction that helps realign tasks, capabilities, processes, and structures of the security apparatus.

Given the complexity of risks to be addressed, missions to be accomplished, actors to be coordinated, and effects to be monitored, homeland security requires a comprehensive conceptual framework. The logic of transformation developed to advance the effectiveness of armed forces provides such a framework. Generally speaking, transformation can be understood as a strategic, multinational, multilevel, and prospective interagency process aimed at continuously adapting the government's foreign and security policy instruments and decision-making processes commensurate with the needs of a dynamic environment.[2] As Figure 1 shows, the conceptual building blocks of transformation are effects-based and network-centric operations, concept development and experimentation, and a Common Relevant Operational Picture. Each of these elements is of key importance to homeland security missions.

---

[2] Ralph Thiele, "Intervention und die Sicherheit zu Hause in Deutschland: Transformation der Sicherheitspolitik unter neuen Vorzeichen," [Intervention and German Homeland Security: Transforming Security Policy Under New Conditions] in *Weniger Souveränität—Mehr Sicherheit [Trading Sovereignty for Security]*, ed. Heiko Borchert (Hamburg: Verlag E.S. Mittler & Sohn, 2004), p. 97.

Figure 1. Homeland Security and Transformation—Philosophy and Building Blocks



Abbreviations: CDE Concept Development and Experimentation; CROP Common Relevant Operational Picture; DIMLE Diplomacy, Information, Military, Law Enforcement, Economics; ER: Emergency Responders; M&S: Modeling and Simulation; PMESII Politics, Military, Economics, Society, Information, Infrastructure

Effects-Based Operations (EBO)

Effects can be defined as outcomes resulting from the deliberate use of a coordinated set of actions involving all relevant state and non-state capabilities across the spectrum of diplomacy, information, military and law enforcement, and economics (DIMLE). The aim is to shape the behavior of actors and to influence conditions consistent with an overall goal (end-state) to be achieved. Most importantly, EBO applies a systems approach, which means that the target to be influenced will be analyzed from various perspectives, thereby paying special attention to political, military, economic, social, information, and infrastructure aspects (PMESII).[3]

EBO is relevant for homeland security because it stipulates the need for interagency interaction beyond the current coordination of activities that is largely born out of bureaucratic stovepipes. An effects-based approach to homeland security requires an overall understanding and a joint definition of effects to be achieved, thereby taking into account all instruments available in the DIMLE spectrum. This could entail measures to

- prevent serious risks from arising, for example through the fight against the proliferation of weapons of mass destruction, the protection of critical infrastructure, or the stockpiling of vaccines;
- contain an actor or the consequences of an event, for example by tightly surveying critical regions that serve as areas of retreat for terrorist actors;
- deter an actor from undertaking certain actions, for example by showing military force or toughening legal regulations (e.g., for fraudulent cyber space activities);
- deny freedom of movement and access to certain groups, for example by restricting immigration regulations, restricting entry guidance for critical infrastructure, or sealing off sanctuaries;

[3] Paul K. Davis, *Effects-Based Operations. A Grand Challenge for the Analytical Community* (Santa Monica, CA: RAND, 2001); Edward A. Smith, *Effects-Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War* (Washington, DC: CCRP, 2002).

- disrupt an actor's ability to act or to effect influence, for example by revealing leadership structures or relationships among key decision-makers, drying financial accounts, or shaping public opinion through information operations;
- defeat an actor or a situation in order to regain control, for example through military and non-military intervention, counter-terrorist activities, or emergency management in case of natural catastrophes;
- stabilize a situation by creating an environment favorable to launching political, economic, and other support activities aimed at promoting the return to pre-crisis conditions of living, for example through emergency help for people (e.g., provision of nutrition, care, and financial support), reconstruction, provision of law and order;
- guarantee conditions of living at pre-crisis levels, for example by reestablishing the proper functioning of government agencies and public services or the smooth running of critical infrastructure and services.

The challenge to implementing these and similar tasks is twofold: First, it is necessary to adopt an all-government approach to capabilities-based planning. Capabilities can be defined as those competencies needed to achieve defined missions. Rather than simply focusing on the provision of single platforms, today's capabilities-based thinking takes into account the complex mix of doctrine, organization, training, leadership, materiel, personnel, and infrastructure needed to achieve successful mission outcome. While capabilities-based planning has become common sense for armed forces, it has hardly gained the same prevalence among civilian departments. This seriously hinders effects-based operations from being planned at all, because planners do not have a "common language" for communicating with each other.

Closely related to capabilities- and effects-based efforts is the question of process-based management across all security-relevant actors.[4]

[4] For a similar argument, see: Martin J. Gorman and Alexander Krongard, "Institutionalizing the Interagency Process. A Goldwater-Nichols Act for the U.S. Government," *Joint Forces Quarterly* 39 (Winter 2005), pp. 51-58.

As was argued above, realigning security tasks along the continuum of crisis prevention, crisis management, and post-crisis stabilization requires a process-based, interagency enterprise architecture. Already a standard requirement for governance in today's networked world,[5] this demand poses serious challenges, because it entails nothing less than fundamental reorganization of the security sector. As Figure 2 points out, all levels of action—from strategic interagency leadership through operational levels of mission preparation and implementation and the organization of key managerial support processes—will be affected.

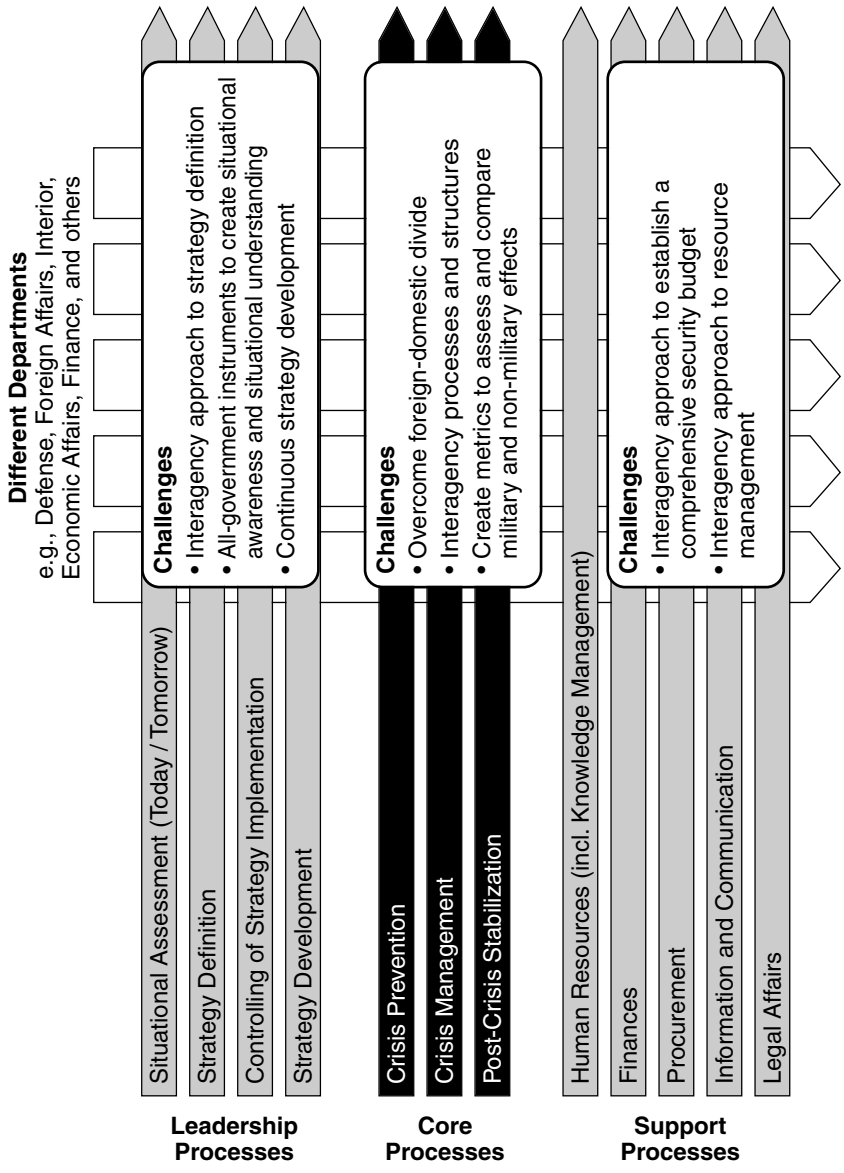
The realignment of security tasks described by the three security core processes referred to above will be seriously hampered without overcoming the structural dichotomy in organizing military and non-military capabilities. At the strategic level it will thus be crucial to implement joint instruments to provide and improve situational awareness and situational understanding and to establish joint processes for setting up and monitoring the implementation of security strategies. Joint approaches to capability building must be developed in tandem with new metrics to assess and to compare effects achieved by military and non-military action. In addition, the redesign will also require a new approach to resource management. Money, personnel, knowledge, and other key resources need to be managed jointly in order to make sure that resource endowment is commensurate with the effects that need to be achieved. This, however, is not possible as long as managerial responsibility for resources is confined to single departments. Therefore, experts have suggested the establishment of unified security budgets aimed at rebalancing different budget categories and making security spending more coherent.[6]

---

[5] Stephen Goldsmith and William D. Eggers, *Governing by Network. The New Shape of the Public Sector* (Washington, DC: Brookings Institution Press, 2004); GAO, *Results-Oriented Government. Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (Washington, DC: United States Government Accountability Office, 2005).

[6] *Report of the Task Force on A Unified Security Budget for the United States, 2006* (New York and Washington, DC: Institute for Foreign Policy and Center for Defense Information, 2005); Thomas Dittler and Adolf Neubecker, "Homeland Security und die Notwendigkeit eines gesamtheitlichen Sicherheitsansatzes" [Homeland Security and the Need for a Comprehensive Security Approach"], in *Weniger Souveränität—Mehr Sicherheit [Trading Sovereignty for Security]*, ed. Heiko Borchert (Hamburg: Verlag E.S. Mittler & Sohn, 2004), p. 152.

Figure 2. Process-Oriented Homeland Security Architecture



Concept Development and Experimentation

Concept development and experimentation (CDE) is the key implementation tool for transformation. Because today's security risks are complex, there is no one-size-fits-all solution. CDE aims at testing in advance what strategies are best suited to tackle different risks, what capabilities are required, and how processes and structures need to be adapted in order to provide smooth interaction. By using modeling, simulation, and other techniques, CDE provides an early assessment of the potential outcome of new thinking, thereby pointing out intended and unintended consequences. As an integral component of the modern art of strategy development, CDE will provide valuable assistance to developing homeland security.

One area of application is capacity building in homeland security. CDE can provide a holistic approach for analyzing the interplay between risks, vulnerabilities, interdependencies, and the resulting need for capabilities. More than other policy areas, homeland security must deal with critical interconnections, especially in the field of infrastructure protection.[7] It is extremely difficult to gain an overview of technical infrastructure networks and their dependent and independent nodes. Being able, for instance, to assess primary, secondary or third order effects of power shortages is therefore key to mitigating their consequences. The same holds true for the safety and security of critical nodes that provide services for more than one country. Think, for instance, of large seaports in the United States or in Europe. Not only would their breakdown encroach upon national security of supply; the highly interdependent network of global supply chains would be affected as well, thereby causing instant economic damage. CDE can help assess these interdependencies and provide risk maps as a basis for adequate counter measures.

Building on these insights it will be possible to produce comprehensive capability maps outlining what is available and what shortfalls need to be addressed. Again, an effects-based approach to homeland security will make it inevitable not to rely only on one instrument of power (e.g., military) but to provide a balanced mix of capabilities. In doing so, the emergency responders' community plays a key role. As

[7] For more on this, see the chapter by Sandra Bell in this volume.

the instrument of the first hour, emergency responders' capabilities largely determine if and to what extent the capabilities of other security-relevant actors will be needed. CDE can be used to determine the relevant mix of capabilities commensurate with different homeland security scenarios, such as natural catastrophes, terrorist attacks with or without weapons of mass destruction, critical infrastructure/services breakdown, or cyber incidents. In assessing the performance of individual capability profiles, CDE helps take into account legal restrictions limiting their use (e.g., domestic use of force, limited sustainability, and others) and potential vulnerabilities (e.g., jamming the mobile phone network in order to avoid the explosion of remotely controlled bombs can have detrimental effects on the usability of emergency responder communication systems).[8]

Network-Centric Operations

Since the publication of the *Joint Vision 2010* for the U.S. Armed Forces the notion of network-centric warfare has come to dominate the international force transformation agenda. In their influential book *Network-Centric Warfare*, David S. Alberts, John J. Garstka, and Frederick P. Stein capture the essence of the new art of delivering military power by "networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[10] While network-centric warfare focuses on the particular application of military power, the principle of network centricity has since been broadened by the concept of network-centric operations (NCO). In its most basic understanding, network centricity refers to the deliberate act of linking goals, capabilities, processes, structures, and capacities of security-relevant state and non-state actors in order to coordinate, harmonize, and integrate their action. Network centricity thus refers to the close interaction between different levels of planning, decision-making, and implementation and vari-

[8] This occurred during the 2004 Madrid bombings. In Israel switching off the mobile phone network is now a standard procedure after suicide attacks.

[9] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare. Developing and Leveraging Information Superiority* (2nd ed.) (Washington, DC: CCRP, 2002), p. 2.

ous actors working together to achieve different tasks by using a wide spectrum of instruments of power.[10]

Homeland security is a cross-sector task that needs to involve a great number of actors at regional, national, and international levels. Therefore, it should embrace the logic of network centricity in order to create a comprehensive "system of systems" that includes law enforcement, police, fire fighters, emergency medical services, hospitals and other emergency responders, armed forces, intelligence services, research institutes, and the corporate sector.[11] At its core, NCO for homeland security implies the establishment of a comprehensive network architecture to include all the relevant actors referred to just above. According to the Markle Foundation Task Force on National Security, the purpose of this network is "to get information into the hands of people who could analyze and act on it (…) and to enhance the government's 'sensemaking' ability—that is, its ability to discern indicators of terrorist activity amid overwhelming amounts of information, and to create more time for all of the actors to make decisions and to prevent or respond to terrorist acts more effectively."[12] While the Markle Task Force is right to emphasize the risk of terrorism, this is, of course, not the only homeland security task. The same basic principle also applies to combating organized crime, human trafficking, money laundering, narcotics trafficking, or any other risk that endangers the homeland.

The consequences will be manifold. Most importantly, it will be necessary to design a network architecture that takes into account the

---

[10] Heiko Borchert, "Vernetzte Sicherheitspolitik und die Transformation des Sicherheitssektors: Weshalb neue Sicherheitsrisiken eine verändertes Sicherheitsmanagement erfordern," [Network-Centric Security and Security Sector Transformation: Why New Security Risks Require New Security Governance], in *Vernetzte Sicherheit. Leitidee der Sicherheitspolitik im 21. Jahrhundert [Network-Centric Security. Security Policy Paradigm for the 21st Century*, ed. Heiko Borchert (Hamburg: Verlag E.S. Mittler & Sohn, 2004), pp. 54-57.

[11] For similar proposals, see: James Jay Carafano, "Preparing Responders to Respond. The Challenges to Emergency Preparedness in the 21st Century," Heritage Lectures No. 812, (Washington, DC: The Heritage Foundation, 2003); Lex Bubbers, *Transforming Homeland Defense Through Network Centric Operations. Establishing Event-Driven, Cross-Agency Task Forces. An Executive Brief* (New York: IBM Global Services, 2005).

[12] Markle Foundation Task Force, *Creating a Trusted Information Network for Homeland Security. Second Report of the Markle Foundation Task Force* (New York: The Markle Foundation, 2003), p. 8.

different technical endowment of the actors to be involved. This puts a premium on standardization as a major instrument to guarantee interoperability. This is a potential Achilles heel of all civilian homeland security actors, as they tend to lack a central authority responsible for defining and enforcing standards.[13] In this regard, the domestic departments and agencies will in the future have to assume a role comparable to the departments of defense in defining the relevant standards in tandem with military, industrial, and scientific partners. Furthermore, they will also have to establish single-buyer authority in order to overcome the heterogeneous buyer environment that is characteristic of today's emergency responder procurement landscape. Embracing network centricity will also influence doctrine and leadership of emergency responders that need to adopt mission-type tactics, which is at the core of network-centric self-synchronization.

Common Relevant Operational Picture

The "mother of all instruments" required to provide effects-based, network-centric operations is a new system for tying information together to present as a Common Relevant Operational Picture (CROP), also called a Common Operations Picture (COP). Conducting joint operations requires joint situational awareness and joint situational understanding provided by the CROP. Technically speaking, the CROP integrates different "pictures" (e.g., air, land, sea, logistics, medical, and other pictures) from various homeland security actors into one comprehensive overview of the homeland security space. Building on the suggestion for a homeland security network submitted above, a CROP provides added value at all levels of operational planning and execution by allowing each partner to access a joint knowledge-base commensurate with his or her individual role and tasks. Against the background of the joint CROP established at the strategic level, requirements for CROPs at lower levels of the command echelon can be derived in a systematic way.

[13] Italy, for instance, has defined nation-wide CBRNE equipment standards and adopted an Incident Command Systems as the national standard for emergency command and control. See: Friedrich Steinhäusler and Frances Edwards (eds.), *NATO and Terrorism. Catastrophic Terrorism and First Responders. Threats and Mitigation* (Heidelberg: Springer, 2005), pp.76-77.

Establishing a CROP comes with various consequences. A vast amount of raw data needs to be processed and assessed quickly. While the first is a challenge for the technical design of the network, the latter refers to the organization of intelligence. Adding emergency responders and other homeland security actors to the list of intelligence clients requires intelligence services to come up with actionable intelligence that deviates from strategic assessments traditionally provided to political decision-makers or theater-based intelligence for military commanders. One issue that needs to be addressed is classification. Because intelligence in the framework of homeland security must reach as many users as possible, upholding traditional classification schemes can be detrimental to informing those that most urgently need intelligence. In addition, the product portfolio might have to be adapted in order to mirror homeland security intelligence requirements. This in turn requires close interaction and dialogue with customers, which can be time-consuming as many of the new homeland security clients may not be familiar with intelligence at all.[14] Furthermore, the creation of a joint database filled by all intelligence services and accessible to all homeland security actors poses legal questions that need to be addressed. This holds especially true for international intelligence cooperation, which, at least so far, has been seriously hampered by diverging intelligence laws, and for the systematic use of privately held data. The value of the latter can not be underestimated. The Markle Foundation has shown that the September 11 terrorists could have been identified from airline reservation systems and searches of public-record data.[15]

Finally, private operators of critical infrastructure and services, supply chain managers, and corporate security managers can provide valuable information based on their own risk assessments. Because private companies provide key public services, government officials must know whether and to what extent homeland security contingencies affect

[14] For more on this, see: Arthur S. Hulnick, *Keeping Us Safe. Secret Intelligence and Homeland Security* (Westport, London: Praeger, 2004), pp. 85-102; Gregory F. Treverton, "Intelligence Gathering, Analysis, and Sharing," in *The Department of Homeland Security's First Year*, ed. Donald F. Kettl (New York: The Century Foundation Press, 2004), pp. 55-76; Henry A. Crumpton, "Intelligence and Homeland Defense," in *Transforming U.S. Intelligence*, eds. Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), pp. 198-219.

[15] Markle Foundation Task Force, *Protecting America's Freedom in the Information Age. A Report of the Markle Foundation Task Force* (New York: The Markle Foundation, 2002), p. 28.

corporate performance. At the same time, it is obvious that the corporate sector is eager to participate in the government's situational assessment in order to decide what actions are needed. This makes it clear that the public-private interface is critical to the success of a homeland security CROP. Thought should therefore be given to ways to link public CROPs with equivalent corporate instruments that are already in use or will be established, as the notions of NCO and real-time enterprises are about to dominate the management world as well.

Outlook: A Transatlantic Agenda for Homeland Security Transformation

This chapter argues that transformation should cover homeland security as well. This would make it possible to develop, in tandem, military and non-military capabilities needed to provide a broad spectrum of tasks aimed at crisis prevention, crisis management, and post-crisis stabilization. Adopting a comprehensive framework for realigning "domestic" and "foreign" security instruments helps overcome a dichotomous approach in favor of a joint continuum of operations to which all state and non-state actors can plug in where their core competencies are best suited. Embracing the transformation mantra also makes it possible to bring in line various international activities within NATO and the European Union and national programs, which have been difficult to coordinate so far. The remainder of this chapter will thus propose initial building blocks for a transatlantic homeland security transformation agenda.

Establish Transatlantic Homeland Security Dialogue Forum

Although there is transatlantic interaction with regard to various homeland security aspects, a comprehensive framework to address all facets is conspiciously absent. In a first step, a dialogue forum should be established. Given the tight international agenda, it is proposed to convene such meetings parallel to the regular U.S.-EU summits, but with the participation of Non-EU NATO members and NATO officials. Given NATO's serious commitment to transformation,[16] its

[16] *Strategic Mission. The Military Challenge* (Norfolk, VA and Mons, Belgium: Allied Command Transformation, Allied Command Operations, 2004).

expertise in civil-military emergency planning, and its key role in specific homeland defense tasks (e.g., missile defense, nuclear umbrella), it would be unwise not to include the alliance. Between summit meetings, expert groups could address different issues to advance transatlantic homeland security cooperation. As will be shown, the new forum can be used to advance practical cooperation projects relevant for transatlantic homeland security transformation.

Include Homeland Security in Capability Planning

Ongoing capability-based planning exercises should be expanded to include homeland security missions as well. This requires the inclusion of emergency responders in current planning activities and the adoption of capability-based planning by the emergency responder community. In addition, ongoing activities to set up databases for civilian and military capabilities relevant for homeland security missions in NATO and the EU should be paralleled. This could help set up a joint NATO-EU Capabilities Group relevant for homeland security. Military capabilities relevant for stabilization, intervention, and homeland security include, among others, intelligence, surveillance, and reconnaissance, command and control, mobility, CBRNE detection and protection, and medical services. Most of these capabilities, however, are in short supply, which means that their use in missions abroad limits their availability at home. Therefore, it could be envisaged to create a joint pool—financed by all countries willing and able to participate—of critical homeland security capabilities.

Create a Collaborative Homeland Security CDE Environment

Concept development and experimentation is key for transformation. Therefore, a collaborative transatlantic homeland security CDE environment should be created that includes NATO's Allied Command Transformation, the European civil-military planning cell in the EU Military Staff, the European Commission, emergency responders from NATO and EU countries, the industry, and academic research institutes. The main purpose would be to devise and continuously develop a single set of homeland security scenarios relevant to testing strengths and weaknesses of current preparation and prepared-

ness as well as existing capabilities. The virtual test environment could be linked with different education institutions across the countries involved.[17] Iterative interaction between all actors engaged would greatly accelerate the introduction of cutting-edge technology into platforms and systems for emergency responders as well as the development of doctrine, training, and education for interagency operations in the homeland security framework.

Set Up a Transatlantic Homeland Security Clearing House and Training Program

A transatlantic homeland security clearing house and joint training program should be established. The clearing house would focus on eliciting lessons learned from most recent homeland security operations, such as the floods in the Gulf of Mexico or in Europe or after action reviews of the London and Madrid bombings. In the United States, the National Memorial Institute for the Prevention of Terrorism has set up the "Lessons Learned Information Sharing" database accessible to emergency responders, where lessons learned, best practice, reports, and documents are stored and shared.[18] NATO and the EU could join forces in setting up a similar Web site, thereby taking into account the civil emergency planning expertise already built up within these organizations. Information gathering and exchange should be complemented by joint training based on tabletop, computer-assisted, and real-world exercises. The provision of support for the United States in the aftermath of hurricanes Katrina and Rita by European and non-European countries makes clear that even very local homeland security contingencies can have an important international dimension. Cooperation for these and other purposes needs to be trained in advance in order to improve interoperability between the different actors involved.

[17] The U.S. Joint National Training Capability, which aims at implementing a simulation environment to train joint, multinational interagency operations, could be used as one of the building blocks. See: Stuart H. Starr, "The Challenges Associated with Achieving Interoperability in Support of Net-Centric Operations," (paper presented at the 10th ICCRTS Meeting, Washington, DC, June 2005), p. 14.

[18] Steinhäusler and Edwards, *NATO and Terrorism*, p. 138.

Think About a Transatlantic CROP

Different situation centers operated by the EU and NATO should be linked with the aim of providing a transatlantic CROP. The EU maintains the Joint Situation Center with the Council General Secretariat, the Monitoring and Information Center, and the Directorate External Relations Crisis Room both in the Commission and the EU Satellite Center. In addition, the Commission maintains and builds up various expert networks aimed at rapidly exchanging information.[19] Integrating information from these various sources into a joint picture, to be complemented by NATO instruments, would greatly add to the joint situational awareness and understanding of transatlantic partners. By improving understanding and awareness, access to information serves as a confidence and security building measure. Today's CROP is thus the contemporary equivalent of the on-site inspections and verification missions that were the hallmark of the Conference and, later, Organization for Security Cooperation in Europe. Therefore, it would make sense to provide access to the CROP and its underlying database to as many countries of the Euro-Atlantic Partnership Council as possible.

Create Homeland Security Science and Technology Programs

Many of the most demanding homeland security tasks, such as counter-terrorism, combating threats against transportation means, cyber security, or traveler authentication, require science and technology support. In 2004 the European Commission launched the Preparatory Action in Security Research, which will lead to the inclusion of security research in the 7th EU Framework Research Program starting in 2007. Homeland security is one of the key areas of these programs. At the same time, the U.S. Department of Homeland Security, in cooperation with other departments and agencies, has launched an ambitious homeland security research program and set up new initiatives to leverage the contribution of the industry and the scientific community.

So far, transatlantic cooperation on homeland security science and technology remains limited. Given the fact that the adoption of cer-

[19] For more on this, see the chapter by Gustav Gustenau in this volume.

tain technology solutions can have wide-ranging effects, not only on technical standards but also on solutions that need to be adopted in other countries because of the first mover's decision (the U.S. Container Security Initiative is a case in point), the lack of cooperation is a problem.[20] The dialogue forum should thus also serve to launch a joint research agenda with common research projects closely related to the needs of joint capabilities planning. Discussing and defining standards for homeland security application is one of the priority areas that should be addressed. Other issues include techniques to advance data mining and data fusion, CBRNE detection, biometrics, the use of radio frequency identification (RFID) in a range of applications, improvement of personal protective equipment of first responders, and, last but not least, modeling and simulation.[21]

Strengthen Resilience from Within in Neighboring Countries

At the outskirts of the Euro-Atlantic community, fragility is prevailing. While the European Union and NATO were successful in exporting stability to those countries that have recently joined them, the same has not yet been achieved in most parts of Northern Africa, the Greater Middle East, or Central Asia. Like the industrial world, the security apparatus of these countries needs to be adapted as well in order to cope with the new security risks. So far, most activities have either focused on advancing the security sector reform agenda with a prime focus on democratic security sector governance[22] or on bilateral train and equip programs to beef up certain security forces. It is high time for the transatlantic community to recognize that more should be done to strengthen resilience within their neighboring countries.

Resilience refers to the ability to recover from shock or disturbance. As was argued above, homeland security is designed to help prevent the rise of security risks, to provide mitigation in case of escalation, and facilitate the return to pre-crisis living conditions. Transferring the

[20] See here: Josef Braml, "Atlantische Auswirkungen amerikanischer Heimatschutzpolitik" [Transatlantic Implications of U.S. Homeland Security], *SWP-Studie* 30, Berlin: SWP, 2005.

[21] For additional suggestions, see: Steinhäusler and Edwards, *NATO and Terrorism*, pp. 144-160.

[22] Heiner Hänggi and Fred Tanner, *Promoting Security Sector Governance in the EU's Neighbourhood.* Chaillot Paper No. 80 (Paris: EU Institute for Security Studies, 2005).

principles of homeland security transformation to neighboring countries would thus serve the dual purpose of improving security in current hot spots and thereby reducing risks for the transatlantic community as well. Although this step alone will not bring lasting peace to the most serious pockets of crises, it can be interpreted as a very important first step. Priority issues to be addressed should include training, education, and organizational and materiel reform based on the principles of transformation. In addition, technical support should provide these countries with access to the most important international databases relevant for homeland security, such as the European and U.S. fingerprint databases, health care databases maintained by the European Commission (such as the Rapid Alert System for Biological and Chemical Agent Attacks), the new European Center for Disease Prevention and Control, and the U.S. Center for Disease Control, as well as warning information networks for critical infrastructure. The last issue deserves particular attention because of the strategic dependence of Europe and the United States on oil and gas resources in the Arabian Peninsula, Central Asia, and Russia. Given the current pattern of terrorist activities, energy infrastructure security in countries of origin and in countries of transit can be singled-out as one of the most important issues of homeland security in these regions and in the transatlantic area as well.

Consider Critical but Neglected Watch-Out Issues

To round off the proposed agenda, the transatlantic community would be well advised to use the dialogue forum to address some neglected long-term issues that are already looming on the horizon. One of these issues is the homeland security impact of privatizing hospitals and medical services. Countries with privatization experience, such as the United States and the United Kingdom, could advise countries like Germany that are about to follow suit. Questions to be addressed could refer to guaranteeing equal standards of training and education among hospital staff in public and private hospitals, providing an adequate number of beds and special treatment facilities (for instance for decontamination), or compensating hospitals for maintaining idle capacities to manage the most demanding homeland security tasks such as CBRNE attacks.[23]

[23] Steinhäusler and Edwards, *NATO and Terrorism*, pp. 152-153.

Another critical issue is the homeland security impact of Europe's aging societies. On the one hand, the pool of people available for emergency response will decline. Together with the growing population concentration in cities, this can lead to serious shortcomings of available capacities in rural areas.[24] In addition, serious questions need to be asked with regard to the level of expertise available among reserve emergency responders and their ability to provide adequate assistance with CBRNE scenarios. Who makes sure that they receive the necessary training, and who pays for it? On the other hand, elderly people require different treatment techniques and drugs. Who is responsible for the provision of these services in times when public health systems and social security are under heavy financial pressure?

Finally, the nexus between homeland security, urban living, and urban development must receive more attention, as big cities are among the most favored targets of terrorist activities. Given the new risk environment, it is necessary to review the preparedness of major cities in dealing with catastrophic terrorisms and other likely homeland scenarios. However, possible negative side-effects should not be overlooked. Based on the experience in New York, Peter Marcuse warns that the "war on terrorism is leading to a continued downgrading of the quality of life in US cities, visible changes in urban form, the loss of public use of public space, restriction on free movement within and to cities, particularly for members of darker-skinned groups, and the decline of open popular participation in the governmental planning and decision-making process."[25] Such warnings need to be taken seriously, because too much is at stake if we ignore potentially detrimental effects of homeland security. It is thus most important that the exchange of lessons learned suggested above address these issues as well.

---

[24] "Im Assistenzeinsatz für das Rote Kreuz. Pilotversuch: Weil Freiwillige fehlen, machen Heeres-Sanitäter Dienst im Rettungswesen," [Assisting the Red Cross. Pilot Project: Army Medical Personnel to Tackle the Shortage of Volunteers], *Kurier*, 4 July 2004, p. 9. See also: "Preparing for Public Health Emergencies: Meeting the Challenges in Rural America. Conference Proceedings and Recommendations" (Boston: Harvard School of Public Health, Center for Public Health Preparedness, 2004);

[25] Peter Marcuse, "The 'War on Terrorism' and Life in Cities," in *Cities, War and Terrorism. Towards an Urban Geopolitics*, ed. Stephen Graham (Oxford: Blackwell Publishing, 2004), p. 264.

Chapter 2

From Territorial Security to Societal Security: Implications for the Transatlantic Strategic Outlook

Esther Brimmer

Defending the nation is the premier responsibility of the state. For millennia, defense has primarily been understood as protection of territory. For generations, emperors, kings and heads of state around the world concentrated on stopping invasions by enemies who were bent on seizing land, resources, or people. However, in our globalizing world simply securing the borders against attack by another country's army is not adequate. "Homeland security" should be more than just defending territory. Too narrow a definition of "homeland security" can lead to inappropriate policies that can erode the basic values of democracy.

Safety depends not only on territorial integrity, but also on "societal security." This chapter will explore what societal security means in the context of homeland security and the implications for the United States, the transatlantic community, and NATO. I will argue that homeland security is an important component of societal security, but that homeland security is a *subset* of societal security. Therefore, while we endeavor to improve homeland security we must not erode fundamental elements of societal security. Moreover, these concepts help us understand the difference between allies and partners in national security. While partners are important for homeland security efforts, permanent allies not only contribute to homeland security, but to societal security as well.

Evolving conceptions of national security

Traditional theories of national security focus on the security of the state. The objective is to protect the country's territory, preserve the well-being of the ruler, and maintain the continuity of the govern-

ment. During the Cold War, the U.S. and its allies needed to contend with the existence of the Soviet Union and its capacity to destroy other countries with nuclear weapons. For decades, NATO strategy reflected similar concerns. In the shadow of the looming Soviet threat, the Alliance was founded to secure its members, which was defined as defending their territorial integrity. Article 6 of the 1949 Washington Treaty explains that the treaty covers armed attack "on the territory of any of the Parties in Europe or North America" and "on the forces, vessels, or aircraft of any of the Parties" when in Europe, the Mediterranean "or the North Atlantic area north of the Tropic of Cancer."[1] However, territorial defense did not extend to far-flung military engagements, such as Vietnam, nor to domestic upheaval.[2]

Even important reevaluations of NATO's mission maintained the over-riding importance of territorial defense to the Alliance. For example, the 1967 Harmel report noted:

> The Atlantic Alliance has two main functions. Its first function is to maintain adequate military strength and political solidarity to deter aggression and other forms of pressure and to defend the territory of member countries if aggression should occur.[3]

Immediately after the fall of the Berlin wall, defending the United States against military invasion was still the leading goal as articulated in the 1990-1991 National Security Strategy of the United States (with international terrorism in second place):

The United States seeks, whenever possible in concert with its allies, to:

> — deter any aggression that could threaten its security and, should deterrence fail, repel or defeat military attack and end conflict on terms favorable to the United States, its interests and its allies;

---

[1] "The North Atlantic Treaty" (Washington, D.C., April 4, 1949), Article 6. Available at http://www.nato.int/docu/basictxt/treaty.htm

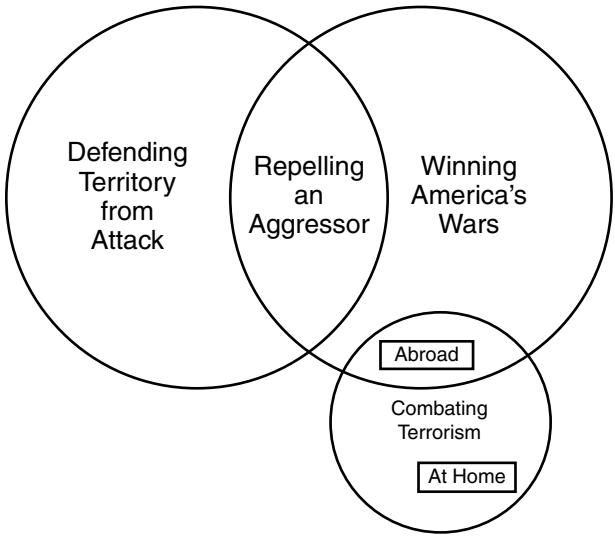
[2] However, the 1949 Treaty did originally include French Algeria, but this clause was rendered inapplicable by Algerian independence in 1962.

[3] "The Future Tasks of the Alliance ('The Harmel Report')," (Brussels: December 13-14, 1967), para. 5. Available at http://www.nato.int/docu/basictxt/b671213a.htm

> — deal effectively with threats to the security of the United States and its citizens and interests short of armed conflict, including the threat of international terrorism;[4]

American national security policy at the end of the Cold War can be represented as interlocking circles linking territorial security and advancing international goals. The military's primary goals were to defend the territorial integrity of the United States and to win wars. Combating terrorism was an element of national security, but was tertiary behind these other two missions. Indeed international anti-terrorism efforts were largely the province of civilian agencies including the Department of State and the Central Intelligence Agency. The Federal Bureau of Investigations (FBI), housed in the Department of Justice, led domestic anti-terrorism action, which was seen in a law enforcement context.

Figure 1. Traditional Military Roles in U.S. National Security



[4] George Bush (Sr), *National Security Strategy of the United States 1990-1991*, (Washington, D.C.: Brassey's (US), 1990), p. 8.

Conceptions of security evolved as the postwar period unfolded. In 1993, the Clinton Administration expressed a vision of post Cold War engagement strategy based on four components:

1. Strengthening the community of major market democracies
2. Fostering new democracies and market economies
3. Dealing with "backlash" states
4. Meeting humanitarian goals.[5]

Much of the 1990s was concerned with the last element and trying to understand the impact of humanitarian crises on the Euro-Atlantic area. How close did an internal conflict have to be before leaders saw it as enough of a threat to take military action? Was it proximity (Bosnia) or the magnitude of the horror (Rwanda) that was decisive? Chart 2 displays these goals. Each pillar contributed to the overall engagement strategy, but the first two were more important.

Weary of battles in the Balkans, shamed by the lack of response in Rwanda, and finally rallied to action in Kosovo, western leaders' understanding of security continued to broaden during the 1990s. Instability, disorder and massive human rights violations were threats to international peace and security and western well-being even if they were not direct attacks on allied soil. The evolution is evident in the1999 Strategic Concept, in which NATO stated "NATO's essential and enduring purpose, set out in the Washington Treaty, is to safeguard the freedom and security of all its members by political and military means."[6]

Figure 2. The Clinton Administration's Strategy of Engagement

Clinton Administration Post Cold War Engagement Strategy (1993)			
1	2	3	4
Strengthening community of market democracies	Fostering new democracies and market economies	Dealing with "backlash" states	Meeting humanitarian goals

[5] Anthony Lake, "From Containment to Enlargement," Speech at the Johns Hopkins School of Advanced International Studies, Washington, D.C., September 21, 1993. Available at http://www.mtholyoke.edu/acad/intrel/lakedoc.html

[6] North Atlantic Council, "The Alliance's Strategic Concept," (Washington, D.C.: April 23-24, 2005), para. 6. Available at http://www.nato.int/docu/pr/1999/p99-065e.htm

The Alliance expressed concern over the spillover effects of failing states and destabilized regions, but these were not seen as direct threats to the allied countries.

> Risks to Allied security are less likely to result from calculated aggression against the territory of the Allies, but rather from the adverse consequences of instabilities that may arise from the serious economic, social and political difficulties, including ethnic rivalries and territorial disputes, which are faced by many countries in central and eastern Europe. The tensions, which may result, as long as they remain limited, should not directly threaten the security and territorial integrity of members of the Alliance. They could, however, lead to crises inimical to European stability…[7]

Thus, by the end of the 1990s world leaders began to understand that national security serious threats could come from nontraditional sources such as non-state actors and internal conflicts.

9/11 and Asymmetric Challenges

The terrorist attacks of September 11, 2001, highlighted and amplified an on-going trend: the NATO allies faced a range of asymmetric threats and challenges from non-state actors, willing and able to strike western targets at home and abroad. The new element was that the threat was not just spillover from humanitarian crises far from orderly powerful countries, but direct attacks at home. Not only would the terrorists strike western embassies or military installations abroad, they would strike at the core of the western system.

Non-state actors were already a significant problem for international leaders. The Balkan wars of the 1990s had already demonstrated that European stability could be deeply affected by turmoil outside the territory of NATO members. Militias, insurgents and other groups, which were statistically weaker than European militaries could still wreak havoc, massacre civilians and ensnare peacekeepers. In these theaters of action conventional militaries and peacekeepers could be stymied by smaller, "weaker" and hence "asymmetric" elements.

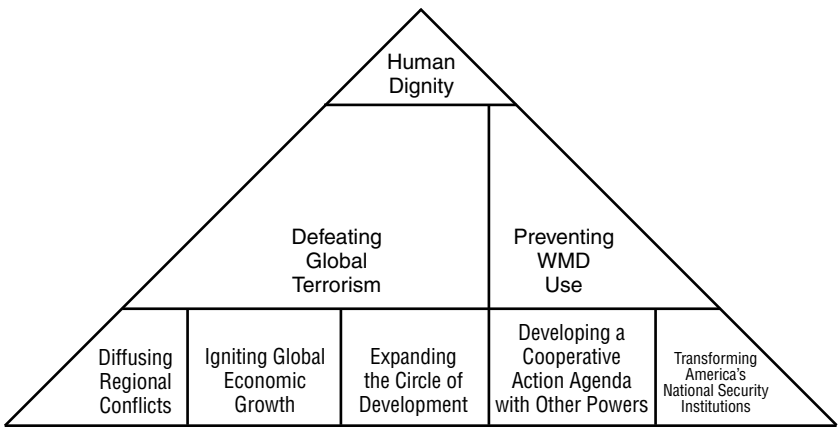
---

[7] "The Alliance's Strategic Concept agreed by the Heads of State and Government participating in the meeting of the North Atlantic Council," (Rome: November 8, 1999), paragraph 9. Available at http://www.nato.int/docu/basictxt/b911108a.htm

The 9/11 attacks showed that a small group of well-organized terrorists could kill thousands of civilians. Modern technology can make a small group capable of being highly lethal. From the dramatic example of using an airplane as a bomb to exploding a homemade—but effective—device in a subway system, terrorist cells can use tools to inflict large-scale damage and loss of life. Moreover, the Internet facilitates communication, enabling terrorists to spread grievances and their own interpretation of issues. Rather than worrying about state-led invasion, many national governments are contending with decentralized threats from terrorist cells and networks.

Written in the wake of 9/11, the 2002 U.S. National Security Strategy begins to raise these issues, but does not go far enough. It identifies several spheres of security, combating terrorism, winning America's wars, and defending the United States from attack. As Chart 3 shows, the Bush Administration gives priority to human dignity and bases this goal on diffusing regional conflicts, igniting global economic growth, expanding the circle of development, developing agendas for cooperative action with other powers, and transforming America's national security institutions. However, two other goals, defeating global terrorism and preventing enemies from using weapons of mass destruction have dominated Administration policy.[8]

Figure 3. The National Security Strategy of the United States



[8] George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: September 2002), pp. 1-2. Available at http://www.whitehouse.gov/nsc/nss.html

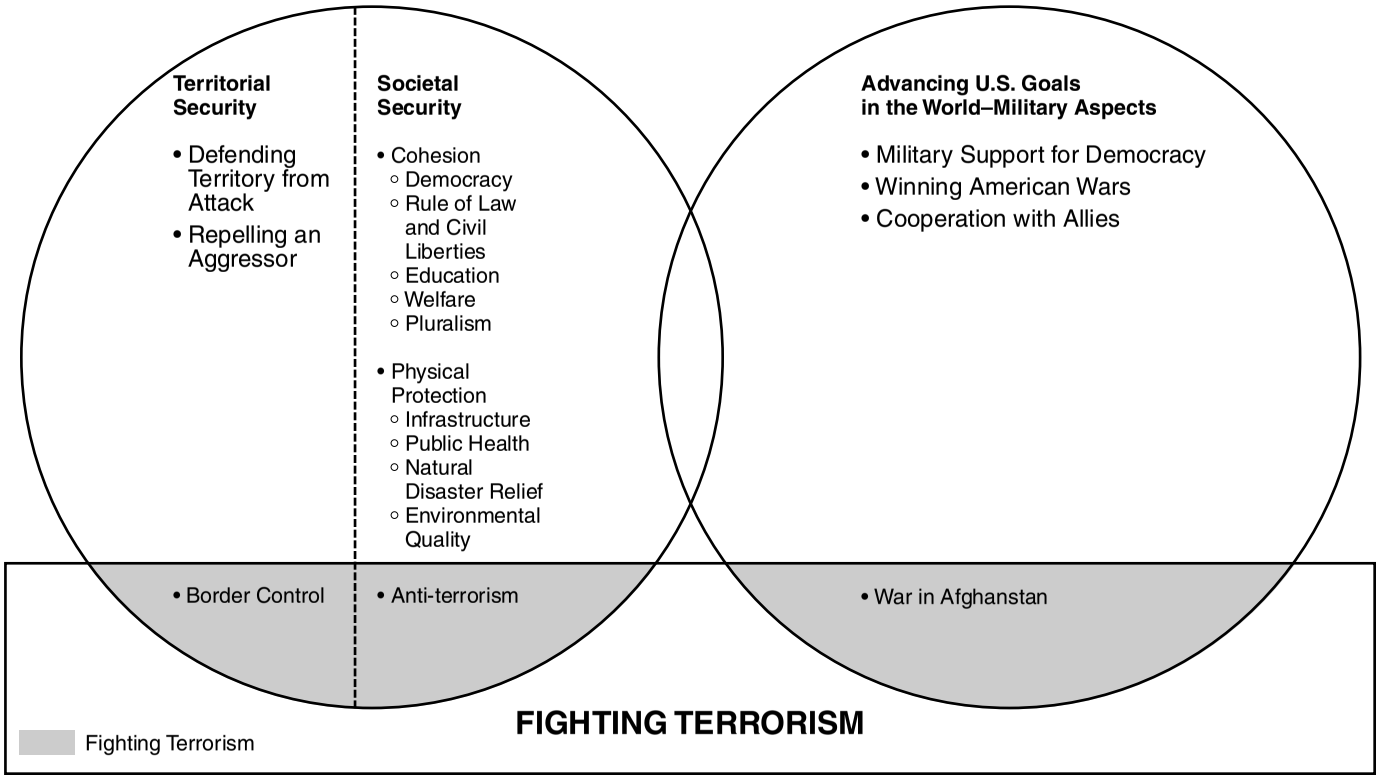
Societal Security

The 2002 National Security Strategy focuses on anti-terrorism efforts. However, Al Qaeda and similar groups pose a more complex challenge to the United States and its allies. They attack to create mayhem, not to invade and run a country. They are not trying to achieve a defined political change in the U.S., but they would like to erode international support for western societies. While members of Al-Qaeda want the U.S. to stop supporting the Saudi regime, most of the groups and individuals loosely associated with Al Qaeda have much more diffuse agendas. These terrorists are not freedom fighters seeking territorial independence for a colony or specific region. They do not want to obtain U.S. land or run the U.S. government. They do not want to seize resources or people. Instead they want to undermine western society.

Defending against modern transnational threats requires a more holistic understanding of security. A delicate web of values, connections, and infrastructure characterizes the modern globalized world. Striking out against this form of modernity means trying to destroy those connections. This chapter argues that defending our societies requires a broader understanding of our objective. Homeland security includes not only preventing an attack, physical protection of assets, and consequence management, but also respect for the character of the society that it seeks to defend. Yes, we need homeland security, but this must be embedded in a larger notion of "societal security." This approach can create a more useful context for homeland security and the transatlantic alliance.

Societal security should focus on protecting people and the vital connections of society from catastrophic manmade or natural threats. As shown in Chart 4, societal security should be an integral part of America's strategic outlook. A more comprehensive understanding of America's strategic position should include societal security alongside territorial security and in conjunction with the country's international goals.

Figure 4. Societal Security and the Strategic Outlook



Ultimately, we want to enhance human safety to achieve societal resilience. Our society should be able to withstand an attack, mute its effects, and recover from the assault. These objectives should inform security priorities.

I posit that societal security should be composed of two elements: cohesion and physical protection. In this context, cohesion refers to the values and qualities that bind a community together which are relevant to security, which are: democracy, the rule of law and civil liberties, education, welfare, and pluralism. Our security policies must not degrade these features, which are central to what makes our society worth defending in the first place.

Democracy is a fundamental component of creating a just society providing a mechanism for the governed to select their leaders and participate in decision-making. A just society is better and more stable than an unjust one (although the transition to democracy can be destabilizing). The rule of law and civil liberty promote and protect equality and liberty and create the political climate of trust necessary for the connections of modern life to thrive. Education and adequate economic well-being are crucial for the human spirit to flourish. Lack of access to education and social exclusion or degradation undermine cohesion. Pluralism is particularly important, but not well understood. Pluralism defends a diversity of cultural and religious expressions within a framework of tolerance guided by certain rules. Pluralism requires that all accept certain principles, including respect for others. Unlike multiculturalism, which tends to confine people in separate cultural traditions, the concept of pluralism better allows each person to fulfill complex multiple identities while maintaining overall cohesion.

The elements of physical protection include infrastructure, public health, natural disaster relief, environmental quality and anti-terrorism measures aimed at thwarting attacks within the U.S. In my societal security model, fighting terrorism is portrayed as a crosscutting policy, not a fundamental sphere of security. Fighting terrorism is an important policy action, but it should not be the defining framework for our strategic outlook.

We can draw on several theoretical traditions to understand how to arrange priorities within the concept of societal security. Our efforts

to enhance human safety can benefit from a rich theoretical tradition that endeavors to highlight the role of the individual person in international affairs. In this section I will draw from four traditions: common security, human needs, human security and Nordic notions of societal security. The first three emerge from policy debates within the economic development community. From their efforts to define the good society and hence the ultimate goal of development, development experts honed useful concepts about ways to enhance human well-being that can help us understand which themes are most important when developing our notion of human safety within societal security.

In the latter portion of the Cold War, there were significant efforts to recover notions of human value amid the overwhelming concern with state security and the threat of nuclear war between the superpowers. In their reports *North-South: A Program for Survival* (1980) and *Common Crisis: North-South Cooperation for World Recovery* (1983), the Independent Commission on International Development Issues led by former German chancellor Willy Brandt sought to connect development issues and strategic world order concerns. The Brandt Commission discussed the interplay between social issues that directly affect people such as hunger, poverty, and human rights with international economic and security affairs. The related notion of common security derives from a celebrated international report of the same name issued by the Independent Commission on Disarmament and Security Issues in 1982. This commission led by Swedish Prime Minister Olaf Palme stressed that both East and West had a common interest in safety and that security had to be achieved together.[9] Taken together these well-publicized reports by political leaders raised the idea that security needed to include the well-being of people.

The notion that national policies needed to connect to people' s well-being was advanced further by the concept of "basic needs."

[9] See Independent Commission on International Development Issues, *North-South: A Program for Survival*, (Cambridge, MA: MIT Press, 1980); The Brandt Commission, *Common Crisis: North-South Cooperation for World Recovery*, (London: Pan Books, 1983); and Independent Commission on Disarmament and Security Issues, *Common Security: A Programme for Disarmament*, (London: Pan Books, 1982); and Andrew Butfoy, "Changing Western Conceptions of Global Security," New Security Agendas, I, available at http://www.arts.monash.edu.au/ncas/teach/unit/pol/chpt05.html

Again, ferment within the development community produced an idea that economic development needed to be geared towards the fundamental elements that sustained human life, not just towards large infrastructure projects. Thus, reducing poverty and hunger or increasing literacy were just (or even more) valid measures than the number of highways or bridges built. If economic development can be linked to human well-being, then the notion that security can be connected to human safety is not a big step.

The third framework discussed here, human security, endeavors to make a direct connection between personal safety and national security. Concepts of human security can help us prioritize what features must be maintained for human well-being. Human security endeavors to use the person rather the state as the unit to be safeguarded, but it also acknowledges that people need social constructs for well-being (provision of food, maintenance of health, etc.).

There have been several efforts to define human security. Indeed, the idea suffers from significant theoretical imprecision.[10] However, within the more coherent expressions of the idea certain core notions can be discerned. The concept of human security appears in a 1994 report by the United Nations Development Program (UNDP). Scholars such as Gary King and Christopher Murray tried to analyze the idea more deeply. Meanwhile, the Canadian and other governments tried to translate the theory into policy. There was even a report on human security by a distinguished international panel headed by the former UN High Commissioner for Refugees Sadako Ogata and Nobel laureate Amartya Sen.[11] Each analysis has a somewhat different definition. Table 1 lists definitions of human security according to the UNDP, King and Murray, and my definition.

---

[10] Roland Paris, "Human Security: Paradigm Shift or Hot Air," *International Security* 26 (Fall 2001): p. 99.

[11] See United Nations Development Program, *Human Development Report* (New York: Oxford University Press, 1994), pp. 22-38; Gary King and Christopher Murray, "Rethinking Human Security," Harvard University, May 4, 2000,accessed at http://gking.harvard.edu/files/hs.pdf; Canadian Department of Foreign Affairs and International Trade, www.dfait-maeci.gc.ca/foreignp/humansecurity/menu-e.asp and Commission on Human Security. *Human Security Now: Protecting and Empowering People* (New York: Commission on Human Security, 2003). Available at www.humansecurity-chs.org

TABLE 1[12] Various Definitions of Human Security

UNDP Definition	King & Murray	Brimmer
Economic security	Income	Food
Food security	Health	Health
Health security	Education	Personal safety
Environmental security	Political security	Political freedom
Personal security	Democracy	Economic security
Community security		Cultural expression
Political security		Environmental quality

While various models of human security exist, most include personal safety, health, and food. A societal conception of security should include providing these three as part of its homeland security plan. Moreover, just as concepts of common security have a notion of mutuality and human security implies interplay between factors that sustain well-being, so our idea of societal security must also include protecting the rich connections that sustain modern life. Food security means not just phytosanitary precautions, but also safeguarding the intricate just-in-time network that brings foodstuffs to cities, many of which have only a few days' supplies available at any one point in time. Other examples of critical networks can be found in the deeply integrated transatlantic realm.[13]

The fourth tradition derives from Nordic conceptions of societal security. During the Cold War neutral countries such as Finland, Sweden, and Switzerland developed notions of "total defense" that enlisted civilian and military resources.[14] In the post Cold War period this idea is evolving towards societal security. However, different analysts ascribe somewhat different features to the term "societal security." Swedish expert Bengt Sundelius develops the notion of "embedded societal security" which addresses society's vulnerabilities through a "comprehensive system for crisis management." This con-

[12] UNDP, pp. 24-25, and Gary King and Christopher Murray, *op cit*, p. 13.

[13] See Daniel Hamilton and Joseph Quinlan, *Partners in Prosperity: The Changing Geography of the Transatlantic Economy* (Washington, D.C.: Center for Transatlantic Relations, 2004) and Daniel Hamilton and Joseph Quinlan, eds., *Deep Integration: How Transatlantic Markets are Leading Globalization* (Washington, D.C.: Center for Transatlantic Relations, 2005).

[14] See Daniel Hamilton, ed., *Protecting the Homeland: European Approaches to Total Defense and Societal Security and their Implications for the United States* (Washington, D.C.: Center for Transatlantic Relations, 2005).

cept creates a new level of security between national defense against attack and relief from domestic disasters.[15] This conception of societal security focuses on physical protection and consequence management; and, therefore, could be considered societal defense.

Danish researcher Ole Wæver links identity and security: "Societal security is about those ideas and practices that identify individuals as members of a social group"[16] This theoretical construct can contribute to our notion of cohesion. Security should be organic and not destroy what it seeks to save. This notion reinforces the importance of protecting civil liberties amid efforts to improve security. According to Wæver, security should protect that which is "existential."[17] He links societal security linked to identity. For example, his notion of societal security would defend the construction known as "Europe."[18] For him, a notion of solidarity is important to societal security. This idea informs this chapter's conception of cohesion.

Homeland Security

Having described the sources of societal security we can delineate which elements are part of homeland security. As Chart 5 shows, homeland security should complement both aspects of societal security and include elements of cohesion and of physical protection. The parts of cohesion relevant for homeland security are the rule of law and civil liberties because these constrain the law enforcement powers that are used in homeland security, but which could undermine key values in society. Within physical protection, infrastructure, public health, natural disaster relief and anti-terrorist activity are relevant for homeland security. These are part of the delicate web of modern interconnections. In contrast, environmental quality is important for physical well-being, but not central to homeland security. Beyond having a basic level of safe drinking water and clean air, the relative air quality or water management are part of societal security, but not to defense of the homeland. Not everything needs to be about national defense to be important.

---

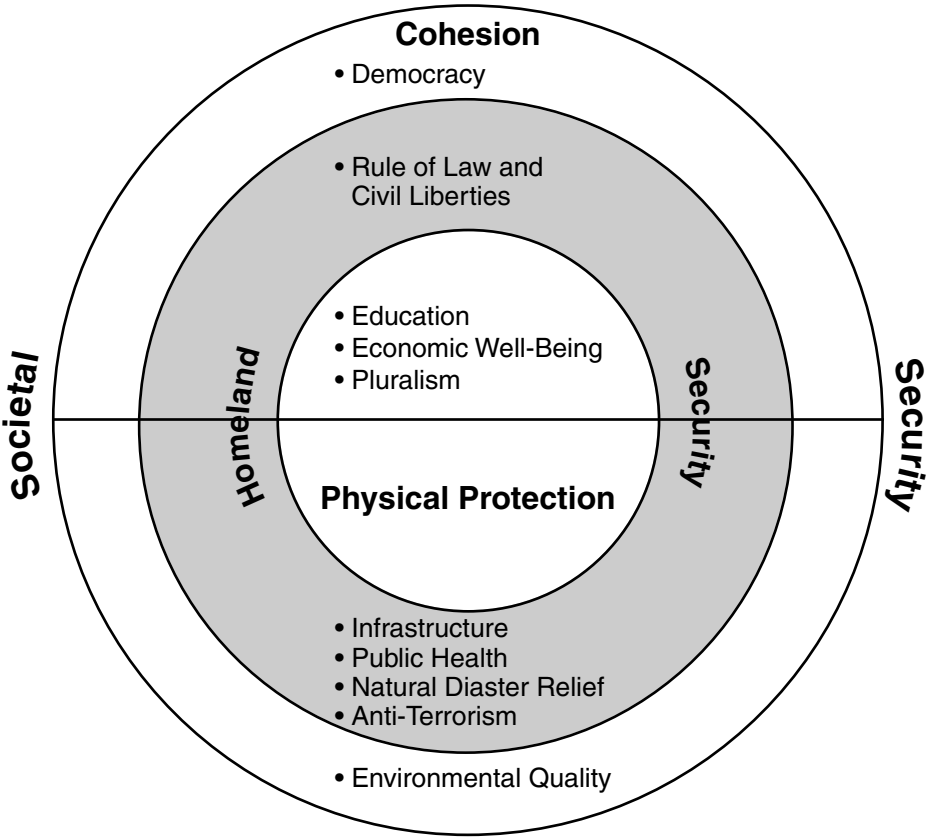
[15] Bengt Sundelius, "From National Total Defense to Embedded Social Security," in Hamilton, ed., *Protecting the Homeland.*

[16] Ole Wæver, "Identity, Integration, and Security: Solving the Sovereignty Puzzle in E.U. Studies," *Journal of International Affairs,* Winter 1995, vol. 48, no. 2, pp. 389-431, p. 405.

[17] Ibid.

[18] Ibid, p. 407.

Chart 5. Societal Security and Homeland Security



In this view of homeland security, physical protection should focus on infrastructure, public health, natural disaster relief and anti-terrorism. Efforts to protect infrastructure should include defending "nodes," critical intersections in the economy that are necessary for society to function. These could include power stations, major ports or Internet hosts. These nodes are crucial for the smooth movement of resources and information. Homeland security would address alternate power sources, supply routes or telecommunications links to back-up these nodes as well as safeguarding the critical power plant and telecom workers needed to run these nodes.

Adequate public health structures are important for people's wellness, but also to help the population recover from a terrorist attack. Thus, homeland security efforts need to include measures to stockpile the means to heal and sustain people in a crisis. Competent mechanisms for relief after a major natural catastrophe are also part of homeland security. One reason to take an all-hazards approach to homeland security is that terrorists and natural catastrophes alike can break crucial societal links. Improving major disaster relief can help strengthen the lines of communication and planning that would be crucial to sustain society after a terrorist attack.

Anti-terrorism is, of course, a basic element of homeland security. Officials such as President Bush and others have devoted significant time and energy to anti-terrorist actions. Preventing attacks within one's own country is vital. National and local leaders in many countries need to focus on this aspect of security, but they should not do so exclusively. It is not the only aspect of homeland security. Taking too narrow a definition of homeland security can leave the country unnecessarily vulnerable. Therefore, a notion of societal security is needed.

Providing society security draws on many parts of the national government. How to allocate resources is an important national decision. Different countries make different choices as explained in several chapters of this book. Our societies need to draw on a wide array of resources to address a richer concept of security. This chapter posits that in the case of the United States, the military should have a role in coordinating with the Department of Homeland Security in three areas of physical protection: infrastructure, natural disaster relief, and aspects of anti-terrorism. The military must work with civilian agencies and, in some cases, the private sector on protecting critical infrastructure. The military can support civilian agencies and should be better linked to the Federal Emergency Management Agency (FEMA) which must take a more active role in relief after a major disaster. FEMA's role is currently woefully inadequate as was demonstrated after Hurricane Katrina. However, in deference to the United States' domestic legal traditions, the expression of military support for disaster relief should be an enhanced National Guard with special homeland security units. In the area of anti-terrorism the military plays a vital role linking the use of force or forcible means internationally and domestic security. For example, military assets can help deal with the

movement of illegal substances on the high seas or hijacking of aircraft or ships. The military should support the Coast Guard in monitoring the movement of people, making the interface between the Navy and Coast Guard even more important. The use of military force was necessary to topple the Taliban, which had sheltered Al Qaeda and the perpetrators of the 9/11 attacks.

Implications for the Transatlantic Strategic Outlook: Allies and Partners

This chapter argues that societal security is composed of cohesion and physical protection. Even with its dominant multifaceted power, the United States cannot provide for internal societal security without the assistance of other countries. Domestic cohesion is based on the quality of our democracy; however, as Americans have understood for six decades, American democracy benefits from having stable democracies in Western Europe and elsewhere. Moreover, the speed and depth of globalization across the Atlantic means that American society is even more closely integrated with Europe than before. True cohesion is based on values. Therefore, the U.S. can only build cohesion, and, thus, societal security with countries that share the same values. The transatlantic community can be called a community because its members share values. Improving relations among its members enhances societal security. How far this community extends is the subject of current debate and underlies questions of the enlargement of the European Union, NATO, and other Euro-Atlantic organizations. The crucial difference between "allies" and "partners" is that allies not only sign collective defense treaties to assist each other, they also contribute to cohesion. Partners may help with physical protection and tactical measures, but are not part of the circle of cohesion. Partners can work together in the anti-terrorism campaign; they can cooperate to defend airspace and sea lanes, but they do not share sufficiently common values to be part of sustaining cohesion.

This analysis of allies can inform our understanding of the role of Euro-Atlantic institutions in societal security. The United States, Canada, and most of Europe share sufficient values to contribute to each other's cohesion.[19] The alliance of twenty-six countries in the

[19] The U.S. also shares values with other countries such as Australia, Japan, and New Zealand, and these countries contribute to cohesion. However, this chapter focuses on transatlantic issues.

region, NATO, contributes to societal security. NATO efforts to support homeland security should concentrate on these areas where it can help both aspects of societal security. NATO reinforces cohesion by emphasizing civilian control of the military, especially when admitting new member states as it has over the decades. This is an aspect of the rule of law, the component of cohesion most relevant to homeland security. In their pursuit of homeland security, NATO members should not adopt practices that undermine the values they share.

NATO plays a greater role in physical protection. Territorial defense is the classic form of physical protection; and was the alliance's principle mission since its founding. As a military alliance, NATO's homeland security activities should complement the role of the military in its member states' physical protection plans. While different states interpret this role differently, there is still scope for NATO to help with infrastructure protection, natural disaster relief, and anti-terrorism efforts. Member states can use NATO auspices to exchange information among militaries on certain aspects of protecting critical nodes. NATO, in cooperation with civilian authorities, could also help channel military assets to member states to after a major natural disaster. NATO can also bring its military force to bear to address military threats that foster terrorism. Thus, it is appropriate that NATO invoked Article 5 after 9/11 and that NATO is deployed in Afghanistan. NATO also provides a security framework formally linking North America and Europe. The logic of Article 5 rests on the notion that an attack form outside on the member states' territory is a threat to all. Extending our concepts from territorial security to societal security means that an attack on the societal structures a member state would also be a danger to all. NATO needs to useful when a member state has to confront a thinking enemy. This chapter argues that Article 5 could be invoked to protect critical infrastructure, especially international infrastructure and to confront international terrorists, as in Afghanistan. NATO can also be a mechanism through which allies can share emergency equipment after a natural disaster.

The European Union also has a role to play in societal security, but it is complex. The chapters by Gustav Gustenau and Gustav Lindstrom discuss the EU's role further. The EU can be important to a conception of societal security in Europe. The fundamental notion of creating "an ever closer union" is premised on building cohesion among member

states. The process of European integration is based on values, which are reinforced through compliance with the Copenhagen criteria and implementation of the accession package. Thus the accession process can contribute to societal security within the EU. However, EU member states have not yet agreed on which aspects of security should be handled at the EU level and which should be national or global. Aspects of cohesion such as education and welfare are national—not EU level—competencies, as are components of physical protection such as public health and natural disaster relief. However, the creation of an EU Counter-terrorism Coordinator, an EU arrest warrant and other steps increased the EU's role. In addition, the European Security Defense Policy (ESDP) does contain civil protection measures that could become a framework for EU anti-terrorism cooperation. The EU can facilitate information exchange among member states to improve coordination among national authorities especially in the areas of physical protection and consequence management. Prevention can involve intelligence cooperation and detention before an expected attack is an even more politically sensitive activity. National governments will want to keep control of rules for intelligence sharing and preventive detention, rather than cede these to Brussels.

Not all of societal security involves military assets or intelligence sharing. Instead, the strength of civil structures and the political climate are also important. The health of member states' democracies is an EU concern. Indeed through the accession process, the EU can project cohesion. Whether the Neighborhood Policy for EU relations with nearby non-candidate countries can also convey cohesion remains as open question.[20] Still the EU can support societal security. The EU can reinforce some aspects of cohesion among members and contribute to physical security. EU member states will have to decide how much they want to EU to advance societal security.

Conclusion and Recommendations

From the transatlantic perspective, the notion of societal security reinforces the need to have greater contact between the U.S. and the EU on homeland security issues. The EU and its member states are

[20] It is also not clear whether EU member states want to build cohesion with nearby countries, or just bolster the Union's physical protection.

part of the realm of transatlantic societal security. To fulfill their own potential for cohesion and physical protection, states in this area need to work together. However, transatlantic cooperation on both aspects of societal security can be problematic. While countries in this region support the rule of law, they have very different conceptions of law enforcement. For example, the many parts of the U.S. permit the death penalty. Also, it is much harder to determine when societal security is under threat. A direct physical attack on territory is usually easier to see. Undermining the rule of law is harder to define and encroaches on areas that the host state may see as sovereign internal affairs. Yet, allies do comment on domestic conditions (such as the death penalty or treatment of minorities), but such reflections can cause diplomatic strain. Still there is greater scope for cooperation on societal security, but this must be understood as both cohesion and physical protection.

Based on the analysis in this chapter the following recommendations may be made:

For the United States:

Cohesion

- Ensure that homeland security measures respect American values. Limit provisions of the Patriot Act and other legislation that erode civil liberties protections.
- The United States and other NATO members should not adopt measures that undermine the values the alliance shares. Therefore, the U.S. should abide by the Geneva Conventions when holding prisoners in Guantanamo and elsewhere.
- The U.S. must not starve social programs that promote cohesion to pay for the physical protection aspects of homeland security.

Physical Protection

- The U.S. should bolster the National Guard and links between civilian and military resources.
- The U.S. should identify key nodes and focus attention on these.
- The U.S. should deepen its commitment to public health both for social cohesion and consequence management.

For NATO:

Cohesion

- NATO can exchange best practices on maintaining civilian control of the military in situations where the military works domestically to support homeland security in an alliance member country.
- NATO can also exchange best practices on cooperation between militaries and intelligence agencies that respects the rule of law.

Physical Protection and Consequence Management

- NATO can help improve exchange of information between militaries about protecting critical infrastructure, especially helping national command structures understand what other militaries can and cannot do to support homeland security in their respective countries.
- NATO can help defense ministries develop and maintain channels of communication to facilitate alliance assistance to local and national authorities in the critical days after a catastophe (with the approval of national authorities).
- NATO can build on its intelligence sharing mechanisms to tailor improvements in anti-terrorism intelligence cooperation.

Chapter 3

Transatlantic Homeland Security and the Challenge of Diverging Risk Perceptions

Gerd Föhrenbach

Over the last fifteen years, there have been significant shifts in the debate on what national security is about. Until 1991, the focus was on territorial defense. In the 1990s, the center of attention shifted to international crisis management and stabilization operations, which the nations of the West have conducted both in or close to their home region and world-wide. Since September 11, 2001, at the latest, it has become clear that this global engagement entails risks for the states involved. In light of developments such as the proliferation of weapons of mass destruction (WMD), strategic terrorism, organized crime and state failure, the debate about national security now also focuses—at least in the U.S.—on the defense of society itself, hence the term homeland security.[1]

In Europe, the debate is still by and large confined to expert circles. Although the issue of homeland security should be as important to Europeans as it is to Americans, the general public and politicians in most countries of the European Union (EU) have so far paid little attention. One of the main reasons of this development is the divergence of the respective risk perceptions on both sides of the Atlantic, which will be analyzed in this chapter.

Specifically, this article will focus on three key aspects. Firstly, the differences between the European and the U.S. risk perception, and the reasons for their divergence, will be discussed. Subsequently, the challenges resulting from these diverging risk perceptions will be

[1] See Heiko Borchert, "Schutz der Heimat und die Rolle der Streitkräfte: Einleitung," in *Weniger Souveränität—Mehr Sicherheit: Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte*, ed. Heiko Borchert (Hamburg, Berlin, Bonn: Mittler, 2004), pp. 7-16; p. 7.

examined. Finally, this article will provide suggestions on how the challenge of diverging risk perceptions could be tackled.[2]

As will be shown, Europeans altogether feel significantly less likely to be personally affected by terrorism or nuclear weapons than Americans. Furthermore, risk perceptions vary among Europe's nations, and the security problems that individual EU members perceive are not necessarily shared by their neighbors. This might eventually jeopardize the solidarity among EU members, and it could also lead to a "strategic division" of the transatlantic security partnership. Therefore, most EU members as well as the Union itself should take the issue of homeland security much more seriously.

What are the differences between the European and the U.S. risk perceptions, and why are they diverging?

The U.S. risk perception

The first sentence of the U.S. National Defense Strategy, published in March 2005, reads, "America is a nation at war."[3] A statement like this would be unthinkable in any official European defense document. Similarly, no European head of state or government calls himself or herself a "war president," as George W. Bush does. Even when taking into consideration that the connotations of the term "war" may sometimes differ on both sides of the Atlantic (think, for example, of President Lyndon B. Johnson's "war on poverty"), it is obvious that Americans perceive themselves as being confronted with severe security challenges.

Specifically, the National Defense Strategy lists four kinds of challenges: traditional (such as the classical military competition between nation states), irregular (like terrorism and insurgency), catastrophic (involving WMD or methods creating WMD-like effects) and disruptive challenges (in case an adversary develops breakthrough technolo-

[2] The author is well aware of the wealth of literature on, and the theoretical aspects of, the topic of perception in international politics. For the sake of brevity, however, this article does not analyze the perceptions and interests of the multiple actors involved in the governmental decision-shaping and decision-making processes on both sides of the Atlantic. Instead, it provides a rather subjective view on the issue.

[3] United States Department of Defense, *The National Defense Strategy of the United States of America*, March 2005, p. 1.

gies to offset U.S. advantages). As the National Defense Strategy points out, these categories overlap and the most dangerous situation arises in case of a complex of challenges.[4]

In particular, it was the terrorist attacks of September 11, 2001 and the mailings of the anthrax letters later that year which destroyed the notion of a secure American homeland. The attacks triggered the most comprehensive reorganization of the U.S. government since World War II. As a result, the Department of Homeland Security was created, consolidating 22 agencies and 180,000 employees and unifying hitherto-fragmented federal structures in a single agency.

The first National Strategy for Homeland Security was published less than one year after the attacks, in July 2002. The strategy defines six critical mission areas, on which the department's efforts have focused since: intelligence and warning; border and transportation security; domestic counterterrorism; protecting critical infrastructure; defending against catastrophic threats; and emergency preparedness and response.[5]

In sum, the U.S. approach to the issue of homeland security has been broad and quite ambitious. Still, much remains to be done. Hurricane Katrina, which struck the U.S. Gulf Coast in late August 2005, swamping large parts of the city of New Orleans, revealed various shortcomings in the response of the federal, state and local governments. Indeed, the Department of Homeland Security "flunked its first big test,"[6] as the British newspaper The Economist put it.

The European risk perception

The European risk perception is quite different. Of course, there are a number of individuals, even in senior government positions, who know about the challenges that Europe faces, and talk about them publicly. Terrorism is "knocking at Italy's door,"[7] says Giuseppe

---

[4] See *The National Defense Strategy of the United States of America*, p. 2f.

[5] See Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, p. viiif.

[6] "The Shaming of America," *The Economist*, September 8, 2005. For a critical appraisal of U.S. homeland security policy, see also Stephen E. Flynn, "The Neglected Homefront," *Foreign Affairs* 83, no. 5 (2004), pp. 20-33.

[7] Quoted in "The Next Target?," *The Economist*, July 14, 2005.

Pisanu, the interior minister, reflecting a conviction widespread among Italians that after the London bombings of July 2005 they are next. Günther Beckstein, the interior minister of the German federal state of Bavaria, argues that Germans should not "delude themselves" and that Germany as one of the leading powers in the struggle against terrorism could become the target of terrorists anytime.[8]

To learn about Europe's risk perception, one could also look at the European Security Strategy drafted by Javier Solana, the European Union's High Representative for the Common Foreign and Security Policy. The European Security Strategy considers terrorism, the proliferation of WMD, failing states and organized crime as the main security challenges. Taking these elements together, the strategy states, "we could be confronted with a very radical threat indeed."[9] It is worth noting at this point that the differences between the risk perception underlying the U.S. National Defense Strategy and Europe's Security Strategy are minor.

However, the picture changes when moving from the abstract political to the personal level. By and large, Europeans feel significantly less threatened than Americans. A survey of transatlantic trends, conducted by the German Marshall Fund of the United States in May and June 2005, asked how likely people on both sides of the Atlantic felt they were to be personally affected by the same threats. It is striking that Americans feel considerably more likely to be personally affected by international terrorism (71 percent) than Europeans (53 percent).[10] Similarly, more American expect to be personally affected by nuclear weapons (67 percent vs. 55 percent of Europeans) and by Islamic fundamentalism (50 percent vs. 40 percent of Europeans). By contrast, it is the Europeans who feel more likely to be affected by global warming (73 percent vs. 64 percent of Americans).

---

[8] Günther Beckstein, "Bedrohung internationaler Terrorismus: Was muss Deutschland für die Innere Sicherheit tun?," in *Homeland Security—Die Bedrohung durch den Terrorismus als Herausforderung für eine gesamtstaatliche Sicherheitsarchitektur*, ed. Deutsche Gesellschaft für Auswärtige Politik, Berliner Forum Zukunft, 29 April 2004, p. 5-9; here: p. 5.

[9] *A Secure Europe in a Better World: European Security Strategy*, Brussels, December 12, 2003, p. 5.

[10] See The German Marshall Fund of the United States, *Transatlantic Trends—Key Findings 2005*, p. 17f.

As a consequence, the notion that homeland security is a vital new policy field is not very widespread in Europe. It is true, the EU has taken several measures to enhance cooperation in the field of justice and home affairs (the appointment of an EU counter-terrorism coordinator and the introduction of the European arrest warrant being two prominent examples). But particularly with regard to networking civilian and military capabilities and the issues of civil protection and the protection of critical infrastructure, the Union still has a long way to go.[11]

In Germany, many politicians and opinion leaders tend to avoid the topic of homeland security for fear of sounding alarmist. Admittedly, after 9/11 there have been several changes in laws and improvements in procedures, but these changes have focused mainly on individual government departments and addressed specific deficiencies rather than enhancing inter-governmental cooperation and furthering the overall understanding of the complexity of the problems. The public debate, if there was one, has been far from comprehensive and quite often ideological preferences have played an important role as, for example, with the contentious subjects of expanding the powers of the federal criminal police office, Bundeskriminalamt, or of using the Bundeswehr for homeland security purposes).

Interestingly, homeland security moves up a little from the bottom of the German political agenda as soon as there is a terrorist attack such as the ones in London or Madrid (March 2004), but it does not take long before public attention drops again. This phenomenon may be explained, at least partly, by the self-image Germans have. Germans like to think of themselves as peaceful, well-meaning members in the family of nations. The public debate on foreign and security policy issues is often conducted in moral terms, if at all. National interests are rarely mentioned, and if they are, they are usually considered synonymous with European interests. Against this background, most Germans find it hard to understand that their open society has

[11] See Anja Dalgaard-Nielsen, "Homeland Security: American and European Responses to September 11th," in Jess Pilegaard, ed., *The Politics of European Security* (Copenhagen: Danish Institute for International Studies, 2004), pp. 159-178 and Implementation of the Action Plan to Combat Terrorism, Note to the European Council Submitted by the Presidency and the EU Counter-Terrorism Coordinator, 16-17 June 2005 [http://ue.eu.int/uedocs/cmsUpload/newWEBre01.en05.pdf].

enemies, that global politics is usually driven by self-interest, and that "hard," military power does still play an important role in international relations.

Certainly, this description does not entirely fit all EU members. France and the UK, to name just two other EU members, are less reticent about the use of force and quite outspoken in pursuing their national interests. Indeed, risk perceptions vary among the Union's twenty-five member states. The British government has taken the issue of homeland security seriously (yet it has chosen to make the changes and adjustments to its policies rather quietly, without causing many headlines in the press). In the Netherlands, too, the risk perception has changed over time. In particular, the murders of Pim Fortuyn, a maverick politician, in 2002 and Theo van Gogh, a film-maker, in 2004 brought about a recognition of the threat to the country's open society by extremism and terrorism, both Muslim and otherwise. In the Scandinavian countries of Denmark, Sweden and Norway (not an EU member), a transformation of defense concepts and civilian crisis management structures had started already in the 1990s. Building on the Cold War concept of "total defense," which means that every sector of society is mobilized in the event of an attack and has a part to play to ensure security, vulnerability commissions were established in all three countries to provide comprehensive risk assessments. The events of 9/11 added further momentum for continuing the transformation.[12]

Despite these differences between, and the changes occurring in, some EU countries, it is nevertheless clear that all Union members prefer a comprehensive approach to international affairs balancing "soft" and "hard power," with an emphasis on "soft power." EU members stress civilian means of conflict resolution and the merits of multilateralism and use different language than their American partners, which Europeans consider to be predisposed to favoring "hard power," military approaches.[13]

---

[12] See Anja Dalgaard-Nielson, "Homeland Security and the Role of the Armed Forces: A Scandinavian Perspective," in *Weniger Souveränität—Mehr Sicherheit*, ed. Borchert, pp. 59-75.

[13] See Wyn Ress and Richard J. Aldrich, "Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence," *International Affairs* 81, no. 5 (2005), pp. 905-923.

Moreover, post-modern views of the nature of conflicts—such as the ones Robert Kagan analyzed in his "Mars vs. Venus" writings—are quite common in the Old World.[14] Actually, one could argue that the sense of security which many members of Europe's political élites felt under America's nuclear umbrella during the Cold War still persists. Having grown accustomed to peace on their continent, the vast majority of Europeans take security for granted. (Ironically, America's security guarantee has contributed to this development). Most Europeans have yet to recognize that the defense of their societies, whose "magnetic power"[15] they are proud of, is in need of a profound overhaul.

In order to better understand the European risk perception, the limits to European unity have also to be taken into consideration. The EU is still mostly an economic community. The term "European Union" suggests a picture of a unified continent which hardly exists in reality. The rejection of the European constitution by France and the Netherlands is a case in point. Many policy fields, including national security, remain under the authority of the twenty-five national governments. This has made the efforts to establish a Common Foreign and Security Policy (CFSP) and a European Security and Defense Policy (ESDP) a difficult undertaking, particularly with regard to contentious key issues such as the Union's position vis-à-vis the U.S.-led invasion and occupation of Iraq. At the same time, Europe-wide solidarity has its limits (see below for a discussion of the EU's solidarity clause). For example, the Madrid and London bombings have been perceived as attacks on Spain and the UK, respectively, much less as attacks on the EU. As a consequence, the political impact has been felt a lot more strongly in those two countries than in the other member states (Italy may be an exception) or at the EU level. A heightened national risk perception does only to a limited degree translate into a heightened EU risk perception. Cynically speaking, it seems that only disasters, man-made or natural, which cut across several national borders may have the potential to create deeper solidarity within the EU.

---

[14] See, for example, Robert Kagan, "Power and Weakness," *Policy Review*, no. 113 (June/July 2002), pp. 3-28.

[15] Javier Solana, "Europe's Leading Role in the Spread of Democracy," *Financial Times*, 14 March 2005.

The new dimension of the security challenges

The U.S. National Strategy for Homeland Security defines the term homeland security as follows: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[16] With regard to the context of this article, three aspects have to be discussed: the "national effort," "terrorism" and "vulnerability."

While it is clear that many of the tasks for a secure homeland have to be carried out at the *national* level, *international* cooperation is indispensable. In an age of easy travel (at least in the transatlantic region) and daily global financial transactions of more than a trillion US-dollars, America cannot guarantee its security on its own. America needs the support of its European partners, just like the Europeans need the support of the U.S. in order to improve the security of their homeland.

As to terrorism, it is its new dimension which lends it such an urgency. Terrorism itself is not a new phenomenon. The world witnessed waves of terrorism before, such as the anarchist violence in the 1880s and 1890s, which claimed hundreds of lives.[17] The difference between yesterday's and today's terrorist challenge lies mainly in the technological progress. The proliferation of WMD and their means of delivery could in the future provide terrorists with the opportunity to inflict damage on an unparalleled scale.

However, the challenge of strategic, or catastrophic, terrorism is hardly on the agenda of Europe's political decisionmakers these days. That is quite surprising for three reasons. Firstly, almost all experts agree that Europe's strategic situation has deteriorated over the last decade. Although the enlargement of NATO and the EU have helped to stabilize Central and Eastern Europe (the Balkan wars notwithstanding), political tensions beyond the southern borders of the EU—i.e., in the "arc of crisis" reaching from North Africa to the Greater Middle East and Caucasus—have by and large increased. It is also surprising because, secondly, the stakes are so high. A so-called dirty

[16] *National Strategy for Homeland Security*, p. 2.

[17] See "Lessons from Anarchy" and "For Jihadist, Read Anarchist," *The Economist*, August 18, 2005.

bomb detonating in the financial district of London or Frankfurt could cause lasting harm to a large number of people—and to the European or the world economy.

Finally, that the threat of strategic terrorism does not attract more attention in Europe is also surprising because there is a connection between vulnerability, homeland security and the capability to act.[18] As the U.S. Strategy for Homeland Security states, "Our great power leaves [our] enemies with few conventional options to do us harm. One such option is to take advantage of our freedom and openness by secretly inserting terrorists in our country to attack our homeland. Homeland security seeks to deny this avenue of attack to our enemies and thus provide a secure foundation for America's ongoing global engagement."[19] This linkage between vulnerability, homeland security and the capability to act also applies to the EU. As a community of twenty-five member states with some 450 million inhabitants, the Union is "inevitably a global player,"[20] as the European Security Strategy states. But in order to share in the responsibility for worldwide security, a sound basis at home is required. The foundation of international engagement is a secure homeland. Policymakers in the U.S. have understood this connection. However, that is not yet the case with most of their European counterparts.

All in all, the threat of strategic terrorism is one reason why homeland security should become one of the main policy fields in Europe. Another reason is the challenge of vulnerability in general. The vulnerability of Western societies has increased significantly over the last ten to twenty years due to the rise of global data networks, the expansion of regional and global trade, and new production methods such as just-in-time delivery. Indeed, Europe's prosperity depends on its tightknit web of industries and its infrastructure. Breakdowns in parts of the key infrastructure or industries can be felt across the continent within days, sometimes hours or even minutes. Such breakdowns may be caused by natural and civilizational disasters as well as by terrorists.

---

[18] See Heiko Borchert and Thomas Pankratz, "Homeland Security aus europäischer Perspektive," in *Weniger Souveränität—Mehr Sicherheit*, ed. Borchert, pp. 17-38; here: p. 18f.

[19] *National Strategy for Homeland Security*, p. 5.

[20] *A Secure Europe in a Better World: European Security Strategy*, p. 1.

As a consequence, it would make sense to use an all-hazard approach to protecting the homeland instead of focusing on terrorism. To be fair, in a number of fields efforts have been made to upgrade and improve protection. However, it is the overall understanding of the magnitude of the challenge which is still mostly missing in Europe.

What are the challenges resulting from diverging risk perceptions?

Against this background of diverging risk perceptions, three challenges may arise. The first one sounds familiar: it is about capabilities. The U.S. invests considerable resources, both financial and human, in the development of procedures and technologies for the purposes of homeland security. Efforts in most European countries and at the EU level have been rather fragmented. Financial support for science and technology in the homeland security area have been increased (for example, through the EU's Security Research Program),[21] but at least so far, emergency responders have not been included in the Union's ongoing capabilities development program. Therefore, there may be an emerging transatlantic discussion on capability gaps in the homeland security sector.

The second challenge lies in what could lead to the "strategic division" of the transatlantic security partnership. If the U.S. and Europe continue to differ significantly in their respective risk perceptions and are also divided as to the national and international measures with which to counter those risks, transatlantic solidarity may be in danger. In effect, the "fundamental guiding principle" of the Atlantic Alliance, which is "common commitment and mutual co-operation among sovereign states in support of the indivisibility of security for all its members,"[22] may be jeopardized.

Yet, not only transatlantic solidarity is at stake. Solidarity among the twenty-five members of the EU could also fall apart. The solidarity clause of the EU stipulates that the members "shall work together

[21] For more information on the Union's security research program see European Commission, Directorate-General Enterprise and Industry, Security Research [http://europa.eu.int/comm/enterprise/security/index_en.htm].

[22] North Atlantic Treaty Organization, *The Alliance's Strategic Concept*, Washington, D.C., 23/24 April 1999, paragraph 8.

to enhance and develop their mutual political solidarity."[23] If EU members were to approach homeland security in different ways rather than by cooperation, this might over time lead to different zones of security in the Union.

For example, positions among EU members vary considerably with regard to the use of military forces for homeland security purposes. While countries like France and Italy have a history of cooperation between the police and the military, others such as Germany have been very cautious in that respect for historic reasons. Spain and Poland put certain constraints on the domestic use of the armed forces, whereas the legal codes of Denmark, Belgium and the Netherlands do not restrict homeland security missions of their national armed forces.[24] The EU constitution includes an expanded solidarity clause,[25] which makes for the first time reference to the concept of homeland security on the Union level, thereby creating a "domestic dimension" of the EU's Security and Defense Policy (ESDP). Since the constitution was rejected by the referendums in France and the Netherlands, it remains to be seen what role the expanded solidarity clause will play in the future.

The third challenge is closely related to the second one. If Europe as a whole does not tackle the issue of homeland security or if individual member states choose national rather than common approaches, Europe's capability to act in the international arena may be dimin-

---

[23] "Consolidated Version of the Treaty on European Union," *Official Journal of the European Communities*, 24 December 2002, C 325/5, article 11 paragraph 2. The solidarity clause has been part of the Treaty on European Union since the Maastricht Treaty came into force in 1993.

[24] See Roman Schmidt-Radefeldt, "Homeland Security durch Streitkräfte: Verfassungsrechtliche Rahmenbedingungen für innereuropäische Militäreinsätze," in *Weniger Souveränität—Mehr Sicherheit*, ed. Borchert, pp. 76-94; here: p. 83ff.

[25] Article I-43 reads, "The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) —prevent the terrorist threat in the territory of the Member States;

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

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

ished. Many security problems in the world require a common effort by the U.S. and Europe. None of the major security challenges will be resolved without close cooperation between Americans and Europeans. A Europe that is more vulnerable at home than its partners across the Atlantic might prove an interesting target for actors opposing Western involvement. The connection between vulnerability, homeland security and the capability to act has already been mentioned. If an EU member could in the future be put under pressure, or even blackmailed, due to a negligent approach to homeland security, multinational missions abroad could be significantly weakened.

What can be done about the diverging risk perceptions?

The attacks of September 11 , 2001, shook the foundations of the U.S., changing the national psyche in a way few events before have. The attacks revealed the many deficiencies, or even failure, of the government institutions in charge of protecting America. As a consequence, the government has undergone a far-reaching restructuring, putting homeland security on top of the national political agenda.

Europeans were shocked, too, but not in the same way. The shock was not as deep and it abated rather soon. The fact that no attack comparable to 9/11 has occurred in Europe has prevented major change in the government structures of most EU countries and at the Union level. Developments in the individual member states have been uneven. In Germany—and most other EU countries, too—the wider public has not developed a lasting interest in the topic of homeland security. A number of security measures have been enacted but on the whole the political élites have, with some notable exceptions, chosen to do little about the issue. It is only slowly dawning on decision-makers that there is a need for change. In some other EU member states, particularly those which have already been targeted, concerns about security are higher, and risk perceptions have altered. Indeed, in the UK and the Scandinavian countries, the transformation of the security sector in fully underway. In most other EU countries and at the Union level itself, however, there has not occurred a profound change in the "security mindset," and government and security structures have yet to be adapted to the new dimension of the challenges.

Therefore, the key task now is to put the subject on the political agenda, which requires sustained commitment and leadership on the

part of the élites. A political dialogue needs to be developed in the Union's member states, particularly in those countries where the issue of homeland security has so far received insufficient attention. Additionally, a dialogue should take place both at the EU and the transatlantic level. The dialogue need not necessarily be based on risk perceptions. Instead, another approach may focus on vulnerabilities, which may be easier to agree on. Such approach should not be restricted to terrorism-related threats. Rather, it should be an all-hazards approach that also deals with the vulnerabilities resulting from civilizational challenges (such as the interdependence of electricity supplies shown by the power breakdowns in the U.S. and the U.K. during the summer of 2003) and natural disasters (like Hurricane Katrina and other kinds of strong storms, whose intensity and frequency may be expected to increase).

However, it should be remembered that most parts of the critical infrastructure are owned or operated by private sector companies. Cooperation between government and the private sector plays a crucial role. Hence, a dialogue with and within the private sector is necessary. Companies with transatlantic business ties are particularly relevant due to the expansion of transatlantic markets.[26] The private sector dialogue might well contribute to the necessary debate in the political realm by raising the awareness of homeland security issues. Ideally, the risk perceptions of the political arena could be harmonized with those of the private sector.

Another aspect are the implications of EU enlargement. As this chapter has shown, perceptions and attitudes with regard to homeland security vary among EU member states. The enlargement of the Union seems to further national introversion. The more EU members there will be in five, ten or fifteen years' time, the more difficult it might be to establish something like a common European strategic culture. If Europe grows ever more diverse, it is hard to imagine that risk perceptions will converge. Enlargement has proven certainly beneficial to exporting stability, yet it comes at a cost for what could be called the "community feeling." This point should be kept in mind when discussing further rounds of EU enlargement.

[26] See Daniel S. Hamilton and Joseph P. Quinlan, eds., *Deep Integration: How Transatlantic Markets are Leading Globalization*

Transatlantic Cooperation on Homeland Security: What Do We Need to Do? What Do We Need to Do Together?

Chapter 4

The Concept of Homeland Security in the European Union and in Austria—A Challenge for the Austrian EU presidency

Gustav E. Gustenau

In the aftermath of the attacks of September 11, 2001, the United States saw itself in a new position having had a direct terrorist attack on their homeland. In response to the realization of the vulnerability of the USA, the country made tremendous efforts to protect its homeland and citizens. The principal answer was a far-reaching reform of the security structure. The Department of Homeland Security was created to coordinate the manifold instruments involved in the matter of securing the homeland. The Administration elaborated the *National Strategy for Homeland Security*.

Unlike the USA, no uniform understanding of what is meant by homeland security has yet developed in Europe. In the USA, a more centralized system has evolved, with a single department and various jurisdictions on both federal and state levels. Therefore, homeland security in the USA has a more vertical structure. On the other hand, both on the European and national levels, a model is developing according to which the agency responsibilities are kept as they are, but these are more closely coordinated.[1]

However there is a great demand to develop an adequate homeland security profile in Europe:

[1] See Borchert Heiko: "Schutz der Heimat und die Rolle der Streitkräfte: Einleitung" in Heiko Borchert (ed.), *Mehr Sicherheit—Weniger Souveranität. Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte* (Hamberg: Verlag E. S. Mittler & Sohn, 2004), p. 8.

- As a result of the European Union enlargement, the borders of the EU extend to instable regions.

- The EU space of "freedom, security and justice" (Tampere 1999) has open borders, freedom of movement and transport. This situation has increased degree of vulnerability.

- The EU has a very high population density, a road network of nearly 4.3 million km, a railroad network of nearly 155,000 km an extended network of oil- and gas-pipelines.[2] Nearly 5 million commercial trucks circulate on the European road network each day and there are over 41,000 landings and take-offs at European airports per day. In the EU there are over 1,100 container and passenger ports. For example, in Rotterdam nearly 10,000 containers leave the port every day. This increased level of economic integration not only has advantages, but also increases risks. A breakdown in parts of these infrastructures systems would affect the EU very rapidly. These few figures demonstrate the tremendous challenges the EU faces to develop a homeland security profile that covers great sections of these risks.

- In Europe split competences exist, as the EU does not have the same competences in all three pillars.[3] And many of the responsibilities for homeland security are under authority of the Member States.

---

[2] See Borchert Heiko, Thomas Pankratz: "Homeland Security aus europäischer Perspektive" in Borchert Heiko (Ed.) *Weniger Souveranität, Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte*, p. 19.

[3] The EU is usually illustrated by three pillars. The first pillar consists of the European Communities. European communities is the collective name of the European Coal and Steel Community (ECSC), the European Economic Community (EEC), and the European Atomic Energy Community (EURATOM). The Maastricht treaty has formed the European Communities as a whole into the first of three pillars of the European Union. The first pillar is also called the Community Pillar or Communities Pillar. It covers matters concerning the Single Market and the free movement of persons, goods, services, and capital across borders. The first pillar encompasses cooperation in fiscal and monetary issues (i.e. the Economic and Monetary Union) and matters related to agriculture, the environment, trade policy. The second pillar consists of the Common Foreign and Security Policy (CFSP) and the European Security and Defense Policy. The third pillar contains police cooperation and cooperation concerning police cooperation and cooperation in the area of criminal law.

- Terror has two aspects: 1) External terrorism; 2) Internal terrorism; Due to large scale immigration and a failed integration policy the threat of internal terrorism increased tremendously within the EU. Even though Europe has experienced internal terrorism (IRA, ETA, Red Brigades etc.) in its history, the new threat of internal terrorism perpetrated by Al-Qaeda and extremists that are inspired by Al-Qaeda has become the main terrorist threat of the European Union. Thus, it is not enough for the EU to organize excellent border control measures. The EU has to go beyond; it will be necessary to develop programs that not only prevent terrorism, but also prevent radicalization and recruitment of members in terrorist organizations.[4]

There is no generally accepted definition of the term homeland security in Europe. It is therefore necessary at this point to describe briefly the approach to homeland security taken by the author of this article. Homeland security is an interagency approach, based on a comprehensive concept of security, which attempts to integrate public and private participants.[5]

Homeland security is comprehensive in its scope. In addition to dealing with naturally occurring dangers (disasters), its central concern is the threat of terrorism (nuclear-terrorism, bio-terrorism, chemical terrorism, cyber terrorism, and conventional terrorism).

This paper, on the one hand, focuses on describing the specific European problem of developing an adequate homeland security profile and, on the other hand, aims to demonstrate the European Union's numerous programs and initiatives that tackle the homeland security issue. Furthermore, the road Austria is taking and the goals pursued by Austria in the light of the EU Presidency will be discussed. The author's final goal is to look into the future and draw action-oriented conclusions of where the challenges for the EU lie when developing and implementing a concept of homeland security that generates added value for Europe.

---

[4] For more on this, see "The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism," online at http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/87258.pdf downloaded June 12, 2005.

[5] For the intention of homeland security see the chapter by Heiko Borchert in this volume, pp. 4-5.

The EU and Homeland Security—Current approaches to address the question: How to tackle the problem in Europe?

The threat of terrorism in Europe has traditionally been considered latent—except in countries that have historic experience in terrorism—however, since the attacks on Madrid and London, this view is beginning to change. Nevertheless, the subject of homeland security receives inadequate attention within the EU. This is also true for the majority of Member States. Europe is facing the challenge of both integrating homeland security as a unified activity across portfolios within Member States, and transforming this process on the level of the European Union.

In this context, the EU is facing a particular challenge, as the constituent parts of homeland security are extremely diverse and shared between a very large number of participants, and neither the *European Security Strategy* nor *The Hague Programme* are able to solve this problem. Above all, the confusion of areas of authority in the European institutions must be removed, and the fight against terrorism and homeland security established as matters, which cut across institutions. This area encompasses all three pillars of the EU and manifold participants and instruments. Coordination of the three pillars and their participants, however, remains an unsolved problem. Many activities of the issue are firmly positioned within the first and third EU pillars, and there are varying areas of authority in the various organs and institutions of the different departments.[6]

The following categorizations can be given as examples (although these statements do not always apply one hundred percent):

Mainly assigned to the first pillar:

- Transport policy (including transport, visa, asylum and immigration policies)
- Measures relating to the prevention of the financing of terrorism are also to be found here.

[6] See Borchert Heiko, Thomas Pankratz: "Homeland Security aus europäischer Perspektive" in Borchert Heiko (Ed.) *Weniger Souveranität, Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte*, pp. 32-35.

Mainly assigned to the third pillar:

- Areas which can be subsumed under the heading "border control" of the EU's external borders.
- Measures and bodies which deal with the area of "recruitment to terrorist organizations" are also to be found here.

The first pillar of the European Union comes predominantly under the authority of the European Commission, while the bulk of second and third pillars are the jurisdiction of the individual Member States (although there are combined jurisdictions here too, e.g. EUROPOL). The second pillar (Common Foreign and Security Policy—CFSP and European Security and Defense Policy ESDP) is, of course, not to be forgotten, as some aspects of CFSP and ESDP feed specifically into the issue of homeland security and the fight against terrorism.

Among the Member States there are of course twenty-five different interests and twenty-five different threat-perceptions. It must also be noted that the individual Member States also operate different security structures. In summary, it can be observed that the EU very often fails to go beyond the process of policy formulation, again leaving the implementation to the individual countries whose actions in turn are determined by their own interests. These brief comments lead us to suspect where the problem lies. However, on the EU level, there are a variety of initiatives and programs to tackle the complex array of topics relating to homeland security with the aim of protecting the population as well as possible while keeping the EU an area of security, freedom and justice.[7]

An overview of achievements by the EU—the development of specific programs and initiatives.

Revised Action Plan on Terrorism (AP II)

The Action Plan on Terrorism has taken a number of measures to enhance the internal security of the Union. Some of these were specifically aimed at combating terrorism and others had more general character, such as various measures taken as part of the establishment of an area of freedom, security and justice. The following measures

[7] (See *the Hague Programme*).

are to be mentioned here: the common European arrest warrant, joint investigation teams, the creation of Eurojust, the reinforcement of Europol, the creation of an integrated border management agency, improvement in the security of travel documents and other measures.

In the aftermath of the March 11 terrorist attacks in Madrid, the Revised Action Plan on Terrorism (AP II) was adopted by the Council of the European Union. This Revised Action plan on Terrorism is to be updated semi-annually and will be revised continually concerning related measures. The Revised Action Plan on Terrorism mentions seven strategic objectives. These are:

1. To deepen the international consensus and enhance international efforts to combat terrorism.
2. To reduce the access of terrorists to financial and other economic resources.
3. To maximize capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and prevent terrorist attacks.
4. To protect the security of international transport and ensure effective systems of border control.
5. To enhance the capability of the EU and its Member States to deal with the consequences of a terrorist attack.
6. To address the factors which contribute to support for and recruitment into terrorism.
7. To target actions in the field of EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.[8]

This Revised Action Plan on Terrorism includes manifold initiatives (nearly 150!), which identify key tasks under each objective, specific achievable targets and the EU bodies responsible for delivery.[9]

---

[8] See "Revised Action Plan on Terrorism" (EU-Document 10694/05) and Commission Staff Working Document SEC (2005) 841; online at http://register.consilium.eu.int/pdf/en/05/st10/st10694.en05.pdf downloaded December 1, 2005.

[9] For more on this, see "Revised Action Plan on Terrorism" (EU-Document 10694/05) and Commission Staff Working Document SEC (2005) 841; online at http://register.consilium.eu.int/pdf/en/05/st10/st10694.en05.pdf downloaded December 1, 2005.

Framework The Contribution of ESDP in the fight against Terrorism[10]

The European Council demanded rapid action on the contribution of the ESDP to the fight against terrorism. In the June 2004 report to the European Council on the implementation of the Declaration on Combating Terrorism,[11] the Political and Security Committee(PSC) was requested to elaborate the conceptual framework identifying the main elements of the ESDP dimension of the fight against terrorism, including preventive aspects. The Framework "The Contribution of ESDP in the Fight against Terrorism" was adopted by the Council. The document has a very important role for the contribution of the military in terms of combating terrorism and this document addresses the ESDP dimension of the fight against terrorism.

This document is based on the following principles: solidarity among EU Member states; voluntary nature of Member States' contribution, clear understanding of the terrorist threat and full use of available threat analysis; cross pillar coordination in support of the EU's common aim in the fight against terrorism; cooperation with different relevant partners; and an understanding of the complementary nature of the ESDP contribution, in full respect of Member States' responsibilities in the fight against terrorism.

The European Security and Defense Policy, which encompasses civilian and military crisis management operations under the Title V of the TEU (Treaty of the European Union), can contribute to the fight against terrorism, either directly or in support of other instruments. The Framework "The Contribution of ESDP in the Fight against Terrorism" mentions four main areas of action:

Prevention: In order to respond to the threat of terrorism the Member States should mobilize all resources, including military ones. Additionally, the prevention of such an asymmetric threat must be supported by the necessary level of information gathering and effective intelligence.

---

[10] For more on this see doc. 14979/04 "Conceptual Framework on the ESDP dimension ot the fight against terrorism"; online at http://register.consilium.eu.int/pdf/en/04/st14/st14797.en04.pdf downloaded December 2, 2005.

[11] For more on this, see doc. 10585/04, "Declaration on Combating Terrorism;" online at http://register.consilium.eu.int/pdf/en/04/st10/st10585.en04.pdf downloaded December 1, 2005.

1. Protection: This document states that protection (including force protection) is a very important aspect of CMOs (Crisis Management Operations). This should reduce the vulnerability of EU assets (personnel, materiel, and so on) in the case of a terrorist threat.

2. Response/Consequence Management: In the field of addressing the effects of an attack, military means can have either a direct or a supporting role.

3. Supporting Third countries: A wider spectrum of ESDP missions might include support to third countries in combating terrorism (as indicated by the European Security Strategy). This field also encompasses the force protection of deployed ESDP missions and protection of EU citizens.

4. The Framework "The Contribution of ESDP in the fight against Terrorism" also includes so-called Action Points which are to be implemented.[12]

The Hague Programme

After the Tampere European Council in 1999, the EU developed a policy in the area of justice and home affairs in the framework of a general program. Not all of the aims have been achieved, but some comprehensive and coordinated progress has been made. Some results that have been achieved in the first five years are: the foundations for a common asylum and immigration policy; the harmonization of border controls has been prepared; improvement of police cooperation; and the groundwork for judicial cooperation on the basis of the principle of mutual recognition of judicial decisions and judgments has been developed.[13] Five years after the European Council's meeting in Tampere, the Council initiated a new agenda to enable the Union to build on the achievements and to meet the new challenges it will face

[12] For more on this, see doc. 14797/04, Framework "The Contribution of ESDP in the fight against Terrorism" online at http://register.consilium.eu.int/pdf/en/04/st14/st14797.en04.pdf downloaded December 2, 2005.

[13] See Council of the European Union, "The Hague Programme: strengthening freedom, security and justice in the European Union," Document 16054/04 (Brussels: December 13, 2004), p. 2; available online at http://register. consilium.eu.int/pdf/en/04/st16/st16054.en04.pdf downloaded December 2, 2005.

effectively. Thus, the Council approved a new multi-annual program to be known as The Hague Programme.

The Hague Programme should strengthen the EU as a common area of freedom, security and justice. The objective of this program is to improve the common capability of the Union and its Member States to guarantee fundamental rights, to ensure minimum procedural safeguards and access to justice, to provide protection in accordance with the Geneva Convention on Refugees and other international treaties, to regulate migration flows towards the EU and within the EU and to improve the management of the control of the external borders of the Union. It should also improve the Union's capabilities to fight cross-border crime and repress the threat of terrorism.

The Hague Programme involves improving and realizing the potential of Europol and Eurojust and the further development of mutual recognition of judicial decisions in civil and in criminal matters with cross-border implications.[14] The Hague Programme emphasizes the dimension of domestic security in the EU and it represents the complement of the European Security Strategy (ESS) concerning domestic security and it ensures freedom, security and justice with the following measures:

Table 1. The Hague Programme

Freedom	Security	Justice
Citizenship of the Union	Improving the exchange of information	EU Court of Justice
Asylum, migration and border policy	Terrorism	Confidence-building and mutual trust
Common European Asylum System	Police cooperation	Judicial cooperation in criminal matters
Legal migration and the fight against illegal employment	Management of crisis within the EU with cross-border effects (ICMA)	Judicial cooperation in civil matters
Integration of third-country nationals	Operational cooperation	
The external dimension of asylum and migration	Crime prevention	
Management of migration flows	Organized crime and corruption	
	European strategy on drugs	

[14] *Ibid*, pp. 2-3.

The Hague Programme contains the Part 2.4 "Management of crisis within the European Union with cross-border effects" (ICMA). This is of high importance within the EU, as there have been very few instruments and mechanisms for cross-border disasters or crisis.[15] Therefore, the European Council requests the Council and the Commission to develop integrated and coordinated EU crisis-management arrangements for crises with cross-border effects within the EU and within the existing structures. These arrangements should be implemented at the latest by July 1, 2006 and should at least address the following issues: further assessment of Member States' capabilities, stockpiling, training, joint exercises and operational plans for civilian crisis management. These arrangements are based upon the "principle of subsidiarity" and the full respect of national competences.[16] Luxemburg, The Netherlands, Great Britain and Austria have agreed to implement ICMA in their EU presidencies.

The Hague Programme faces the problem that there is nearly no reference to the second pillar of the EU. As mentioned before, homeland security encompasses all three pillars with all participants, actors and instruments and a program that excludes one pillar as a whole is not as comprehensive as needed to tackle the challenge of homeland security.

Declaration of the "Solidarity Clause"

In the aftermath of the terrorist attack on Madrid the EU decided on a declaration to act "in the spirit of the clause of solidarity" as it is stated in the Art. I-43 of the draft of the Constitutional Treaty of the EU. This was not a partial implementation of one part of the Constitutional Treaty, it is a parallel process to the further development of the constitution.

---

[15] The "Community Mechanism for Civil Protection" was set up by the Council Decision of October 2001. It pools civil protection capabilities of 30 participating states (the twenty five Member States, Bulgaria, Romania, Iceland, Liechtenstein and Norway). For more information see: "Community cooperation in the field of Civil Protection" online at http://europa.eu.int/comm/environment/civil/prote/mechanism.htm downloaded December 12, 2005.

[16] "The Hague Programme: stregthening freedom, security and justice in the European Union," *op cit*, p. 24, para 2.4.

This declaration is only politically binding; thus, it is not mandatory in a judicial way. The main actors in this field are the Member States. They are able to make use of all adequate assets at their sole discretion. Military assets were mentioned explicitly, but what assets will be used by the Member States? There is no automatic requirement to make use of military assets.

FRONTEX—European Agency for the Management of Operational Cooperation at the External Border of the Member States

The European Agency for the Management of Operational Cooperation at the External Border of the Member States (FRONTEX) is located in Warsaw, Poland, and has been operational since May 1, 2005. FRONTEX has the function of coordinating the management of the external border of the Member States and of providing support to the new Member States to train border guards and to give operational and technical support at the external borders of the EU.

FRONTEX in particular has the following tasks:

- To coordinate operational cooperation between Member States in the field of management of external borders,
- To assist Member States in the training of national border guards, including the establishment of common training standards,
- To carry out risk analyses,
- To follow up the development of research relevant for the control of persons and surveillance of external borders,
- To assist Member States in circumstances, requiring increased technical and operational assistance at external borders,
- To provide Member States with the necessary support in organizing joint return operations.[17]

[17] For more information see: http://europa.eu.int/scadplus/leg/en/lvb/l33216.htm downloaded December 2, 2005.

This agency only supports the national border control institutions, but should not displace them. It is important to mention that FRONTEX has no authority within the Member States.

Further programs in this field are: The *revised CBRN-Programme*, the EU *Programme for the "Prevention, Preparedness and Consequence Management of Terrorism*, the *European Security Research Programme*, the development of the *Schengen Information System II (SIS II)* and the "*Comprehensive package in the fight against terrorism.*"[18] Another program is the EUMC database (regarding military capabilities and capacities).[19]

A very complex and important area is Critical Infrastructure Protection (CIP). The EU is very interested to push forward programs and initiatives for Critical Infrastructure Protection. The following points should be mentioned: the *CIP-Inventory programme*, the *European Programme for Critical Infrastructure Protection (EPCIP)* and the *EU Critical Infrastructure Warning Information Network (EUCI-WIN)* which is a part of EPCIP.[20]

On December 1, 2005, a new Counter-Terrorism Strategy for the EU was endorsed. The guideline of this concept is: To fight terrorism in a comprehensive way, make Europe safer and provide the people in Europe with freedom, security and justice.[21] Four specific objectives and foci are to be derived:

---

[18] For more information see chapter by Gustav Lindström in this volume.

[19] At a meeting in February 2003 the PSC assigned the EUMC (European Union Military Council) to set up a database regarding military capabilities and capacities, which are relevant for the prevention of terrorist attacks. The database should provide quicker respond of terrorist attacks and a better coordination. The Member States should notify their contributions and this database should be updated continuously. The content of this database should also be accessible for Civil Protection Mechanisms. This program gives reference to 7 scenarios, which should encompass the whole spectrum. These scenarios are: conventional explosion, which could affect the critical Infrastructure of a Member State, C-Scenario, B-Scenario, N/R-Scenario, terrorist attack of an oil-vessel, Agro-Terrorism, contamination of foods. Military contribution is mentioned in search and rescue tasks, transport and recovery, medical support, logistic support, CBRN-support, demining and technical support.

[20] For more information see: com (2004) 702 final, Communication from the Commission to the Council and the European Parliament—Critical Infrastructure Protection in the fight against terrorism.

[21] See "The European Union Counter-Terrorism Strategy"; online at http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/87257.pdf downloaded December 2, 2005, p. 6.

1) Prevent: To prevent people turning to terrorism by tackling the root causes which can lead to radicalization and recruitment to terrorist organizations

2) Protect: To protect the citizens and infrastructure within the EU, and reduce the vulnerability. This includes improved security of borders, transport and critical infrastructure.

3) Pursue: This field deals with the cross border prosecution of terrorists within the EU and globally. Also to prevent planning, travel and communication in order to disrupt terrorist activity.

4) Respond: This objective deals with activities to manage and minimize the consequences of a terrorist attack by improving capabilities to deal with.[22]

These processes are located mostly in the first and third pillar of the EU (except the Framework "The Contribution of ESDP in the fight against Terrorism" and the EUMC database). There are some central and coordinating instruments on EU level, but the problem is that these instruments do not have a lot of resources and authority. The main actors in the realization of all these programs and initiatives are the Member States (because of the principle of subsidiarity) and there will be no intervention in the competences of the Member States.

Homeland Security in Austria

Austria's focus on Homeland Security during its EU presidency 2006

In addition to its own essential national security interests, Austria's security strategy is oriented towards the European Union. For smaller states such as Austria, the European Union offers the ability to reinforce security by working together with others and to participate in the formulation of the European security architecture.

Every EU presidency is confronted with major challenges. Examples that come to mind are: financing the EU, horizontal and integrated expansion and advancing the Constitutional Treaty. It must be clear

[22] "The European Union Counter-Terrorism Strategy"; online at http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/87257.pdf downloaded December 12, 2005, p. 3.

that the freedom of action of any presidency is limited. Limitations arise from the need to complete measures already initiated, agreed and, to a large extent, already determined. These could be termed the "mandatory program." The completion of the "mandatory program" is a criterion of a presidency's success or failure. In addition, a presidency can also determine priorities. This could be termed as the "free program." Priorities will be determined with reference to long-term strategic programs, issues that arose under the Luxemburg and British presidencies and the mandate of the Austrian presidency, also coordinated with Finland, which will take on the presidency after Austria. The main objective is to accelerate and push the implementation process rather than introduce new anti-terrorist measures.

The loss of strategic direction has impact on far reaching concepts and visions. After the rejection of the Constitutional Treaty and the controversy about financing the EU, the EU finds itself in a vital crisis. A reflection period of one year was initiated and this "general crisis" of the EU has had an impact on the development of far reaching reform processes and concepts. For this reason Austria decided to focus on pragmatic and practicable measures during its presidency.

One of the foci of the Austrian presidency will be an increased implementation of ongoing processes like the Revised Action Plan on Combating Terrorism and the Management of Crisis within the EU with cross border effects (ICMA). One further focus in this area will be the Prevention of Proliferation with the Proliferation Security Initiative (PSI) and the Container Security Initiative (CSI).

The PSI is a global political initiative with the objective to prevent effectively the proliferation of weapons of mass destruction (WMD), their delivery systems, and related materials and technology worldwide with the use of force in the case of the failure of political and diplomatic measures. As the proliferation of WMD presents an increasing global threat, it is a field of concern of the EU and the CFSP. A strategy against proliferation was adopted in the European Council on December 12, 2003. In a statement in 2004 the EU agreed to support the PSI officially. Austria also supports the PSI; Austria is expected to play an active role in this initiative.

In order to prevent terrorism at a preliminary stage, Austria will emphasize a long term Action Plan against radicalization and recruit-

ing of terrorists. In this field the focus will be on an interreligious and intercultural dialogue.

In the field of foreign policy regarding the Common area of freedom security and justice, Austria will focus on European neighborhood policy and on the West Balkans. This European neighborhood policy encompasses the countries of Eastern Europe[23] and the Mediterranean.[24] This European neighborhood policy considers that there are three types of countries:

1) Countries that will be EU Members

2) Countries that likely will be EU Members

3) Countries that never will be EU Members

Austria developed a partnership program for these countries, which is the basis for tight cooperation in terms of migration, trafficking, terrorism, organized crime and so on.

In the Ministry of Defense the emphasis lies on:

- The contribution to the generation of a cross-governmental "Annual Situation Report"
- Consequence management after terrorist attacks
- Force protection of forces in EU-lead operations

Also the implementation of the Action points of the Framework "The Contribution of ESDP in the fight against Terrorism" is one of the prior objectives within the Ministry of Defense during the Austrian EU presidency.

Austria and Homeland Security—a special problem?

In Austria, homeland security implementation has fundamental flaws relating to whether the political elites would address this issue. I have called this problem an "…entirely political decision with far

[23] The Ukraine, Belarus, Moldova, Georgia, Armenia, Azerbaijan,

[24] Syria, Lebanon, Israel, Palestinian Autonomy, Jordan, Egypt, Lybia, Tunisia, Algeria, Morocco,

reaching consequences, which political leaders do not want a priori (Translation of the author)."[25] In Austria, these problems are also subject to the political elite's perception of the threat. As a result, the risk of a catastrophic terrorist scenario is not actually taken seriously even though the possibility of isolated acts of terrorism in Austria is not at all ruled out.

These conditions are not at all conducive to comprehensive reform and restructuring of the security sector to counter a new threat in a changed political environment. In addition, the lack of a strategic, nationwide structure in Austria is a problem for the central leadership of military forces. Austria also has no paramilitary troops that fill the gap between the police and the army and which could be used for homeland security and the lack of resources means that one cannot assume that troops of this type can currently (or at any time in the near future) be introduced.[26]

Nonetheless, even in Austria some developments have been made addressing the issue of homeland security. In Austria the issue of homeland security follows an all hazards-approach.

This is expressed in the elaboration of a Grand Strategy for Comprehensive Security from which are derived sub-strategies. These sub-strategies are: Teilstrategie Verteidigungspolitik (Defense Policy), Teilstrategie Innere Sicherheit (Internal Security), Teilstrategie IKT-Sicherheit (Information and Communication Technology Policy), Teilstrategie Verkehrs- und Infrastrukturpolitik (Transport and Infrastructure Policy), Teilstrategie Wirtschaftspolitik (Economy Policy), Teilstrategie Landwirtschaftspolicy (Agricultural Policy), Teilstrategie Finanzpolitik (Financial Policy), Teilstrategie Außenpolitik (Foreign Policy), Teilstrategie Bildungs- und Informationspolitik (Education and Information Policy). Also the Austrian Security and Defense Doctrine (SDD) from 2001 emphasizes the

[25] Gustenau, Gustav: Sicherheitspolitische Aspekte der Homeland Security aus österreichischer Sicht oder Verteidigungspolitik versus Homeland Security: Zum Stand der Debatte in Österreich, in: Borchert, Heiko (Ed.): Weniger Souveränität -Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte, p. 134.

[26] See Gustenau, Gustav: Sicherheitspolitische Aspekte der Homeland Security aus österreichischer Sicht oder Verteidigungspolitik versus Homeland Security: Zum Stand der Debatte in Österreich, in: Borchert, Heiko (Ed.): Weniger Souveränität -Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte, p. 140.

principle of comprehensive security where all the instruments of the aforementioned policies should be equal side by side.[27]

Future tasks to be accomplished in the EU and Austria to provide adequate protection of their citizens.

In the EU, homeland security represents a complex challenge with the individual Member States as the main players. All the same, the EU has a collective responsibility in all three pillars. As the EU Constitutional Treaty ran aground, expectations are that the willingness to make major institutional changes is low and that any action taken at EU level will have to be made with the structures as they are.

The scope of homeland security requirements varies. This is why a differentiated "needs-driven" and "added-value" homeland security profile must be developed for Europe.

While a consistent and interagency homeland security concept that reaches across all agencies (and is nearly all-inclusive) would be feasible on national level, this is no realistic option on EU level.

Therefore, the areas of homeland security responsibility and the tasks need to be split up. Based on the tasks defined by the Homeland S security strategy in the USA, various homeland security areas and tasks can be identified:

- intelligence services and early warning
- security of borders and transport
- anti-terror measures, including defense against catastrophic terrorist attacks

[27] See Gustenau, Gustav: Sicherheitspolitische Aspekte der Homeland Security aus österreichischer Sicht oder Verteidigungspolitik versus Homeland Security: Zum Stand der Debatte in Österreich, in: Borchert, Heiko (Hrsg.): Weniger Souveränität—Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte, p. 142—143—To date the process of implementation of the Grand Strategy and the Sub-Strategies are nearly completed. The author was member of elaboration team in the Bundeskanzleramt (Federal chancellery) of all sub-strategies and was in charge to elaborate the sub-strategie "Verteidigungspolitik—defense-policy."

- protection of critical infrastructure, perhaps also as a separate division "Protection of ICT Infrastructure"
- reaction and aid in the case of disaster (natural)[28]

The question is, whether the EU should be equally responsible for all the different areas of homeland security.

Basically, the EU's role is to take preventive action and coordinate activities between Member States while providing support in the development of concepts. Furthermore, the EU should perform a so-called clearinghouse-function. There will always be activities of the EU, even within the homeland security issues that will need to be carried out at the level of the individual Member State or by a "coalition of the willing." This would include the deployment of military means as a preventive measure in the war against terrorism (perhaps outside of Europe).

The EU could encourage and/or coordinate bi- and multi-lateral initiatives of groups of countries within the EU. The French/Spanish cooperation, the G5 group (Great Britain, France, Germany, Italy, Spain), or the "Salzburg Group" (Austria, the Czech Republic, Poland, Slovakia and Slovenia) are some examples. Another example could be the Common European Arrest Warrant.[29]

Other areas that would provide the European Union with a certain "added value" are intelligence and early warning. The EU could also take on a major role in further developing and intensifying existing cooperation projects and networking efforts in the intelligence systems (e.g. the Council's Situation Centre, SITCEN)

In the area of the protection of critical infrastructure the EU should focus on European critical infrastructure while Member States ought to be responsible for the protection of critical infrastructure on their national territory. Examples of European critical infrastructure are the European satellite navigation system "Galileo" or the European satellite centre in Spain. A very important role for the EU could be the identification and analysis of cross border networks and interdepen-

[28] See "National Strategy For Homeland Security," online at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf downloaded December 12, 2005, pp. 15—37.

[29] Daniel Keohane, "The EU and international terrorism," in: *Securing the European homeland: The EU, terrorism and homeland security* (Gütersloh: Bertelsmann Stiftung, 2005), p. 11.

dencies. Moreover, the European Union ought to identify any critical infrastructure that is essential for the safety and functionality of Europe outside of the EU and subject this infrastructure to a critical analysis. Furthermore, the EU should introduce and coordinate appropriate measures that also include the support of those countries where the critical infrastructure is located. The EU also ought to identify critical infrastructure in Member States that is important for the whole EU and initiate and coordinate joint protection measures for the protection of such critical infrastructure (e.g. the port of Rotterdam).

In the field of critical infrastructure protection the EU should analyze existing standards for safety and security of critical infrastructure or rather analyze existing standards in order to harmonize and complement these standards ("clearinghouse function"). To establish a monitoring system for compliance of the existing standards is considered very important.

The EU could become more involved in risk analysis and benefit from this commitment. Jointly with Member States, it could develop appropriate tools in order to conduct this risk analysis, taking into account that risk analysis may vary depending on the type of danger.

A very decisive point for the EU would be the creation of common legal regulations in order to ensure the competitiveness of civilian operators of critical infrastructure in the framework of the *public-private-partnership (PPP)*. On the one hand the economic interests of civilian operators of critical infrastructure have to be aligned with the safety and security considerations of the Member States. On the other hand the EU has to ensure that the safety and security standards within the Member States do not differ in a way that distorts market competition.

This did not happen in the USA where the Bush Administration apparently avoids intervening in the competencies and freedoms of the private economy, trusting that the private companies will take appropriate measures for their own protection. This did not occur; however, as the companies feared competitive disadvantages. It is obvious that the market's regulatory forces have failed; and, therefore, many large parts of critical infrastructure in the USA remain unprotected.

Another option could be the creation of crisis intervention teams (including creation of databases with specialists.) This option is cur-

rently under consideration for the second pillar in order to make instruments for civil protection available quickly and reliably. In this area, the EU could also be in charge of mutually harmonizing and coordinating these databases with others. This does not suffice, however, to get the requisite number of troops deployed and available. The EU would also have to make sure that the forces made available are compatible and interoperable.

The EU could also develop mechanisms and instruments with considerable added value in the area of consequence management and use these if necessary. In any case, the EU would primarily provide support for the individual Member States. This support could be provided by making experts and means available. The creation of adequate databases would make this support and civilian-military expertise available promptly.

In this context, the EU should also encourage and coordinate the development of common legal regulations in order to facilitate the deployment of military forces in the framework of homeland security (as provided by the solidarity clause). Legislation as such, however, falls within the competence of the individual Member State, but the EU could perform a clearinghouse function.

Austria could serve as an example here. The deployment of Austrian armed forces is governed by the constitutional law on "Cooperation and Solidarity in the Deployment Abroad of Units and Individuals." (KSE-BVG). The dispatch of military forces is only admissible for humanitarian purposes and disaster relief in Europe and the dispatch of troops in accordance with the Foreign Troop Act (Truppenaufenthaltsgesetz) offers no legal basis for the presence of foreign troops or security forces for counter terrorism.

In other European countries, this legal basis is often much broader in scope and the European Union could create some added value here. Today, the deployment of military means based on the aforementioned solidarity clause equates to the deployment of armed forces.[30] The

[30] Schmidt-Radefeldt, Roman: Homeland Security durch Streitkräfte: Verfassungsrechtliche Rahmenbedingungen für innereuropäische Militäreinsätze, in: Borchert, Heiko (Ed.): Weniger Souveränität -Mehr Sicherheit—Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte, pp. 90—91

deployment laws and laws regarding the presence of military forces of the individual Member States would have to be harmonized here.

Consideration should also be given to the formation of civilian-military homeland security units. Such homeland security units, however, would have to be created at a national level. Here too, the EU would have to take on a "clearinghouse function," select the appropriate units for the various situations and deploy them, meaning, the EU would also have to ensure in this respect that the process is "needs-driven" and not "resource-driven." A similar process would be conceivable here as the one required for the creation of the Helsinki Headline Goal (HHG).

At the Helsinki European Council meeting in December 1999 the EU members set themselves a military capacity and capability target known as the Headline Goal. Corresponding with this goal the EU Member States should be able to deploy 60,000 troops within 60 days and these forces will be created in a modular fashion on the basis of national contributions. These forces should be military self-sustaining with the necessary command, control and intelligence capabilities, logistics, combat support services and additionally, as appropriate, air and naval elements. The forces will be able to cover the full range of Petersberg tasks as set out in the Amsterdam Treaty. These Petersberg tasks include humanitarian and rescue tasks, peacekeeping tasks and tasks of combat forces in crisis management, including peacemaking (in some contexts named "peace enforcement")

Civilian assets were added to the Headline goals at the June 2000 European Council meeting in Santa Maria da Feira. There the EU Member States decided to provide 5,000 police officers for international missions; and the Member States agreed to deploy up to 1,000 police officers within 30 days when needed.[31] The experience to set up the process to achieve this Headline goal could be used to create such civil-military homeland security units.

The EU should also be aware of the transatlantic dimension of homeland security and that homeland security has mutual interdepen-

[31] For more information on this see: Gustav Lindström, "The Headline Goal," online at http://www.iss-eu-org/esdp/05-gl.pdf downloaded December 2, 2005.

dencies on both sides of the Atlantic. The more safe the USA will be the less safe Europe will be. The better security measures prevent terrorist attacks, the coordination of terrorist organizations, their financing, the recruitment of new members and so on, the likelier it is, that such terrorist organizations will shift their attention elsewhere. They will shift to places where they can act in a more or less undisturbed environment. It is likely that such a place will be, among others, Europe.

With the European homeland is as unprotected as it is, the EU will be unable to conduct more ambitious ESDP-missions that are accomplished in an unfriendly or even hostile environment.

Building up a strategic partnership including homeland security issues, is a necessary step to strengthen the transatlantic dialogue between Europe and the USA. Given the fact that Austria tried to keep neutral in the transatlantic dispute over Iraq 2003, it can be argued that Austria might have a role of a mediator to improve the transatlantic relations. But a frank analysis of the Austrian position in security policy will lead to the conclusion that in Austria the political intention for such a distinguished and ambitious security policy is absent.

For this reason the expected profile of the Austrian EU presidency will be limited to the function of a honest broker and a facilitator of ongoing and already initiated European programs and processes. In this context homeland security policy will fit in to this big picture.

Chapter 5

What Does the United States Need to Do? The United States and Homeland Security

Lawrence J. Korb

Fighting terrorist networks abroad is a vital part of protecting the American people, but it is far from a comprehensive strategy. The United States must also work relentlessly to ensure that we do not suffer any more devastating attacks on our own territory. Homeland security is one of the most complex tasks we face, but complexity is no excuse for inaction. Terrorist groups like Al-Qaeda have the luxury of targeting Americans at the time and place of their choosing.

To be sure, the United States has made some progress in safeguarding the homeland since the attacks of September 11, 2001. Over White House objections, Congress created the Department of Homeland Security (DHS) to consolidate in a single agency border protection, immigration, transportation safety, emergency management and more. The Bush Administration has also created several other new positions and centers. These include the White House Homeland Security Adviser, the Director of National Intelligence, the National Counter Terrorism Center, and the National Security Service in the FBI. The Pentagon has created a new combatant command, the Northern Command (NORTHCOM) and an assistant secretary of defense with responsibility for protecting the homeland.

In 2002, the Department of Homeland Security issued the first National Strategy for Homeland Security and more recently identified the kinds of attacks most likely to cause catastrophic casualties and damage. Washington has also increased funding for federal agencies, state governments and local communities. And some private sector companies have increased security. In June 2005, the Pentagon

released its strategy for homeland defense and civil support, which delineated the role of the Department of Defense (DoD) in homeland defense and homeland security over the next decade.[1]

The Problem

However, more than four years after 9/11, homeland security in the United States is not the priority it should be. As analyses from the Homeland Security Department's Inspector General, the Government Accountability Office (GAO), congressional committees, and the 9/11 Public Disclosure Project (a group established by the 9/11 commissioners to see how its recommendations are implemented) demonstrate, the administration's efforts to protect the homeland have been slow at best and reckless at worst, leaving the American people far less secure than we should be more than four years after 9/11. Policies and funding priorities only vaguely reflect the professed strategy or the numerous other blueprints that have followed. The public disclosure project concluded on October 21, 2005 that the Bush Administration and the Congress have made minimal or unsatisfactory progress on more than half of its recommendations. And in its final report on December 5, 2005, the commissioners gave the U.S. government grades of C, D, and F on 28 of its 41 recommendations.[2]

Examples of our failings in this area are numerous. Our borders are still porous. Only those who fly into the country are screened by the Department of Homeland Security's Biometric Identification System. Visitors at land border checkpoints are not screened and the 25,000,000 people flying in represent only 3 percent of those who come to the United States each year.[3] Moreover, there are only 10,000 border patrol agents guarding the 8,000 miles of land borders, and

[1] Department of Homeland Security, *National Strategy for Homeland Security*, July 2002. Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005.

[2] Philip Shenon, "9/11 Panel Criticizes Reform Effort at the F.B.I," *New York Times*, October 21, 2005, p. A19. 9/11 Public Disclosure Project, *Final Report on 9/11 Commission Recommendations*, December 5, 2005, available at http://www.9-11pdp.org/. For a summary of all the failings of the Bush Administration in this area see Richard A. Clark, "Things Left Undone," *The Atlantic Monthly*, November 2005, pp. 37-38.

[3] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports of Entry, Office of Inspector General, Department of Homeland Security, February 2005.

only 1,000 of these agents patrol the 3,000 mile long border with Canada. Finally, the number of immigration agents has remained steady at 2,000 while the number of people unlawfully present in the U.S. has risen from a few million in the early 1990s to 12 million.[4]

Protection of our sea coasts is not in much better shape. Only 5 percent of the 9,000,000 sea going containers, that enter this country, are even given a cursory examination for signs of use or infiltration.[5] The Customs Trade Partnership against Terrorism relies primarily on the "pledge" of shippers to send the only "legitimate cargo," rather than having customs agents validate security for these shippers.[6]

The primary agency for safeguarding this country from threats from the sea is the Coast Guard. Yet this nation's oldest sea service has only 186 aircraft, 88 cutters, and 40,000 people to protect 95,000 miles of shoreline and 3.4 million miles of open water of our economic zone. Moreover, many of the Coast Guard ships are nearing the end of their useful service lives. Of the world's 39 naval fleets, the U.S. Coast Guard ships are on average younger than only one other fleet.[7] Given the fact that the coast guard budget for buying new ships and aircraft in fiscal year 2005 was only $1 billion ($20 million less than 2004), this situation will not improve soon.

The nation's capability for finding terrorists once they are here is not much better than our ability to prevent their entering. The FBI, rather than DHS, has been given the domestic counter terrorism mission even though the bureau bungled the mission prior to 9/11. Yet four years after 9/11, it still has not overhauled its anti-terrorism programs and is still plagued by institutional customs and cultures that continue to resist change. Thus, it is not in much better shape to carry

---

[4] Blas Nuñez-Neto, Border Security: The Role of the U.S. Border Patrol, CRS Report for Congress, Updated May 10, 2005, available at http://www.fas.org/sgp/crs/homesec/RL32562.pdf. Heritage Foundation, *Executive Memorandum No. 982*, September 25, 2005.

[5] 9 Million Containers: Audit of Targeting Ocean Going Inspection Containers (unclassified summary), Office of the Inspector General, Department of Homeland Security, July 2005. 10% inspection rate: Alex Ortolani and Robert Block, "Keeping Cargo Safe from Terror," *The Wall Street Journal*, July 29, 2005.

[6] Cargo Security: Partnership Program Grants Importer Reduced Scrutiny with Limited Assurance of Improved Security, Report to Congressional Requesters, Government Accountability Office, March 2005 (GAO-05-404).

[7] Mimi Hall, "Coast Guard Plagued by Breakdowns," *USA Today*, July 6, 2005.

out this mission now than it was on September 11, 2001. The FBI's $170 million software program, which is supposed to let agents in one city let agents in another city know what they have in the files, does not yet work; as of July 2005, the bureau has over 8,000 hours of wiretap recordings not yet translated; and the FBI still does not provide much useful information to state, local, and private sector security directors.[8]

Airline security is supposed to be a high priority, but despite the fact that the Transportation Security Administration (TSA) has 60,000 employees and a $5 billion a year budget, a Government Accountability Office (GAO) study has concluded that screening of checked passenger baggage is still inadequate.[9]

Train and subway security is in even worse shape. Despite the fact that every day ten times more people use public transit than fly, and that terrorists have targeted surface transportation far more than aircraft, the federal government has allocated only $155 million of the $6 billion necessary to secure the nation's transit systems. In effect, the federal government spends only 2.5 cents on rail subway security for every dollar it allots to aviation security.[10]

The federal government has actually compounded the problem of surface security by allowing highly lethal chemicals and gases to be shipped routinely on rail cars through major urban areas, and for the first time in three decades, it approved replacement of a liquid natural gas tank port in a city.

But, the greatest failure of the Bush Administration over the last four years in protecting the homeland has been its unwillingness to accelerate its efforts to secure Russia's nuclear bombs and other weapons-adaptable nuclear materials, which are subject to theft or diversion. Less nuclear material has been secured in the past four years than in the four years before 9/11 because we have spent less money on the Nuclear Cooperative Threat Reduction (Nunn-Lugar)

---

[8] Shenon, op. cit.

[9] Aviation Security: Screener Training and Performance Measurement Strengthened But More Work Remains, Government Accountability Office, May 2005 (GAO-05-457).

[10] Center for Defense Information and Foreign Policy in Focus, *A Unified National Security Budget for the United States*," May 2005, p. 39.

program in that time. As the 9/11 commissioners noted in their final report, "Countering the greatest threat to America's security is still not the top national security priority of the President and the Congress." At the present rate, the job will not be finished until 2022, despite the fact that a terrorist acquiring this material could use it to kill more than 1 million people in a major American city.[11]

Nor are we much better prepared to deal with the aftermath of another terrorist attack. For example, police and firefighters in large cities still cannot communicate reliably in a major crisis, and no American city has sufficient excess capacity to deal with such occurrences as a major lethal chemical plant attack, rail car leak, biological weapons attack or pandemic. For example, only 10 percent of fire departments nationwide have personnel and equipment to handle a building collapse, police departments throughout the United States do not have protective gear required to secure a site after an attack with WMD; public health laboratories in most states do not have the basic equipment to adequately respond to chemical or biological attacks, and most cities do not have the equipment needed to determine which hazardous agents emergency responders are facing following an attack.[12]

Finally, as the response to Hurricane Katrina demonstrates, DHS has made only limping progress in the admittedly difficult task of integrating 22 agencies and 180,000 employees. Despite the creation of the Homeland Security Council in the White House and the promulgation by the DHS of a National Response Plan, homeland security remains bureaucratically separated from national security inside and outside the White House. This was demonstrated by a Joint Chiefs of Staff (JCS) review of the failed response to Hurricane Katrina. According to the JCS, DHS response plans lack detail on how the Pentagon and other federal agencies should assist local leaders in the event of a natural of man-made disaster.[13]

---

[11] Ibid, p. 34, and the *Final Report on the 9/11 Commission Recommendations*, p. 14.

[12] See *Emergency Responders: Drastically Underfunded, Dangerously Unprepared*, Independent Task Force on Emergency Responders, Council on Foreign Relations, June 2003, *Defeating the Jihadists: A Blueprint for Action, Richard Clarke, et al.*, Century Foundation, 2004, p.129, and Stephen Flynn, *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism*, HarperCollins, 2004.

[13] Tom Bowman, "Reviews Fault U.S. Disaster Response Plans," *The Baltimore Sun*, October 24, 2005, p. 1.

Perhaps most egregiously, the government has failed to take the necessary steps to protect citizens from catastrophic risks posed by terrorist attacks on our critical infrastructure, 85 percent of which is owned by the private sector. Every day thousands of chemical plants manufacture and use deadly chemicals such as chlorine that, if released into the atmosphere, can cause massive casualties. Yet the White House has effectively turned over responsibility for protecting the public to private companies that too often have chosen not to bide by voluntary safety standards. The government has defended industry's right to ship toxic substances through major urban areas, been lax in safeguarding civilian and military nuclear facilities, and removed potentially life-saving public information from the Internet. It has underfunded and given scant attention to the protection of railways, the electrical power grid, the country's computer systems, and emergency personnel. Nor has it adequately prepared communities for a potential catastrophe.[14]

The Reasons

Why has so little has been done to protect the homeland since 9/11? There are three interrelated reasons.

First, and foremost is the lack of funding. In any area of government, dollars are policy. Not only did the president not raise taxes after 9/11 to fight what he calls the global war on terrorism, he actually continued to cut them. Consequently the federal government is running annual deficits of about $500 billion, making it difficult to allocate increased funds to many areas of the federal budget, including Homeland Security.

Moreover, when it comes to allocating scarce resources to threats to our national security, the Bush Administration has emphasized or given priority to the offensive component of its national security strategy. Since 9/11 spending for the offensive component the Department of Defense has risen from $304 billion to $442 billion, not counting the $300 billion spent on the wars in Iraq and Afghanistan. This

[14] Lawrence J. Korb and Robert O. Boorstin, *Integrated Power: A National Security Strategy for the 21st Century*, Center for American Progress, June 2005, p. 42.

increase is more than three times the entire annual budget for Homeland Security, which is currently $40 billion.[15]

Second, the strategy of the Bush Administration to combat radical jihadists is to fight them over there in Iraq so we do not have to fight them here. Since the invasion of Iraq in March 2003, the United States has spent more than $200 billion prosecuting the war in that country. This is about five times what the administration spends annually on Homeland Security. Moreover, we continue to spend nearly every six weeks in Iraq more than we spend yearly on Homeland Security. For example, this country could provide security upgrades for or all subways and commuter rails for what we spend every 20 days in Iraq; security upgrades for 361 ports for four days in Iraq; and explosive screening for all U.S. passenger airliners for ten days in Iraq.

In addition, because so much of the National Guard's personnel and equipment is in Iraq, the Guard would have severe problems in responding to a natural or man-made disaster in the United States. In December 2005, seven of the Army National Guard's enhanced or top notch brigades and their equipment were in Iraq. Consequently, according to the GAO, guard units in the U.S. have only 34 percent of their authorized equipment.[16]

Finally, the war in Iraq has monopolized the time and attention the president and his security team leading them to ignore many of the problems of homeland preparedness. As we have seen in the aftermath of Hurricane Katrina, neither the president nor his advisers realize how unprepared this nation is for a natural let alone a man-made disaster, that is, another major terrorist attack.

This emphasis on fighting them over there so we will not have to fight them here and using the National Guard as adjuncts to the deployed Army is very much in keeping with the American tradition, that dates back to World War I, of taking the fight to the enemy. However, after the attacks of 9/11, that mindset should have changed. In the age of global terrorism, protecting the homeland should be

[15] The budget for DHS is $27 billion. Not counting funds in the Department of Defense's Homeland Security programs, 31 other agencies spend $13 billion on homeland security.

[16] David S. Cloud, "Lack of Equipment Slowed the Guard, Report Contends," *The New York Times*, October 21, 2005, p. A20.

given equal priority with projecting power abroad. But this balanced approach has not been embraced in practice by the Bush Administration. Four years after 9/11, combating the terrorists in Iraq and Afghanistan receives the bulk of time, attention, and money.

Ironically, an activist foreign policy of taking the fight to the enemy should require a strong homeland security policy to protect one's population from retaliation by the enemy. However, the Bush Administration feels that engaging them overseas will actually have the opposite effect. By sending the forces to Iraq, the Bush Administration wants to make that nation the new front in the global war on terror. It hopes to draw into Iraq those radical jihadists who otherwise would focus on attacking the U.S. homeland. The fact that the invasion of Iraq has not only increased the number of terrorists with a global reach, but also offered these new recruits training in terrorist tactics seems not to have occurred to the president and his advisors.

Third, there is ongoing historical tension in this country over the appropriate size of the government and the appropriate role of the various levels and branches of government. Republicans, who currently control both the executive and legislative branches of the federal government, are against big government and for a unilateral foreign policy. Therefore, when DHS came into existence, the administration tried to make it revenue neutral, that is, the new department would receive no more money then the 22 previously existing organizations that merged into it. And to pursue a unilateral foreign policy, the Republicans feel this nation needs a national missile defense. Consequently, the Bush Administration now spends six times more per year on national missile defense than on port security and more on national missile defense than the entire Coast Guard, even though there is a much greater likelihood that a nuclear weapon will enter this country in a shipping container than on a long-range missile.[17]

The federal system also complicates responsibility for Homeland Security. Because of skyrocketing national budget deficits, the federal government seeks to get hard pressed state and local governments to take on the responsibility for protecting their own areas. For example, nearly one third of the states had to cut their public health budgets in

[17] In fiscal year 2005, the Bush Administration spent $7.6 billion on the Coast Guard and $11 billion on Missile Defense.

the last two years.[18] Moreover, when the federal government does give grants to state and local governments, their representatives in the Congress insist that the same priority be given to low risk rural states as endangered populated areas. Thus, states have used federal Homeland Security funding on such "critical" projects as air conditioning garbage trucks and buying Kevlar body armor for dogs.

The Solutions

Urgent action is required to prevent future attacks, reduce existing threats, and manage the consequences of a successful attack on the U.S. homeland. Given current federal budget deficits and constant constraints on resources, we must apply our energies and resources to those targets where an attack would cause the greatest loss of life and economic damage. We must also escape the "protect against the last attack" mentality that followed 9/11 as evidenced by disproportionate spending to protect airline passengers while shortchanging other important areas.

An effective homeland security strategy must have three primary components: detecting and disrupting potential terrorist attacks while protecting civil liberties; guarding critical infrastructure; and improving emergency planning, response and recovery. In each of these areas the United States must provide funding according to the magnitude of the vulnerability; increase transparency; and—where applicable—invest in research and development. The combination of trained personnel and our country's natural advantages in technology and science will prove critical to our success.

Preventing Attacks

As the 9/11 Commission and others have argued, the United States must move immediately to improve our domestic intelligence agencies, upgrade detection and warning systems, and improve border security. Achieving these goals will require extraordinary efforts to change institutional cultures and will mean long-term commitments of resources.

---

[18] *A Unified National Security Budget for the United States* Ibid, p. 8

As part of this, we must also reverse the policies adopted in the wake of 9/11 that violate core American values, threaten our economic growth and pose false choices. We can both disrupt terrorist networks and protect civil liberties. We can keep our doors open to non-citizens who make a real and lasting contribution to our society and still bring to justice terrorists who have taken up residence in the United States. The United States must take the following actions:

- Increase dramatically the FBI's counterterrorism capabilities and upgrade its analytic staff and information technology.
- Improve intelligence sharing within the federal government and establish Homeland Security Operations Centers in critical locations to improve the flow of threat information between federal and state and local authorities.
- Update airline passenger screening to include use of consolidated terrorist watch lists and improve the speed with which international and domestic airlines share passenger manifests with appropriate authorities.
- Introduce biometric technology within three years at all land, port and air terminals while implementing strong and appropriate privacy safeguards.
- Implement immediately the top priority recommendations of the National Strategy to Secure Cyberspace, including special efforts to guard the banking and financial sectors.
- Amend the Patriot Act to rescind all authorities that do not enhance American security from terrorists. Require the FBI to demonstrate clearly that any request for additional authorities will enhance our security from terrorists without unnecessarily limiting our civil liberties.

Securing Critical Infrastructure

The years since 9/11 have taught us that purely voluntary approaches are insufficient to safeguard communities from attacks on chemical plants and other potential terrorist targets. Tax incentives, low interest loans and homeland security grants to relieve some financial burden on industry can encourage the upgrading and implemen-

tation of stronger security standards. But, where voluntary codes and incentives fail, the United States should create new regulations and legal safeguards. These should be based on a national infrastructure protection plan with priorities guided by a comprehensive inventory and assessment of public and private critical infrastructure. At every step, the United States should increase transparency and provide communities with as much information as possible about hazards and emergency procedures while protecting data that is classified or could be used to assist an attack. The United States should:

- Implement a 12-month action plan to reduce risks posed by chemical facilities by creating a priority list of vulnerable sites; issue new federal guidelines to reduce hazards, introduce safer chemicals; and institute hazard-reduction and target-hardening measures.

- Improve port security by increasing Coast Guard funding; accelerate implementation of the Maritime Transportation Security Act; and promote global standards, research, and installation of state-of-the-art container safety and scanning technology.

- Improve air security by instituting 100 percent air cargo screening funded by a surcharge on shippers; upgrade explosive detectors at airports; increase perimeter security at airports; and fund continued research to deter the threat to commercial aircraft from shoulder-fired missiles.

- Redirect hazardous rail shipments away from urban centers, including prime targets such as Washington, D.C.; provide resources to help localities better protect rail tracks and train stations; and implement comprehensive security standards for the transport of hazardous materials.

- Set and enforce more stringent security standards at nuclear power reactors and other facilities where nuclear and radiological materials are used or stored, and transfer responsibility for safety at all nuclear facilities to the National Nuclear Security Administration.

- Design and coordinate new regional plans to provide protection and backup for the country's electrical power grid.

Improving Emergency Preparedness and Response

The United States must invest in emergency response personnel, equipment and technology that will minimize damage and speed recovery in the case of a successful attack. Much of the ultimate cost of a terrorist attack depends upon the speed and effectiveness with which the government responds. Our goal must be to prevent significant casualties, destruction of property, economic disruption, and a loss of public confidence in government policies and institutions. On the positive side, investments in this sector will also improve our country's everyday health, law enforcement and emergency services capabilities.

The nature of today's weapons and a terrorist group's asymmetric advantages, and public psychology mean that every incident will require a tailored plan and response. Our most effective federal plan is to focus on the basics. That means integration at all levels: unifying so-called "crisis management" and "consequence management" plans; rationalizing responses from the public and private sectors; linking federal, state and local government personnel; and standardizing preparation and response measures.

Completing these tasks requires, first and foremost, a new reporting and information-sharing system in which decision makers and emergency personnel speak the same language and understand how individual tasks fit into an overall plan. It will also require a new federal commitment to helping states and localities receive homeland security grants and get reimbursement for unexpected security costs. Only then will we build the cooperation and confidence necessary to assess, respond, recover and adapt our strategy to prevent future attacks. The United States must:

- Improve tactical counterterrorism, with a focus on response to an attack in an urban area using a nuclear weapon, biological agent, or radiological bomb.
- Create specialized National Guard units devoted to incident response that are not deployed overseas except in times of extreme national emergency.
- Invest in public and private efforts to improve chemical, biological and radiological sensors; develop and prepare to use decontamination processes; and upgrade medical surveillance capabilities.

- Increase pharmaceutical and vaccine stockpiles and invest in development and distribution systems for a broad spectrum of vaccines, preventive medications and antidotes.
- Replace the current color-coded public alert scheme with a system that issues warnings to the general public only when specific actions need to be taken.
- Work with the insurance industry to create a permanent risk arrangement system, such as a government-sponsored reinsurance corporation capitalized by the private sector and backed by the government.

The Costs

Taking all these steps can be done by increasing the budget for Homeland Security by $25 billion a year.[19] While this is not an insignificant amount, it represents only 5 percent of what the Bush Administration spends on the offensive component of national security. More than $25 billion can be found in the defense department's annual budget by eliminating obsolete weapons like the F/A-22 and the Virginia class submarine, which are designed to fight enemies from a bygone era, keeping national missile defense in a research mode until it is fully tested, and reducing our nuclear weapons stockpile from 7,000 to 1,000 warheads.

Conclusion

Protecting the U.S. homeland will require a shift in attention and priorities. Since 9/11, the Bush Administration has focused too much energy and resources on the offensive component of national security and not enough on the defensive or Homeland Security portion. But, unless it takes the steps outlined above, it may win the battle abroad, but lose the war at home, which after all is the goal of the radical jihadists.

Chapter 6

Structures and Cultures—Civil-Military Cooperation in Homeland Security: The Danish Case

Anja Dalgaard-Nielsen

"This is a warning to all European countries, but first and foremost to Denmark, which still has soldiers in Muslim countries," ran a message posted on the internet and signed by the Abu Hafs al-Masri Brigades in the wake of the terrorist attacks on London, July 7, 2005.[1]

The Abu Hafs Brigades are not believed to have operational capabilities and the group therefore hardly poses a direct threat to European security. The message nevertheless highlighted a politically awkward fact: Surely, keeping a distance from the US is by no means a guarantee against Al-Qaeda inspired terrorism, witness the threats issued against France in 2004 due to its law banning religious symbols including Muslim headscarves in public schools.[2] Yet, being a close ally of the US and maintaining troops in places like Iraq and Afghanistan can bring a country unwanted attention from the international Al-Qaeda inspired salafi-jihadist movement or contribute to domestic radicalization.

In a 2004 report the UK's Home Office pointed to the British presence in Iraq as a driver of domestic radicalization—radicalization made plain when home grown terrorist struck the London subway in

---

[1] Cited in "Ny terrortrussel fra Al Qaida-gruppe," *Jyllands-Posten*, July 13, 2005, p. 1.

[2] For threats against France, see Roger Cohen, "A French ex-hostage describes his ordeal," *International Herald Tribune*, 10 January, 2005; Alan Riding, "France Reports Threat From an Islamic Group," *New York Times*, 17 March, 2004.

July 2005.[3] In Denmark's case, the engagement in Iraq has sparked more frequent coverage of the Scandinavian country in the Arab media and it has been singled out in extremist warnings on a number of occasions beginning in August 2004. In sum, international engagements might well increase the threat to the homelands of America's European partners.

Foreign and security policy neither should, nor can be adjusted to placate the people who subscribe to Al-Qaeda's world view. Yet, arguably an activist foreign policy like the Danish or British must go hand in hand with a robust, flexible, and coordinated homeland security system. Homeland security is here defined as coordinated efforts to prevent, protect, and respond to terrorism as well as natural or man-made disasters.[4]

The need for enhanced civil-military cooperation to create homeland security is, as elaborated elsewhere in this book, increasingly emphasized on both sides of the Atlantic. This chapter, with a view to extracting lessons of relevance to policy-makers and practitioners on both sides of the Atlantic, looks at ongoing Danish efforts in the field.

Civil-military cooperation, it is argued, depends on forging the right structures (joint planning processes; clear distribution of functions and responsibilities; clarity as to chain of command; information sharing; joint exercises and evaluation). However, the chapter points out, effective homeland security also depends on the existence of a culture of cross-governmental cooperation. Otherwise, the friction that arises between differing civilian and military organizational cultures might undermine the best thought out plans and policies. A culture of cross-governmental cooperation, the chapter suggests, could be promoted by more joint education of the leaders of the

[3] Home Office, "Relations with the Muslim Community," April 6, 2004.

[4] The definition corresponds to the all-hazard approach taken by most European governments. Though the definition of homeland security in the US National Strategy for Homeland Security emphasizes only terrorism, the Department of Homeland Security is increasingly emphasizing the all-hazard approach as well. For the US definition of homeland security see Office of Homeland Security, *National Strategy for Homeland Security*, Washington DC, 2002, p. 2. For the emerging emphasis on all-hazards see Department of Homeland Security, "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," Office of the Press Secretary, July 2005.

involved agencies, since these elites are the key shapers of organizational culture.[5]

The chapter opens with a brief discussion of the structural and cultural requirements for effective and efficient civil-military homeland security cooperation. It proceeds to use the Danish case to illustrate these requirements. It provides an overview over current Danish efforts and discusses the hurdles and obstacles encountered in the process of enhancing civil-military homeland security cooperation in Denmark. Finally, it is pointed out how some of these hurdles might be overcome, and what other countries may learn from the Danish experience.

Structure and Culture: Requirements for Civil-Military Cooperation

The militaries of the transatlantic area have from time to time provided help to national emergency management agencies or rescue services in connection with natural disasters or other emergencies. Thus, military assistance to civilian authorities is not new. Extreme weather conditions as well as accidents and disasters continue to pose challenges, witness the havoc wrought by Hurricane Katrina. However, with the rise of Al-Qaeda inspired terrorism, risks to the homeland have become more unpredictable in terms of their nature and their scope. Engineered disasters, such as multiple simultaneous terrorist attacks or incidents involving CBRN (Chemical, Biological, Radiological, Nuclear) materials have become more likely.[6]

The new threat environment raises new questions and poses new challenges to both the civilian and the military side—the military might be required to perform a broader range of tasks to protect the homeland, and both civilian and military actors will have to adjust habits and customs as the military's role expands.

---

[5] The chapter is based on a review of key policy documents combined with personal interviews with high ranking representatives from the involved agencies, including the Danish National Police, Danish Defense Command, the Ministry of Defense, the Danish Prime Minister's Office, and the Danish Emergency Management Agency. The interviews were carried out between June and October 2005.

[6] Department of Defense, *Strategy for Homeland Defense and Civil Support*, Washington DC, June 2005, p. 1.

A number of Rand studies have pointed to the need for an examination of military doctrine, organization, training, leadership development, and materiel in light of new homeland security tasks. They point out that the military needs to contemplate and plan for multiple tasks such as providing facility security and infrastructure protection (patrolling, protection, air defense systems, expertise as regards protection of IT systems); support to law enforcement (sharing intelligence, training facilities, expertise, specialized equipment, and provide direct support for civil law enforcement); reassurance (presence, patrolling, guard duty); WMD protection (detection, decontamination, evacuation, search and rescue, medical treatment); and consequence management (crowd control, provide utilities, food and shelter, removal of debris, reconstruction).[7]

The US Department of Defense has issued a Strategy for Homeland Defense and Civil Support, in which it addresses overall questions regarding tasks, priorities, organization, training, and materiel. In turn, NORTHCOM—the US command in charge of defense of the homeland—based on fifteen different threat scenarios has drafted plans for the military's role in homeland security based on fifteen different crisis scenarios. Current planning spans from modest support missions with civil authorities in the lead to major emergency management efforts after a mass-casualty CBN-attack—a scenario in which the military due to the scale and severity of the crisis is foreseen to take the lead. On the European side of the Atlantic, European military research institutes have begun to address some of the same questions.[8]

However, a flexible, coordinated, and cost-effective homeland security effort arguably requires not just the armed forces, but all major actors in homeland security to critically analyze existing structures—plans, functions, responsibilities, processes, chains of command, and channels of information. Moreover, the effort should, at least at the strategic level, be joint, not agency specific.

---

[7] Lynn E. Davis, David E. Mosher, Richard R. Brennan, Michael D. Greenberg, K. Scott McMahon, Charles W. Yost, *Army Forces for Homeland Security* (Santa Monica: Rand, 2004); Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options* (Santa Monica: Rand, 2001), p. 21.

[8] Department of Defense, *Strategy for Homeland Defense and Civil Support*, Washington DC, June 2005; Bradley Graham, "War Plans Drafted to Counter Terror Attacks in the U.S.," *Washington Post*, 8. August, 2005. For an example of European research, see Heiko Borchert (ed.), *Mehr Sicherheit—Weniger Souveränität. Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte* (Hamburg: Verlag E. S. Mittler & Sohn, 2004).

A coordinated and cost-effective effort requires the civilian and the military side to develop a common understanding of what tasks the military should perform or support, what capabilities it should provide, how fast, and for how long. This requires at least rough agreement on the probability of various scenarios and the response capabilities required in each, as well as an overview over the capabilities already available in the civilian system. In other words, national police forces, emergency management agencies, and the armed forces need to develop common planning scenarios and common planning goals.[9]

Common scenarios and planning goals also entail clarifying who is responsible for what. The British experience refined over years of combating IRA terrorism indicates that such clarity is central in order to prevent that bureaucratic turf wars impair and delay the effort. Likewise, the problems that hampered the US response to Hurricane Katrina illustrated the importance of such clarity—gaps between local, state-level and federal planning efforts have been identified as one of the key problems leading to late and insufficient evacuation, rescue, and relief efforts. Thus, the establishment of clear areas of responsibilities should be combined with an overview over all levels of the homeland security system to make sure that important issues do not fall between the cracks in a layered system.[10]

At the operational level mechanisms of coordination, clear lines of authority, and a common situational picture are important to ensure an effective multi-agency response to major incidents. Coordination of the rescue effort in New Orleans in the wake of Katrina, involving federal, state level and local personnel, was hampered by the existence of three parallel chains of command instead of one. Likewise, the September 11th Commission has documented how the rescue effort in the towers of the World Trade Center was hampered by the absence of coordination, unity of command, and a com-

[9] Lynn E. Davis, "Defining the Army's Homeland Security Needs," in Lynn E. Davis and Jeremy Shapiro, *The US Army and the New National Security Strategy* (Santa Monica: Rand, 2003), p. 66.

[10] "Hurricane Katrina and US homeland security," *IISS Strategic Comments*, Vol. 11 Issue 7, September 2005; Terence Taylor, "United Kingdom" i Yonah Alexander (red.) *Combating Terrorism. Strategies of Ten Countries* (Ann Arbor: University of Michigan Press, 2002), s. 197.

mon situational picture. Some floors were searched twice by different services, and according to witnesses, some fire fighters in the World Trade Center's North Tower refused to take evacuation orders from New York Police Department officers after the collapse of the South Tower. Finally, 911 operators, unaware that the South Tower had collapsed, told callers from the North Tower to stay in place and wait for help at points in time when emergency stairwells were still passable.[11] Finally, joint training, exercises, and evaluation are key to identify gaps in the structures as well as to keeping policies and plans updated and operational skills honed.[12]

International coordination and standardization when it comes to forging these structures would, obviously, add further robustness to national systems. It would facilitate the stepping in of partner countries to support a country whose national capabilities are overwhelmed by a catastrophic incident. The EU is cooperating on a number of homeland security areas, as elaborated elsewhere in this volume. Transatlantic homeland security cooperation is also on the rise.[13]

In sum, the past years have seen an increased focus on the need to forge new plans, priorities, structures, and processes in order to enhance civil-military cooperation in homeland security. Yet, though forging the right structures is important, arguably, it is not sufficient. Culturalist theories of organizational change would emphasize how friction between differing organizational cultures (the values, beliefs, and assumptions shared by the members of an organization) may derail even the best thought out policies and plans. Diverging perceptions of the environment and of the homeland security mission, diverse notions about methods and instruments to be deployed, differ-

[11] "Hurricane Katrina and US homeland security," *IISS Strategic Comments*, Vol. 11 Issue 7, September 2005; The National Commission on Terrorist Attacks on the United States, *The 9/11 Commission Report*, (Washington DC, July 2004), p. 295, 310, 318, 321-322.

[12] United States Government Accountability Office, *Department of Homeland Security. Strategic Management of Training Important for Successful Transformation*, GAO-05-888, p. 1; Daniel R. Walker, *The Organization and Training of Joint Task Forces*, Air University Press, Maxwell Air Force base, Alabama, April 1996, p. 26.

[13] See Anja Dalgaard-Nielsen and Daniel Hamilton, eds., *Transatlantic Homeland Security. Protecting Society in the Age of Catastrophic Terrorism*, (Routledge, 2006).

ent success criteria, and resulting misunderstandings and mutual distrust are likely to complicate the effort.[14]

Thus, structural reforms do not in themselves ensure cooperation. On the contrary, they might trigger defensive reactions because specific organizational turfs, norms, and procedures are thus challenged.[15] Indeed, it appears, that the break-down of law and order and the slow relief effort in New Orleans in the wake of Katrina was not due to a shortage of personnel—the US was eventually able to muster 70.000 troops, 21 military vessels and 215 aircraft in the region hit by Katrina—but due to a reluctance on part of civilian actors to *request* this help.[16]

The reluctance to deploy troops at home has deep historical roots in many countries and can clearly not be overcome overnight. Yet, a starting point could be to utilize common education, exercises and drills of civilian and military actors to build mutual trust. Common education, exercises, and drills are, as noted above, crucial in honing skills and checking for gaps in planning and coordination mechanisms. But common education and training might also help promote a common understanding of the mission and the goals, promote a common language, common skills, mutual knowledge, and common experiences. Over time such activities might serve to make different cultures converge and to promote a common culture of cross-governmental cooperation.[17]

---

[14] On organizational culture and change see Jeff Dooley, Cultural Aspects of Systemic Themanager.org, available on http://www.themanager.org/Knowledgebase/Management/Change.htm (Accessed October 18, 2005). See also Ronald L. Jefferson, Wendt, Alexander, and Katzenstein, Peter J. (1996) "Norms, Identity, and Culture in National Security Policy," in Katzenstein, Peter J. (ed.) *The Culture of National Security*, Columbia University Press, 1996. The same argument applies to international cooperation where differing national security cultures may complicate international homeland security cooperation. The problem of diverging threat perceptions in Europe and the US respectively is discussed in depth elsewhere in this volume.

[15] Jeff Dooley, Cultural Aspects of Systemic Themanager.org, available on http://www.themanager.org/Knowledgebase/Management/Change.htm (Accessed October 18, 2005).

[16] US Senate Homeland Security Committee hearings have revealed conflicting perspectives on whether local, state, or federal level authorities are to fault for the failure to request this help in a timely fashion. Spencer S. Hsu, "Repeat of Past Mistakes mars Government's Disaster Response," *Washington Post*, October 16, 2005; Spencer S. Hsu, "Messages Depict Disarray in Federal Katrina Response," *Washington Post*, October 18, 2005; Senate Committee on Homeland Security and Governmental Affairs, Testimony of Marty J. Bahamonde, Office of Public Affairs, FEMA, October 20, 2005.

[17] Daniel R. Walker, *The Organization and Training of Joint Task Forces*, Air University Press, Maxwell Air Force base, Alabama, April 1996, p. 26.

In sum, existing policy studies of civil-military cooperation tend to emphasize the need to adjust military structures in order to create more effective civil-military homeland security cooperation. Yet, arguably it is necessary for all the major actors to jointly adjust their planning, processes, command arrangements, and training. In this process, policymakers pushing for increased civil-military cooperation must pay attention to distinct organizational cultures, which might otherwise undermine the effectiveness of the joint structures. A culture of cross-governmental cooperation should be actively promoted through education and training.

The Danish Case

The Danish efforts to promote civil-military cooperation in the field of homeland security should be of broader interest for three reasons. First, Denmark is a small country, with a tradition for cross-governmental and civil-military cooperation (for example Denmark has no coast guard and thus the navy carries out patrolling, maritime search and rescue, and environmental monitoring. Military special operations forces and police special units also have a long tradition for cooperating when it comes to special high-end tasks), and a relatively pragmatic view on using the armed forces to support civilian authorities in responding to disasters or accidents. Thus, Denmark should be well placed to intensify civil-military cooperation.

Second, and related, the need to ensure optimal use of scarce resources—be they civil or military—is likely to be more keenly felt than in larger countries.

Thirdly, unlike the US, Denmark has not been forced to reform its security system in the wake of a major attack on its soil—a situation not necessarily conducive to well thought through solutions. Instead, reform has been more gradual. Yet, the new experience of being singled out for salafi-jihadist attention adds a measure of urgency to the ongoing efforts and secures counter-terrorism a place near the top of the political agenda. Thus, political pressure might help soften bureaucratic resistance to structural changes that inevitably upsets old turfs, procedures and priorities, or, in other words, challenges organizational culture.

All in all, the Danish case should point to opportunities for other countries, yet, it might also indicate the sticking points, calling for particular political attention if civil-military cooperation is to become effective—if the implementation of a particular aspect of civil-military cooperation is problematic in a Danish context, it is likely to demand a very targeted effort in larger countries with more strict dividing lines between different government agencies.

The Danish homeland security system did receive a shake-up after September 11, 2001. Among the initiatives were new anti-terrorism laws, significantly expanded resources to the two Danish intelligence services, new equipment to the Danish Emergency Management Agency, and a Danish push for reinforced homeland security cooperation in the EU, among others, a proposal to develop a set of EU homeland security headline goals.[18]

As part of the effort to enhance Danish homeland security, civil-military cooperation has been intensified. The Danish Defense Forces Act (2004) established that Danish armed forces have two major tasks: To participate in international crisis management efforts and to support civilian authorities in the provision of homeland security in case of terrorist attacks, disasters or accidents.[19] The major civilian partners in homeland security at the national level are the National Police including the Danish Security Intelligence Service, both reporting to the Minister of Justice, and the Danish Emergency Management Agency (DEMA), originally reporting to the Minister of the Interior.

In an attempt to reduce the number of seams in the system, DEMA was transferred from the Ministry of the Interior to the Ministry of Defense as of February 2004. The reorganization, it was hoped, would permit rationalization through common use of support structures, logistics, schools, depots, and infrastructure. By creating a common

[18] For a fuller account of the reaction to September 11 in the Scandinavian countries see Anja Dalgaard-Nielsen "Homeland Security and the Role of the Armed Forces: A Scandinavian Perspective" in Heiko Borchert (ed.), *Mehr Sicherheit—Weniger Souveränität. Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte* (Hamburg: Verlag E. S. Mittler & Sohn, 2004).

[19] "Arbejdsgruppen vedrørende en samling af det civile beredskab og forsvarets opgaver," Copenhagen, December 2003; Forsvarsforlig, Ministry of Defense, Copenhagen, 10. June, 2004.

pool of resources, more common education, and common planning, it was also hoped, the system would become more efficient.[20]

Some critics argued that DEMA should instead have been transferred to the Ministry of Justice to avoid a militarization of the system. Opponents of this, however, argued that the functions of DEMA had very little affinity with the functions of the police and would fit more naturally under the Ministry of Defense. Thus, the Minister of Defense, through DEMA, is now responsible for coordinating cross-governmental civilian preparedness and response planning. The police, however, is responsible for operational coordination in case of an incident—natural or man-made—that requires a response from more than one governmental agency (for example police, fire fighters, and health workers).[21]

To expand the pool of personnel available for homeland security needs the education of Danish conscripts has been adjusted to focus on homeland security tasks. Conscripts currently serve four months and their education comprises basic skills such as guard duty, first aid, fire fighting and civil rescue support. Within three years of having completed the education they can be called up to serve in a "total defense force" with homeland security tasks.[22] The Danish Home Guard is likewise available to support homeland security needs. The Home Guard has almost 60,000 members and a tradition for assisting DEMA or the police in connection with disasters or large public events. If requested by the police the Home Guard assists with specific tasks in peacetime such as monitoring and guarding critical facilities, providing sanitary units, and assisting with traffic control.[23] A new Center for Biological Preparedness likewise is based

[20] Ministry of Defence on behalf of the Government, *Et robust og sikkert samfund. Regeringens politik for beredskabet i Danmark*, Copenhagen, June 2005, p. 7.

[21] Udvalget for National Sårbarhedsudredning, *National Sårbarhedsudredning*, Birkeroed, 2004, p. 28.

[22] For a fuller account of the role of the new homeland security force see Anja Dalgaard-Nielsen "Homeland Security and the Role of the Armed Forces: A Scandinavian Perspective" in Heiko Borchert (ed.), *Mehr Sicherheit—Weniger Souveränität. Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte* (Hamburg: Verlag E. S. Mittler & Sohn, 2004).

[23] Statsrevisoratet, 7/03 Beretning om hjemmeværnet, <http://www.ft.dk/BAGGRUND/statsrev/0703.htm#V> (accessed: 14. October 2004).

on cooperation between civilian medical personnel and the military, which makes transport capability available for the center's bio-hazard teams.

All in all the Danish system has already been revamped to enhance civil-military cooperation in homeland security and civilian and military agencies already cooperate on a number of tasks. Yet, as elaborated below, there are still shortfalls in the efforts to forge optimal structures—arguably in part due diverging organizational cultures between the major actors involved.

Common Planning Scenarios and Goals

To what extent have the actors in Danish homeland security developed a common threat and risk assessment, and a common understanding of what tasks the military should perform or support, what capabilities it should provide, how fast, and for how long?

At an overall level, representatives from the key agencies involved in homeland security at the national level—the Ministry of Defense, the Defense Command, DEMA, and the National Police—seem to share a common notion of the homeland security mission: a flexible and coordinated effort, drawing on the total resources of the civil and military sector in an effective manner. They also consistently emphasize the willingness to be pragmatic in the search for mutually acceptable solutions to reach that common goal.[24]

On a number of more specific issues, however, they differ. Firstly, threat perceptions diverge. Whereas the military is contemplating a range of events, from small scale to mass-casualty incidents, the police mainly focus on smaller events, where the need for resources would not overwhelm civilian actors.

The police emphasize that military units might assist civilian law-enforcement when it comes to monitoring or searching a large area, providing disaster relief, traffic control etc. Representatives of the police, however, insist that whenever a task entails even a small risk that it will be necessary to use force against civilians, it is a job for the

[24] Author's interviews, Copenhagen, July 12 and 14, August 17 and 19, 2005.

police, not military units.[25] There is reluctance when it comes to drawing on the typically young members of the total defense force for any tasks that might bring them into direct contact with the population (crowd control and some forms of guard duty). For softer tasks, such as traffic control, monitoring critical infrastructure or searching larger areas, the police prefer to rely on elements of the Home Guard—the so-called police home guard—rather than the total defense force.

Whereas the military emphasizes that situations might arise, in which all organized manpower resources could be needed and should be used across a range of tasks, they refer to the police as the actor, which is requesting and leading the joint effort, and thus should take the lead in developing planning scenarios and task lists. This reticence might reflect that Danish armed forces, in line with their American counterparts, do not wish to signal an intention to usurp the area of homeland security. Another reason, however, might be that whereas the military increasingly takes the homeland security part of its mission seriously, international deployments are still regarded as the core task. As the active component of the Danish military in line with the US military operates with dual-capable and in effect dual-hatted forces, situations with competing demands at home and abroad might arise. This points to the question whether certain assets should be earmarked for homeland security purposes. The US military has, for example, dedicated a command and control element together with a number of National Guard WMD-detection teams for domestic use only.[26]

Thus, the willingness to push for a systematic planning process, which could reveal the need for the military to earmark resources and capabilities for domestic use only, might be limited. The problem in this respect, however, is that the police have less of a tradition of strategic planning (scenario development, simulations and exercises, systematic feed-back from these and subsequent adjustment of plans and policies) than the military side.

---

[25] Author's interviews, Copenhagen, July 14, 2005.

[26] Department of Defense, *Strategy for Homeland Defense and Civil Support*, Washington DC, June 2005, p. 39. A related issue pertains to the planning horizon of different actors in the homeland security system. Whereas domestic situations requiring a manpower surge can arise with little or no warning (accidents, natural disasters, terrorist attacks, political events requiring a high level of security), the military planning horizon is typically longer and does not necessarily permit for the kind of flexibility the police would like to see.

As a result, there is currently no systematic effort to develop a range of common planning scenarios and goals like the ones produced by, for example, NORTHCOM and consequently, there is no clear cross-governmental consensus as to what specific tasks what military units should plan and train for in homeland security and whether certain capabilities should be earmarked for homeland security needs. A joint working group consisting of representatives from the police and the military is currently looking at various coordination issues, chiefly, though, legal and financial aspects of civil-military cooperation.

In sum, whereas the actors in the Danish homeland security system do have a common frame of reference regarding the overall mission—a flexible and coordinated effort drawing on the total resources of the civil and military sector in an effective manner—they have yet to converge on a common threat perception. Common planning scenarios and common planning goals, making explicit what tasks the military should perform and what, if any, capabilities should be earmarked for domestic use only are still to be developed. Developing joint scenarios, including high-end incidents, and planning goals would not only make the Danish system better prepared to handle extreme incidents—a systematic process of imagining, planning for, gaming, exercising and evaluating a range of different scenarios is arguably a key ingredient in creating the flexibility that the major actors themselves identify as a key goal.

Operational Coordination

To what extent are areas of responsibility and lines of authority and operational command and control clear in the Danish system?

The Danish emergency management system is based on the principle of sectoral responsibility. This entails, that the agency, which in normal times have responsibility for a given area maintains responsibility in case of a crisis, disaster or terrorist attack. DEMA is supervising the emergency preparedness plans and procedures of the different agencies. With the aim to create a more coherent emergency planning system a number of cross-governmental coordination groups have been established and DEMA is currently developing uniform guidelines for vulnerability- and risk assessment to be applied across the government.[27]

[27] Ministry of Defence on behalf of the Government, *Regeringens redegørelse om beredskabet*, June 2005, p. 4.

The Danish system has three levels, based on the principle that local actors respond first. If an incident exceeds a certain scale, local efforts are supported by resources from the so-called regional preparedness centers. The local chief of police is coordinating multi-agency local crisis management efforts as well as the regional reinforcements. If local and regional resources are overwhelmed by an incident on a national scale or multiple serious incidents in more locations a new National Operative Staff chaired by the National Police Commissioner will be activated to coordinate the effort. The staff is composed of representatives from the National Police, the Defense Command, and DEMA as well as other agencies depending on the nature of specific incidents. The task of the staff is to "establish and maintain an overview" over an incident/incidents in order to "provide the foundation for making decisions about coordination and prioritization" in the management of the incident/incidents.[28]

In terms of lines of authority, the Danish system appears clear and should permit Danish authorities to avoid the problems that hampered for example the US response to Katrina, arising from unclear or parallel lines of command and authority.

The national staff is an important innovation. The system of locally coordinated response reinforced, if necessary, by regional or national resources, works well when it comes to handling the most likely smaller or medium size incidents. Yet, it is not geared to handle a situation where the scale of an incident makes resources scarce; and, thus, requires a central prioritization of national resources between different localities. The national staff has the potential to fill this gap.

Ironically, though, the staff, or in case of internal disagreement, the chairman of the staff, is not given the mandate to decide authoritatively how to prioritize resources in case of more simultaneous incidents and a need that exceeds the available capacity. Some of the involved actors consider such a prospect rather theoretical and believe that should it arise, peer pressure would ensure that the necessary decisions would be taken anyway.[29] Yet, replacing the currently rather

[28] Ministry of Defence, *Regeringens redegørelse om beredskabet*, Copenhagen, June 2005, p. 6.

[29] Author's interviews, Copenhagen, July 14, 2005.

vague mandate with one giving staff/chairman the competence to decide authoritatively if necessary, however, would seem like a very inexpensive way of hedging against losing precious time due to arguments internally in the staff or between the national staff and local or regional actors during a national crisis.

Changing the institutional set-ups, however, is not enough. As pointed out by culturalist theories of organizational change and as illustrated with the establishment of the US Department of Homeland Security (DHS), the mere moving of different agencies into the same Department and giving a Secretary the authority to coordinate their activities does not in itself guarantee cooperation. Different cultures still clash inside the DHS and hamper cooperation.

Moreover, pushing too hard for clear lines of command and control might provoke a backlash complicating rather than facilitating cooperation, at least as long as the actors do not, as discussed above, share a common view of risks, probabilities, and tasks. In other words, leaving delimitation of responsibilities and lines of authority unclear in extreme, but not very likely situations might prevent turf wars and institutional anxieties from erupting. The down side to this, of course, is that the national system, as argued, will not be in optimal shape to handle a truly grave incident.

Education, Exercises, Evaluation

To what extent do the various actors in Danish homeland security train and exercise together and to what extent are the educational programs coordinated and integrated?

As mentioned above, the education of conscripts in the armed forces includes homeland security relevant tasks. DEMA has assisted the Danish Army Command in putting together this part of the new education. Moreover, DEMA officers and officers in the military services attend the same schools for part of their education. Finally, once a year DEMA, the Defence Academy and the National Commissioner organize a five-day seminar for employees of the central ministries, involved with national emergency management planning. The focus is

on national security and defense policy, national emergency planning, and crisis management.[30]

During the years between the end of the Cold War and September 11, 2001, there was little focus on exercising the national level of the Danish emergency and crisis management system. After September 11th Denmark has had two tabletop exercises, one in November 2003 and one in November 2005.[31] The 2003 exercise highlighted problems in terms of willingness and ability on part of the central actors in the national crisis management system to share knowledge and exchange classified information. It also pointed to the need for more cross-governmental coordination of communication with the press and information to the public.[32] The 2005 exercise will provide a benchmark as to whether these shortfalls have been addressed.

Tabletop exercises that cut across more government agencies and levels are crucial, particularly at times where an existing system is undergoing reform. Simulations and exercises can help identify potential seams and gaps before an emergency situation makes them apparent. Simulations and exercises also help expose potential dilemmas, giving decision makers a chance to contemplate them at more leisure than during a real incident, and thus, hopefully, help promote better thought through decisions. An intensification of this activity would appear a worthwhile investment to improve the Danish homeland security system. Moreover, live exercises, activating all levels of the homeland security system and actors from the major different agencies involved would be desirable.[33]

---

[30] Direktiv for kursus for centrale beredskabsmyndigheder, Beredskabsstyrelsen, available on http://www.brs.dk/fagomraade/tilsyn/udd/Uddannelseskatalog/direktiv_kurser/ledelse_og_organisation/landsdaekkende_totalforsvarskursus/frame.htm (Accessed on October 17, 2005); Ministry of Defence, *Regeringens redegørelse om beredskabet*, Copenhagen, June 2005, p. 12.

[31] Danish officials from the national level of Denmark's crisis management system (National Police, Police Security Intelligence Service, Ministry of Defense, Defense Command, Emergency Management Agency) also participate in the yearly NATO tabletop Crisis Management Exercise (CMX).

[32] Øvelsesledelsen, *Samlet evalueringsrapport. Krisestyringsøvelse 2003 (KRISØV 2003)*, January 2004, available on http://www.brs.dk/info/rapport/kriseoevelse2003/evauleringsrapport.pdf (Accessed October 19, 2005).

[33] Ministry of Defence, *Regeringens redegørelse om beredskabet*, Copenhagen, June 2005, p. 11.

To facilitate cross-governmental evaluation a committee—the so-called Kontaktudvalg—composed of representatives from the major actors in the emergency preparedness system has been established. The Kontaktudvalg can charge ad-hoc groups to evaluate specific incident management operations.[34] Arguably, however, systematic evaluation should be carried out by an independent committee specializing in the task instead of members of he evaluated agencies themselves.

A Culture of Cross-Governmental Cooperation

The discussion above shows, that there are remaining gaps in the structures of the emerging Danish system for civil-military cooperation in homeland security. Common planning scenarios and goals,[35] a national staff with the mandate to make tough decisions if necessary, live national exercises, and an independent evaluation system are still lacking. Yet, on other important issues, the structures appear in good shape: Areas of responsibility and lines of authority are clear when it comes to handling small and medium sized incidents—the creation of a national staff indicates at least an awareness of the existence of a gap when it comes to handling large-scale incidents; education and training is integrated to a remarkable extent; operational coordination between different agencies in local incident management seems to function seamlessly.

The relative good shape of the structures of civil-military homeland security cooperation could be seen as an expression of a high level of political attention given to the area over the past couple of years, resulting in pressure on the involved agencies to coordinate their efforts. Political decisions have begun to create some structures that put a premium on cooperation. But also, the Danish tradition for cross-governmental cooperation arguably also means, that a culture of cross-governmental cooperation already exists, as evident in, for

[34] Ibid. p. 13.

[35] The actors in Denmark's homeland security system, for example, have not jointly addressed some of the most grave possible scenarios—in what circumstances would a crisis be so grave that the military, not the civilian side would take the lead? What happens if the national headquarters disappear? Though such scenarios might seem remote, it would make good sense to at leas discuss them in order to hedge against being wholly unprepared in case of a catastrophic event.

example, the common definition of the homeland security mission proposed by representatives of all the major agencies interviewed for this chapter. Arguably, this culture has provided a firm foundation on which current efforts to enhance civil-military cooperation could build.

The Danish reform process has seen examples of cultural clashes and defensive reactions, particularly in the discussion over the National Operative Staff, resulting in a rather weak and vague mandate. Cultural differences are also evident when looking at threat perceptions and planning processes. Whereas civilian actors have been frustrated with what they perceive as an exaggerated military focus on high consequence-low probability scenarios, military actors have been frustrated with a perceived almost exclusive civilian focus on low consequence-high probability scenarios.[36]

Nevertheless, these differences have been contained. The squabbles have not derailed overall progress in enhancing civil-military cooperation in homeland security, neither do they appear to have had any negative impact on operational and practical cooperation.

Arguably, an active attempt at strengthening the existing culture of cross-governmental cooperation is key to further progress when it comes to fixing the remaining gaps in the Danish system. Historical experience indicates that it frequently takes major disasters to significantly alter threat perceptions, worldviews, and organizational cultures and habits. Yet, common education and common exercises might incrementally cause different perceptions to converge.[37]

Education of the various actors in Denmark's homeland security is already to a significant extent integrated—a factor that probably is contributing to the high level of trust between operational personnel from different authorities. Yet, in order to make the threat perceptions and different cultures converge at the central level, common education of leaders about strategic issues, with an eye to further a common understanding of threats, probabilities, priorities, and tasks could be stepped up. The current five day "Totalforsvars kursus" could be

[36] Author's interviews, Copenhagen, July 12 and 14, August 17 and 19, 2005.

[37] United States Government Accountability Office, *Department of Homeland Security. Strategic Management of Training Important for Successful Transformation*, GAO-05-888, p. 1.

expanded to a longer course with a yearly update, obligatory for key administrative and operational leaders. More frequent gaming and live exercises should further the convergence of perspectives as well.

This, in turn, would not only facilitate the task of developing common planning goals, but might also with time make all the involved actors comfortable with a national operative staff with real power, by making the actors confident that they see the problem, the tasks, and the objectives in a more or less similar manner.

In sum, culture impacts the extent to which common structures are accepted and common plans effective. Structures that compel different agencies to work together, in turn, are likely to impact culture over time and lead to a strengthening of a culture of cross-governmental cooperation. The limited scope of this case study does not permit for strong generalizations, but the Danish case indicates, that decision makers and agency leaders seeking to promote civil-military homeland security cooperation need to pay attention to both structures and culture—in particular the latter appears to have been neglected in the studies and actual policies in the area of civil-military homeland security cooperation of recent years.

Conclusion: International Implications of the Danish Experience

The new security environment is characterized by a higher level of uncertainty. A number of high consequence and low or uncertain probability threats to homelands on both sides of the Atlantic have emerged. Creating standing new civilian capabilities to deal with all high consequence-low probability threats would be prohibitively expensive. This has given rise to new demands for civil-military cooperation and for a military contribution to provide homeland security on both sides of the Atlantic.

Denmark has been particularly well placed to push for such cooperation, leveraging off from a tradition of civil-military cooperation and with a good deal of political pressure on the involved agencies to coordinate their efforts. The result is, with some remaining gaps, a system characterized by a high level of integration and coordination when it comes to education, training, and practical operational cooperation.

The Danish case indicates the importance of paying attention to both structure and culture in the effort to enhance civil-military homeland security cooperation. Proclamations of political intent and re-organization of governmental structures do not suffice. Even in a Danish context, where the tradition for cross-governmental cooperation is strong, where the military has long carried out or supported a variety of tasks at home, and where political pressure for a coordinated civil-military efforts is high, turf considerations and differences between the cultures of civilian and military agencies have made for a number of complications, particularly in regard to forging new structures for national crisis management and with regard to systematic strategic homeland security planning.

Civil and military threat perceptions and priorities are likely to diverge even more in most other countries. A targeted effort to make them converge through joint strategic level education and common exercising should thus be an imminent concern in order to ensure that new structures for civil-military cooperation do not give a false sense of security, but actually contribute to a robust and flexible protection of US and European homelands. In a world, where the boundary between internal and external security can no longer be upheld, and where a high international profile is likely to increase the risk to the homeland, such a system is not just key to domestic safety and security, but also to the ability to stay engaged in stabilization and reconstruction missions abroad.

Chapter 7

The EU's Approach to Homeland Security: Balancing Safety and European Ideals

Gustav Lindstrom

The concept of homeland security is relatively new at the EU level.[1] For many, the phrase "homeland" resonates most strongly at the country level. In fact, many European policymakers prefer to use terms such as internal security, civil protection, or collaborative security when referring to intra-EU security issues. Yet despite varying expressions, there is a growing realization that pan-European homeland security is increasingly important, especially in light of changes in the security environment which blur the lines between internal and external threats and highlight the importance of cross-border cooperation.

This chapter analyses the EU's approach to homeland security and its likely evolution over the next few years. It places particular emphasis on the EU's efforts to strike a balance between internal security requirements, especially in the field of anti-terrorism, and adequate levels of civil liberties.

The EU Approach to Homeland Security

As a supranational organization, the EU's approach to homeland security is fairly unique. Four key observations can be made. First, the EU does not function as a "first responder" in the traditional sense. Rather, it focuses on complementing security policies that exist among individual member states in ways that are consistent with the principle of subsidiarity.[2] As such, the bulk of EU contributions take the form of

[1] Specifically when referring to peacetime. It should be acknowledged that several EU member states have quasi-military forces to maintain internal security.

[2] According to the subsidiarity principle, the EU should not legislate when the objective can be better achieved at a more decentralized (local) level.

initiatives to enhance cross-border cooperation (e.g. in the field of anti-terrorism), coordination support, information sharing, and collaboration with national and international partners.

Second, the EU's approach to homeland security is not centralized in a single agency or institution. Instead, several institutions across the EU's three pillars address homeland security objectives.[3] Principal among them are the European Commission (hereafter Commission) and the Council of the European Union (hereafter Council). Examples of activities range from Commission efforts to improve critical infrastructure protection across the EU to the Council's establishment of a Counter-Terrorism Coordinator to facilitate policy coordination in the fight against terrorism.

While the Commission and the Council are the principal policy actors at the EU-level, there are also a host of EU agencies that play a role in homeland security. One example is the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX/AMOCEB). Established in October 2004 and based in Warsaw, one of its principal tasks is to coordinate the activities of national border guards at the EU's external borders. Relating to homeland security, it will "follow up on the development of research relevant for the control and surveillance of external borders"—effectively giving it a role in how individuals enter into the Schengen area.[4]

A third characteristic of the EU's approach to homeland security is that it evolves both gradually and sporadically. It is gradual in the sense that independent policy initiatives in areas such as transportation, health, and law enforcement have progressively come to form the core of a nascent EU's approach to homeland secu-

[3] Pillar one is the "Community domain" and covers areas such as transport, trade, economic and monetary affairs. Decisions in the first pillar are taken through the Community method involving the Commission, Parliament and the Council. Pillar two consists of the Common Foreign and Security Policy (CFSP). Pillar three addresses co-operation in police matters, criminal law, asylum, migration and judicial co-operation in civil matters. The Council decides and implements policies in pillars two and three with member States and the Commission entitled to submit proposals.

[4] European Commission, "Basic facts about the External Borders Agency," MEMO/05/230, Brussels, 30 June 2005, p. 1.

rity.[5] The approach is sporadic in the sense that these policy developments often occur in response to large-scale events affecting internal security such as the Madrid terrorist attacks in March 2004 and the July 2005 bombings in London. Not surprisingly, in the absence of a unifying strategy, the EU approach is functional and reactive in nature, especially as many policies have been taken independently from one another. Moreover, key decisions have been transposed into national law at different rates across member states, affecting the coherence and effectiveness of policies at the EU level. For example, the EU arrest warrant (EAW), adopted in June 2002, became applicable across the EU-25 only in April 2005 when Italy adopted the EAW.[6] Finally, EU member states themselves have enacted policies that provide different degrees of protection, resulting in varying levels of security across Europe. Over time, however, these policies are being fine-tuned so they can work more efficiently.

Fourth, a substantial proportion of the EU's homeland security activities focus on the fight against terrorism. The prominence of anti-terrorism initiatives is linked to the attacks in New York/Washington D.C., Madrid, and London, and to the reactive nature of the policy development process. In the aftermath of each of these attacks, the EU stepped up its anti-terrorist activities to boost security across Europe. The focus on terrorism is also partly attributable to overall societal concern. According to the most recent *Transatlantic Trends* survey, 95 percent of those surveyed across nine EU member states viewed terrorism as an "extremely important" or "important" threat over the next ten years. The finding is consistent with a similar result from 2004 (96 percent).[7] Given the EU's strong focus on anti-terrorism, both at the EU and member state levels, the next section briefly summarizes recent steps taken in this area.

---

[5] For an overview of EU activities, see Gustav Lindstrom, "Protecting the European Homeland: The CBR dimension," Chaillot Paper n° 69, (Paris: EU Institute for Security Studies, July 2004). For additional background information see "Securing the European homeland: The EU, terrorism and homeland security," Bertelsmann Stiftung (ed.), Gütersloh, August 2005.

[6] The European Arrest Warrant facilitates extraditions of suspects one member state to another.

[7] The nine countries are Germany, France, Italy, Netherlands, Poland, Portugal, Spain, Slovakia, and the United Kingdom. Interviews were carried out between May 30 and June 17 2005. The sample size was approximately 1,000 for each country. "Transatlantic Trends 2005," Topline Data 2005. German Marshall Fund of the United States and the Compagnia di San Paolo, 2005.

Initiatives Since 9/11[8]

The September 11th attacks in the United States caught the attention of policy makers worldwide. For Europe, these attacks signaled the emergence of a new threat and highlighted the importance of cross-border cooperation. As a result, several measures were introduced in the EU following the 9/11 attacks. These were packaged into a Plan of Action to Combat Terrorism.[9] Beyond practical actions to enhance security in the field of transportation, a set of policies were introduced to enhance collaboration within the judicial, law enforcement, and financial sectors. Well-known initiatives include the Framework decision on the European arrest warrant and the Framework decision on setting up joint investigation teams.[10] To facilitate intra-European judicial cooperation with respect to serious cross-border crime, the EU established EUROJUST. To strengthen collaboration across the Atlantic, several agreements were sealed with the United States, including the EU-US agreements on mutual legal assistance and on extradition.

The March 2004 attacks in Madrid signaled that Europe is not immune to these new threats. These attacks "hit home" for many Europeans, prompting the creation and implementation of additional anti-terrorism measures. Importantly, a Declaration on Combating Terrorism was unveiled at the March 25-26, 2004, European Council meeting. Among other things, it laid the groundwork for an enhanced intelligence capability within the Council Secretariat, the adoption of a solidarity clause, and the set-up of exchanges of information on con-

---

[8] Gustav Gustenau covers this area in greater detail in Chapter 4.

[9] Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001. Available at ue.eu.int/ueDocs/cms_Data/ docs/pressData/en/ec/140.en.pdf. See also the "'Road Map' of all the Measures and Initiatives to be Implemented under the Action Plan Decided on by the European Council on 21 September 2001" Accessible in "From Nice to Laeken—European defence: core documents," Chaillot Papers n°51, (Paris: EU Institute for Security Studies, April 2002).

[10] "A framework decision is an instrument that is used to approximate (align) the laws and regulations of the Member States. Proposals are made on the initiative of the Commission or a Member State and they have to be adopted unanimously. They are binding on the Member States as to the result to be achieved but leave the choice of form and methods to the national authorities." Definition from the web site on the European Convention, accessed November 2005 at http://european-convention.eu.int/glossary.asp?lang=EN&content=F.

victions for terrorist offences.[11] In addition, it called for the rapid implementation of initiatives introduced under the September 2001 Plan of Action to Combat Terrorism.

As a follow-on, the European Council endorsed the Hague Programme in November 2004. It contains numerous proposals for augmenting judicial and law enforcement cooperation over the next five years. Responding to the priorities identified in the Hague Programme, the European Commission launched its five-year action plan for Freedom, Justice, and Security in May 2005. Among its ten priority areas are measures to enhance the EU's capacity to fight terrorism while striking a balance between privacy and security.[12]

A flurry of policy activity also followed in the aftermath of the London bombings in July 2005. Less than two weeks after the bombings, the Commission issued a Communication on ensuring greater security of explosives detonators, bomb-making equipment and firearms.[13] A few months later, the Commission offered a comprehensive package in the fight against terrorism. The package includes four initiatives, among them a proposal for a directive on the retention of communications traffic data, a €7 million pilot project in the field of prevention, preparedness and response to terrorist attacks, and a Communication addressing radicalization and recruitment of terrorists (September 2005).[14]

---

[11] See "Declaration on Combating Terrorism," Council of the European Union, doc. 7906/04, Brussels, 29 March 2004. For the Revised Action Plan on Terrorism (updated June 2005), see "Commission Staff Working Document: Revised Action Plan on Terrorism," European Commission, SEC(2005) 841, Brussels, 17 June 2005. See also the Communication from the Commission to the Council and the European Parliament on "Prevention, preparedness and response to terrorist attacks," European Commission, COM(2004) 698 Final, Brussels, 20 November 2004.

[12] For more information, see: http://europa.eu.int/comm/justice_home/news/information_dossiers/the_hague_priorities/index_en.htm

[13] European Commission document COM(2005) 329 Final, Brussels 18 July 2005.

[14] "Commission presents comprehensive Counterterrorism package," European Commission IP/05/1166, Brussels, 21 September 2005. "Commission allots 7 Mio€ for a 'pilot project' in the field of prevention, preparedness and response to terrorist attacks," European Commission MEMO/05/330, Brussels, 21 September 2005. "Commission proposes rules on communication data retention which are both effective for law enforcement and respectful of rights and business interests," European Commission, IP/05/1167, Brussels, 21 September 2005. "The Council of Europe new Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism (#198), European Commission, MEMO/05/331, Brussels, 21 September 2005. "Terrorist recruitment: a Commission's Communication addressing the factors contributing to violent radicalisation," European Commission, MEMO/05/329, Brussels, 21 September 2005.

The four initiatives contained in the Commission package tackle different dimensions of terrorism. The initiative on the retention of communications traffic data aims to facilitate the investigation of serious crimes and terrorism. It represents a modified version of the draft framework decision presented by five EU member states in April 2004 (described in greater detail later on).[15] The €7 million pilot project initiative concentrates on critical infrastructure protection. About 77 percent or €5.4 million of the funds will be allocated towards the future European Programme for Critical Infrastructure Protection and the development of consequence management capabilities for events with cross-border implications.

To confront the financing of terrorism, the third initiative proposes that the Commission be authorized to negotiate on behalf of the Community vis-à-vis specific parts of the Council of Europe's Convention on "Laundering Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism."[16] Finally, the fourth initiative, in the form of a Communication, proposes measures to limit the potential for violent radicalization. Among other things, it calls for the establishment of a network of European experts to explore means for decreasing the potential for terrorist recruitment in Europe.[17]

Policy actions in the wake of the July bombings have not been restricted to EU policymakers alone. Members states are also considering various actions, most of which concentrate on boosting domestic surveillance. For example:

---

[15] See "Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism," Council of the European Union, doc. 8958/04, Brussels, 28 April 2004.

[16] Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm

[17] While these initiatives have the potential to curb some terrorist activity, it must be stressed that they in many ways can be circumvented. The fact that terrorists rely on simple, asymmetrical means to avoid and respond to anti-terrorism measures introduced by decision-makers serves to limit their effectiveness—especially in the long-run. For example, tracking and monitor financial activities can be very difficult if only small sums of money are involved. To illustrate the point, the Madrid attacks are estimated to have cost approximately $10,000, an amount that could have been transferred in small sums. See "First report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al Qaeda and the Taliban and associated individuals and entities," United Nations Security Council, S/2004/679, New York, August 25, 2004.

- In France, the Interior Ministry is considering ways to heighten internal surveillance. This includes video surveillance in public spaces, for example in buses, and the collection of communications data.[18] The target date for adoption of these and other initiatives is December 2005.

- In Germany, policymakers are considering whether to increase surveillance in public areas such as subway stations.

- The UK unveiled a 12-point plan in the wake of the London attacks to strengthen the capability of immigration and criminal justice systems to fight terrorism.[19] Among others, there are provisions for facilitating the deportation and expulsion of individuals fostering hatred or advocating violence; the refusal of asylum to anyone who has participated or had anything to do with terrorism; and making it an offence to glorify terrorism. Another element is the possibility of extending the period a suspect can be held without charges from 14 to 90 days.[20]

- In Italy, the senate approved a new anti-terror plan on July 22, 2005. Among its provisions are speedier deportations of foreign national suspected of terrorism, closer surveillance of Internet and telephone traffic, and doubling of the time suspects can remain in custody without charges to 24 hours.[21] The Parliament's lower house needs to pass the bill before it can become law.

- Spain is considering steps to make it mandatory for customers buying pre-paid mobile phone cards to show proof of identity.

---

[18] "Europe and Terrorism: the French Lesson," *The Economist*, August 13, 2005, p. 25-26.

[19] For an independent review, see the report by Lord Carlile of Berriew, "Proposals by Her Majesty's Government for changes to the laws against terrorism," accessible at: http://security.homeoffice.gov.uk/news-and-publications1/publication-search/independent-reviews/carlile-review-121005?view=Standard&pubID=241429

[20] This provision was defeated on November 9, 2005, in the House of Commons. The House of Commons passed an alternate proposal calling for a maximum detention period of 28 days.

[21] Elisabeth Rosenthal, "An Italian proposes new rules on security," *The International Herald Tribune*, 13 July 2005. Accessed October 2005 at http://www.iht.com/articles/2005/07/13/europe/web.italy.php

In addition to a strong interest in expanding surveillance, there is growing focus on the potential for expelling foreign nationals associated with terrorist activities. Such proposals are controversial, especially if the criteria for deportations are not clear. For example, certain opposition parties and civil liberties groups in the UK have criticized the government's 12-point plan against terrorism for being too vague with certain key formulations relating to the criteria for expulsions.[22] As a result, some elements of the initial proposals have been modified. In a revised version, additional evidence is required before a charge can be leveled against individuals suspected of glorifying terrorism.[23]

The Interplay Between Safety and European Ideals

With the latest round of policy initiates in motion, there is growing concern over the balance between safety and civil liberties in Europe. Since its inception, the EU (and formerly the European Community) has placed strong emphasis on individual freedoms and rights. The establishment of the "four freedoms" (freedom of movement of people, goods, services and capital) is generally considered to be a cornerstone of the EU. The importance of the free movement of people was highlighted further with the introduction of the Schengen Convention into the EU umbrella at the 1997 EU Summit in Amsterdam (which came into force on May 1, 1999). It opened the door for passport-free travel across the EU member states that accepted its measures.[24]

With respect to fundamental rights, EU decision makers announced the Charter of Fundamental Rights of the European Union at the Nice Summit of December 2000. It brought together all personal, civil, political, economic and social rights into a single text.[25] Aiming to consolidate this text at the EU level, the Charter of Fundamental Rights was integrated into the now defunct (at least in its current form) Treaty

[22] "Clarke waters down anti-terror law," *The Guardian*, October 6, 2005. Accessed October 2005 at http://www.guardian.co.uk/uklatest/story/0,1271,-5325869,00.html.

[23] To view the version as of October 11, 2005, see http://www.publications.parliament.uk/pa/cm200506/cmbills/055/2006055.htm

[24] Member states participating in Schengen are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, the Netherlands, Luxembourg, Portugal, Spain, and Sweden. Two countries outside the EU, Norway and Iceland, also participate in Schengen.

[25] Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1, Brussels, 18 December 2000.

establishing a Constitution for Europe.[26] Collectively, these and other efforts aiming to guarantee robust individual freedoms and rights are consistent with European values and ideals.

However, with several waves of terrorist attacks inside and outside Europe in recent years, individual freedoms and rights are being reviewed. Notable areas affected include the privacy of communications and the openness of borders. Among the measures that are most likely to draw the attention of individuals concerned with the loss of fundamental rights are:

- Data retention proposals concerning the maintenance of internet and phone records for a specified amount of time within the EU;
- Provisions for the inclusion of biometric data into EU passports;[27]
- The gradual introduction of the 2nd generation Schengen Information System (SIS II) by 2006 which will facilitate the exchange of data on certain categories of persons and property;[28]
- A continued EU-US agreement on the transfer of passenger name record (PNR) data of airline travelers entering the United States; and,
- Initiatives to facilitate the banning and expulsion of certain individuals within the EU

The case of data retention

The issue of data retention provides a good illustration of the inherent tension associated with balancing security requirements and civil liberties. In the wake of the Madrid terrorist attacks, France,

[26] The Constitution was rejected in national referendums in France and Holland at the end of the first semester of 2005. The text of the Charter is accessible at http://europa.eu.int/comm/justice_home/unit/charte/index_en.html. For more on fundamental rights within the EU see http://europa.eu.int/eur-lex/en/about/abc/abc_10.html

[27] See "Council Regulation on standards for security features and biometrics in passports and travel documents issued by member states," Council of the European Union, Doc. 15152/04. Brussels, 10 December 2004.

[28] For more on the system see http://europa.eu.int/scadplus/leg/en/lvb/l33183.htm

Ireland, Sweden, and the UK proposed a draft Framework Decision (draft FD) on data retention. It called for the collection and retention of "traffic data" originating from electronic communication networks and services.[29] According to the draft FD, records could be held up to three years. If approved, member states would have to comply with the draft FD by January 2007.[30]

From the start, the draft FD stood on shaky legal grounds since the harmonization of communication policies at the EU level falls under the competency of the Community (i.e., the Commission). In spite of this limitation, the draft FD moved forward only to be voted down by the European Parliament on May 26, 2005, during the consultation procedure. Even after modifications, the European Parliament rejected the draft FD a second time on June 7, 2005. The rejections were not surprising. The European Parliament had demonstrated strong support for privacy protections earlier when the Commission was negotiating the passenger name record (PNR) agreement with the United States in the aftermath of the 9/11 attacks. The European Parliament may have galvanized its position further when the Commission and the Council approved the PNR agreement in spite of its repeated objections.[31]

Nonetheless, the momentum for data retention has continued. On September 21, 2005, the Commission presented its own data retention proposal. Unlike the Council draft FD, the Commission proposal calls for shorter retention periods: a year for fixed and mobile telephony data and six months for IP-based communications data. Given that the proposal will go through the "co-decision" procedure—giving the European Parliament a greater say in shaping the proposal—members of the European Parliament and the European Commission are looking to reach a compromise on the final version of the text by

[29] Traffic data refers to information such as the location of the caller, time of the call, duration of the call, and number dialed.

[30] As of 2004, a majority of EU member states (15) do not have mandatory data retention obligations. In half of those with data retention schemes, data retention is not operational since implementing measures are still missing. "Data Retention Directive," European Commission, MEMO/05/328, Brussels 21 September 2005.

[31] It should be noted that the European Parliament has brought a legal case against the PNR agreement that was heard by the Court of Justice in mid-October 2005. Its outcome, although unlikely to come out in the next year, may very well give an indication of how such data will be handled in the future.

the end of 2005. According to the Commission, the proposal is consistent with Community law and the Charter on Fundamental Rights, justified by Article 52 of the Charter.[32]

Still, it remains to be seen whether data plans can go forward under their current formulation. Mr. Peter Hustinx, the European Data Protection Supervisor, has highlighted several areas that require further clarification. Among them are:

- Consistency with article eight of the Charter of Fundamental Rights of the European Union, which maintains that "everyone has the right to the protection of personal data concerning him or her," raising the issue of proportionality.[33]

- Consistency with Directive 2002/58/EC of the European Parliament and of Council stipulating that traffic data must be erased as soon as storage is no longer needed for purposes related to the communication itself.[34]

- Consistency with case law of the European Court of Human Rights. According to Mr. Hustinx, the Dudgeon case lays down that "justifications for interference should outweigh the detrimental effect that the very existence of the legislative provisions in question could have on subjects."[35]

There are also societal concerns over the data retention schemes. For example, as of early October 2005, about 50,000 EU citizens had

---

[32] "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others." Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1, Brussels, 18 December 2000, p. 21.

[33] (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority. Ibid, p. 10.

[34] Available at europa.eu.int/eur-lex/pri/en/ oj/dat/2002/l_201/l_20120020731en00370047.pdf

[35] Opinion of the European Data Protection Supervisor, 26 September 2005, p. 3. Available at http://www.edps.eu.int/12_en_opinions.htm,

signed an on-line petition against data retention.[36] On October 19, 2005, a European Civil Liberties Network was launched. Consisting of civil rights organizations across Europe, its main aim is to defend civil liberties and raise awareness among Europeans concerning the potential ramifications arising from proposed anti-terrorist legislation.[37]

Balancing homeland security and civil liberties

Obtaining a balance between homeland security and individuals' rights is difficult. It calls for a calculation of both the benefits of different policy measures and their costs. Regarding benefits, it is particularly difficult to quantify the number of lives that can be saved or the amount of damage that could be averted through different homeland security policies. The fact that homeland security breaches tend to be low probability, high impact events, further complicates the picture.

It is also critical to assess whether or not proposed measures target the right people or groups (those who threaten the European homeland) and deter the intended crimes. If it turns out that a particular security initiative has a strong impact on curbing petty crime but has no impact on securing the homeland that must be taken into account when assessing whether or not potential benefits outweigh the costs. It is also important to assess how measures contribute to homeland security. For example, if additional surveillance can help piece together an attack after the fact but not prevent it, how should we estimate its value?

Turning to costs, both monetary and non-monetary costs need to be taken into account. There are the monetary costs associated with the implementation of policies or the effects of a security breach, but there are also costs associated with the loss of freedoms which are harder to value.[38] Costs streams may rise unexpectedly, especially if those intent on attacking the European homeland adjust their methods to circumvent existing policies. There may be spillover effects,

[36] http://www.dataretentionisnosolution.com/

[37] For more see http://www.ecln.org/

[38] For example with respect to data retention, it has been estimated that for a large network provider costs might increase by an additional €150 million to maintain data for a 12-month period. Opinion of the European Data Protection Supervisor, 26 September 2005. Available at http://www.edps.eu.int/12_en_opinions.htm, p. 13.

especially if the attack is unconventional in nature. For example, an attack on information systems can affect a variety of industries that rely on such systems for their daily work. Since costs and benefits can occur in the future, consideration must be given to how far forward costs and benefits need to be projected.[39] While challenging, consideration of both benefits and costs is critical when deciding among policy alternatives that aim to enhance security.

Likely Developments in EU Homeland Security

Given the delicate balance between the implementation of policies that aim to protect citizens across Europe and the need to guarantee fundamental freedoms to the greatest extent possible, what are some likely scenarios for the development of EU homeland security in the coming years?

A likely scenario is that certain EU member states or clusters of member states will move ahead and deepen their security collaboration either bilaterally or multilaterally—especially in the area of anti-terrorism. Under such a scheme, member states that share borders or specific concerns would move ahead with specific security enhancing projects without having to engage other EU member states. Carrying out such collaboration outside the EU framework would provide participants with greater levels of flexibility concerning the modes of cooperation. Over time, such agreements could be fine-tuned to demonstrate their value added to non-participating EU member states, opening the door for their incorporation into the EU framework (such as the Schengen Convention).

One route to incorporating such agreements at the EU level would be through EU intergovernmental conferences. Other options exist as well. For example, an agreement or treaty may be made open for membership to other EU member states should they desire to join and meet any applicable requirements. With the addition of new member states, such initiatives may attain a critical mass that facilitates incorporation into the EU framework. Specifically, with eight or more member states

[39] Gustav Lindstrom, "The Fight Against Terrorism and Civil Liberties: A Zero Sum Game?," in "Les Dossiers de L'Abécédaire Parlementaire," Assembly of Western European Union, Paris, 2nd Trimester 2004, pp. 19-22.

partaking in an agreement, it can be brought to the EU as an area of reinforced cooperation. Alternatively, certain aspects of an agreement or treaty may serve as a useful basis for work at the EU-level, be it to inform upcoming Commission legislative proposals or highlight areas that may require future attention by the EU.[40]

To a certain degree, this scenario is already underway. For example since 2003, the G5 countries (France, Germany, Italy, Spain, and the UK) have held periodic meetings at the level of interior ministers to discuss issues such as illegal immigration, border controls, and organized crime. At their latest meeting held on July 4-5, 2005, the G5 interior ministers agreed to adopt several policy directions. Among them are the establishment of "an exchange mechanism on genetic traces and fingerprints" and setting "up control and registration mechanisms not just for entry but also for exit from their territory."[41]

A second cluster of EU member states (Austria, Belgium, France, Germany, Luxembourg, Netherlands, and Spain) signed a convention in Prüm on 27 May 2005 boosting the prospects for cross-border cooperation.[42] Among its provisions is the establishment of national DNA analysis files, the option of deploying air marshals, and the introduction of joint patrols to enhance police cooperation.[43] The Prüm Treaty signatories have signaled that within three years of its entry into force, an initiative will be presented to incorporate the provisions of the Convention "into the legal framework of the European Union."[44]

With respect to instruments, the EU is likely to continue fine-tuning its homeland security initiatives. A greater focus on the link between internal and external security may result in closer cooperation between Commission and Council instruments—despite the cur-

[40] See for example "'New ideas' on Counter-Terrorism from the July JHA Council: Next steps." Council of the European Union, document 11910/05, Brussels, 2 September 2005.

[41] G5 Operational Conclusions, available at http://www.interieur.gouv.fr/rubriques/c/c2_le_ministere/c21_actualite/2005_07_05_g5/Draft_conclusions.DOC, p. 1 and p. 4.

[42] Prüm Convention, Council of the European Council, doc. 10900/05, Brussels, 7 July 2005.

[43] Prüm Convention, Council of the European Council, doc. 10900/05, Brussels, 7 July 2005.

[44] Ibid, p. 4.

rent status of the Draft Treaty establishing a Constitution for Europe. With respect to the link between internal and external security, the European Council endorsed a "Conceptual Framework on the ESDP dimension of the fight against terrorism in December 2004."[45] Among others things, it identifies potential areas for action concerning prevention, protection, consequence management, and support to third countries in the fight against terrorism. The EU Solidarity Programme, geared to deal with chemical, biological, radiological, or nuclear (CBRN) events, is likewise evolving. It currently represents a widened and revised version of the 2002 CBRN Programme introduced jointly by the Council and Commission. The majority of its new elements were presented at the 25 March European Council and the 17-18 June 2004 European Council. Among its six strategic goals are: strengthening risk assessment and analysis of terrorist threats and choice of targets; improving detection, identification, and alert mechanisms (e.g. through the introduction of ARGUS, a secure general rapid alert system); and boosting preventative measures (e.g. by strengthening and enhancing intelligence and judicial capacities).[46]

Another important development is EU investments in security enhancing technologies. In March 2003, the Commission launched the Preparatory Action in the field of Security Research (PASR) to fund security related research projects. Among projects currently funded are initiatives to improve the protection of rail passengers, enhancing safety at European harbors, and protecting airliners against man portable air defense systems.[47] The initial funding cycle of €65 million spanning three years will eventually give way to a fully fledged European Security Research Programme, likely to be funded at the order of €500 million per year starting in 2007 as part of the Seventh EU Framework Programme.

---

[45] Council of the European Union, doc. 14797/04, Brussels, 18 November 2004. ESDP stands for European Security and Defence Policy.

[46] For more information, see "EU Solidarity Programme on the consequences of terrorist threats and attacks", Council of the European Union, doc. 15480/04, Brussels, 1 December 2004.

[47] For a fuller description, see "13 new security research projects to combat terrorism", European Commission MEMO/05/277, Brussels, 2 August 2005.

Conclusion

In the end, protecting the European homeland, combating terrorism, and ensuring civil liberties require careful calibration. Recognizing that one hundred percent security at all times is not feasible, policymakers need to weigh the costs, benefits, and consequences of enacted policies. Achieving success in these areas requires walking a fine line, especially when implementing policies that impact civil liberties. Fortunately, protecting the homeland and ensuring civil liberties need not be a zero-sum game. There are a variety of alternatives that policymakers can consider.

First, with respect to data retention, most individuals accept that some personal data may need to be collected to fight terrorism effectively. Nonetheless, how personal data is collected, used, and stored can vary. Some approaches protect civil liberties more than others. Individuals are more likely to sacrifice certain rights if they understand the necessity and implications. Failure to inform the public in advance of what data will be collected, when, how, and from where can produce a backlash. Thus, transparency is a key ingredient for successful policy implementation.

In many instances, citizens are concerned that data will be retained unnecessarily. To minimize such concerns, personal data should be retained only when warranted, for the shortest timeframe possible, and permanently destroyed when no longer needed. In other cases, concerns stem from the perception that databases will be increasingly cross-linked to facilitate the tracking of suspected terrorists. While combining databases can prove useful, it is important to resist the temptation to link databases that provide limited added value in the fight against terrorism.[48] To limit societal concern, databases with information unlikely to yield results in the fight against terrorism should remain detached.[49]

[48] An example might be the potential inclusion of databases containing medical information. While an unlikely development, the fact that the perception exists is enough to cause societal concern over eventual data sharing with interested outsiders such as insurance groups.

[49] For a more detailed discussion on databases and anti-terrorism see Lindstrom, "The Fight Against Terrorism and Civil Liberties: A Zero Sum Game?," in "Les Dossiers de L'Abécédaire Parlementaire," Assembly of Western European Union, Paris, 2nd Trimester 2004.

Second, the use of sunset clauses allows policymakers to act swiftly and to be responsive in the short-term, while ensuring that that only properly formulated, effective policies endure over the long-term. Attaching an "expiration date" to legislation makes it easier for policymakers to discard measures that prove ineffective or overly burdensome on civil liberties. [50]

Ultimately, however, homeland security is about more than surveillance and data retention. While concerns surface quickly in these areas, issues of civil rights, privacy, and legal protection extend to other policies as well. Looking forward, initiatives involving handfuls of member states may prove to be useful test beds for the creation of EU level homeland security policies. Policymakers should pay careful attention to what provokes social and legal debate, and to what works, and to what doesn't work—both at the EU level and among member states—with the overarching goal of providing a coherent homeland security framework that protects both Europe and its ideals.

Over the long-term, policymakers should strive to formulate an EU strategy on homeland security that streamlines measures currently distributed across different policy domains. In addition to harmonizing existing measures and instruments, it would provide policymakers with a reference for future decisions, and allow them to identify which areas need to be prioritized and which types of resources are required to achieve key goals.[51]

[50] Anja Dalgaard-Nielsen, "Civil Liberties and Counter-Terrorism: A European Point of View," Center for Transatlantic Relations, School of Advanced International Studies, The Johns Hopkins University, Washington, D.C., 2004.

[51] For additional recommendations see Lindstrom, "Protecting the European Homeland: The CBR dimension," pp. 66-73.

Connecting Key Capabilities

Chapter 8

Defending Critical Infrastructure and Systems

Sandra J. Bell

The Oxford English Dictionary[1] entry for "*defend*" is "*resist an attack on; protect from harm or danger*" which implies there is a chance of danger or loss to whatever needs defending. Such a chance is more commonly described as "*risk*" and there are many conceptual frameworks for understanding risk, at the core of of which are three basic elements:

- A driver for action which is more commonly known as the "*threat*,"
- A deficiency in a plan that allows deviation often known as a "*vulnerability*"
- A danger or loss known as a "*consequence.*"

In the case of a nation's critical infrastructure the risks are manifold ranging from man-made risks such as terrorism and natural disasters such as severe weather, hurricanes and flooding. Most nations do not have a bottomless pit of money and resources with which to ensure that their infrastructure is completely is robust and therefore must prioritize protective action based on an understanding of the probability of an event occurring together with the consequences. Therefor, nations need to be able to carry out comprehensive threat assessments, assess the vulnerabilities of specific infrastructure elements, assets or sites and be able to quantify the downstream consequences of the losses of infrastructure elements. Only then can they decide where best to place effort to achieve maximum effect.

Such analysis sounds straightforward however, is very difficult to

[1] Oxford English Dictionary

achieve in practice for a number of reasons including:

- National security, economic prosperity and national well-being are dependent on a set of highly interdependent critical infrastructures.
- The ownership of the critical infrastructure of many nations rests with trans-national companies within the private sector.
- The data that is essential to enable such analysis rests within both the public and private sectors and there are significant barriers to the sharing of such information.
- The extreme events that are likely to cause the severest consequences and therefore warrant priority treatment are thankfully rare meaning that historical evidence is frequently too scant to be useful.

This paper will look at practical examples to support threat, vulnerability and consequence analysis and make recommendations for future improvements.

Threat Analysis

Emergencies and disasters are newsworthy events and because they often have a highly visual impact they frequently receive disproportionate media attention. Additionally, the 24/7 nature of the media means that often a running commentary is provided for many disasters and emergencies which concentrates attention on the immediate consequences rather than the longer term downstream cost. This leads to a skewed perception of risk where the rarest events are often deemed the most probable and those with harsh immediate impact deemed the most severe.

Perhaps the area where such a skewed perception is likely to have the worst consequences is in the area of critical infrastructure. Failures in the infrastructure are likely to have a wide reaching effect on the public but, at an individual level, the public have very little control of the defence of such systems. People generally have less appetite for risks over which they have little or no control.[2] Coupled with this is the fact the people frequently look to their elected government to take

[2] Adams, John. "Risk assessment: Placing terror threats in context." Royal United Services Institute, *Jane's Homeland Security and Resilience Monitor*, October 2005, Vol. 4, No. 6.

the lead in the defence of such systems. Therefore there is a risk that decisions regarding defence of critical infrastructure are politicized and effort is expended on highly visual protection from the most rare events at the expense of long term investment in the reslience of aging infrastructure. It therefore very important that risks are set in context and that not just the short term impact is considered when prioritizing security investment. An understanding of the threats faced and their probability of occurrence is at the heart of understanding the risks that need addressed.

As covered in a previous chapter, throughout the world there are many individuals and organisations with a wide and varied spectrum of motivations and aims. There are organisations and individuals with single issue grievances such as the stopping in-vivo drug testing to those that aspire to the dismantling of the democracy of the whole of the Western world. This means that the nature of the threat (objective, target and method of attack) is also wide and varied and, as many of the individuals and organisations involved either cannot or will not negotiate or have grievances and aims that are fundamentally at odds with the fabric of democracy, many nations are, and will be for the foreseeable future, at risk from man-made threats.

Man-made threats

Although the motivations and ultimate aims of those wishing to cause harm are wide and varied and defy ready classification the objectives of the man-made threats generally fall into five broad categories, which in turn indicate likely targets and methods of attacks. These five categories are frequently sequential and are: Capturing Attention, Obtaining Acknowledgement of Existence, Securing Recognition of the Cause, Establishing Authority and finally Governance. Although nations will simultaneously face threats from organisations and individuals at all stages of objective, at any one time there will generally be a dominant threat and therefore a certain type of act with a higher probability of occurrence. Knowing the dominant threat and associated objective allows nations to ascertain which acts are most probable and therefore where best to place protective measures. There are many ways of doing this and an example from the UK is discussed below:

Example 1: The 21st Century threat of terrorism in the UK

In December 2000 and January 2001, as part of a study into virtual war gaming, Defence Evaluation and Research Agency (DERA), Director of Force Development (DfD) and the Joint Doctrine and Concepts Centre (JDCC) questioned several hundred defence and security experts at all levels throughout their organisations and asked them to predict future high impact low probability events.[3] After the ideas about little green men from outer space and those ideas that defied the laws of physics had been removed, a dataset of 83 ideas relating to man-made threats remained.

To determine the dominant threat the ideas were categorized as a function of objective, target and method of attack. (See Figures 1, 2 and 3). The five objectives are described below and the categories for method of attack and target are self-explanatory.

1. *Attention:* The objective at this stage is not at all sophisticated—all that is needed is to capture attention for as long as possible with the relevant audience for as long as possible. There is often no attempt to advertize what the political aim is and it is not uncommon for several terrorist groups to either claim responsibility for events or encourage the assumption that they were somehow implicated. Single issue or domestic terrorist groups frequently require only to grab the attention of a small community of decision makers or government officials but, as the political aims of International Terrorism include the dismantling of the whole western democracy, then the audience in this case is the whole world. Shocks and surprises are frequently the best way to grab attention in normal life and terror acts designed to grab attention also use these tactics. Signatures of this type of act include: events perpetrated without warning, breaching of social norms in terms of method of attack and target, unsophisticated methods of attack, and indiscriminate mass lethality.

2. *Acknowledgement:* Events designed to obtain acknowledgement of existence are frequently designed to sow seeds of doubt about the governing body. These types of events tend to be aimed at audiences who might have sympathy with the political aims of

[3] S. J. Bell, "*High Impact Low Probability Events*" Future Issues for Defence Conference, Defence Academy Shrivenham, February 26, 2001.

the terrorists and targets will often be those in power or the system of power. As the objective is to start to gain sympathy for the cause the targets are likely to be constrained rather than indiscriminate, there are likely to be warnings and the methods need to be sophisticated enough to reach the right target and be able to issue a warning.

3. *Recognition*: The objective here is a "show of power." Again, shock and surprise are the main tactics but the target is often iconic rather than indiscriminate. The aim is to show that this is a force to be taken seriously. With respect to single issue or domestic threats, targets are often politicians or heads of industry and murder and kidnap are common but with International Terrorism the audience is again, the world and events such as 9/11 typify an International Terrorism "show of power" event.
4. *Authority*: Here the objective is to capture a niche or minority following that adds legitimacy to the political aim. Propaganda and blackmail are established tactics together with the manipulation of vulnerable or disenfranchised groups. With respect to International Terrorism, this activity is on a much larger scale and includes taking advantage of entire failing states and countries for political gain.
5. *Governance*: The ultimate objective is the fulfilling of the political aim. Ideally, terrorist groups will have achieved sufficient political legitimacy so that they do not have to carry out an illegal act of terror to achieve their ultimate aim. However, this is not always the case and assassinations of leaders and coups are common to achieve this objective.

Figure 1 indicates that the dominant threat is from events designed to obtain acknowledgement of existence. The aim is to sow seeds of doubt and start to recruit minority sympathy. Such an objective seeks to reach as many people as possible and therefore indicated that the critical infrastructure may not necessarily be a target in itself but that, as it is a means to affect many people, could be used as a platform or vehicle. Figure 2 confirms this hypothesis indicating that indiscriminate attacks on large numbers of the people causing mass fatalities was considered most likely, and critical infrastructure such as public transport systems were a favorite attack platform, whereas attacks on the critical infrastructure in their own right scored relatively low.

Figure 1. Idea count as a function of objective

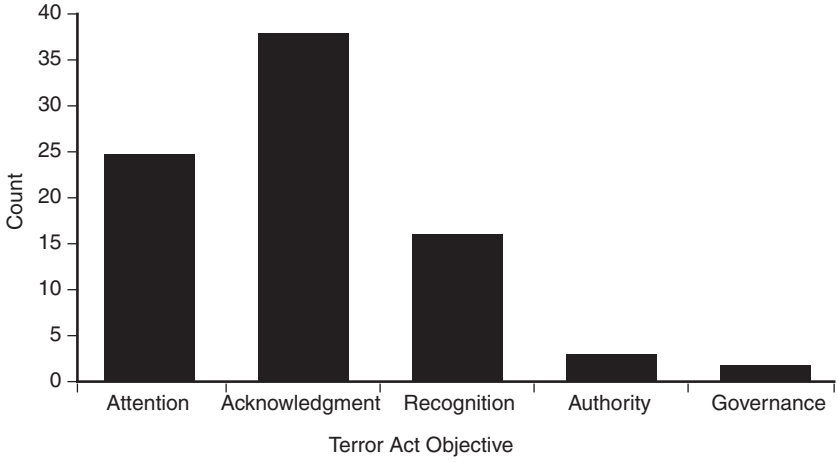


Figure 2. Idea count as a function of target

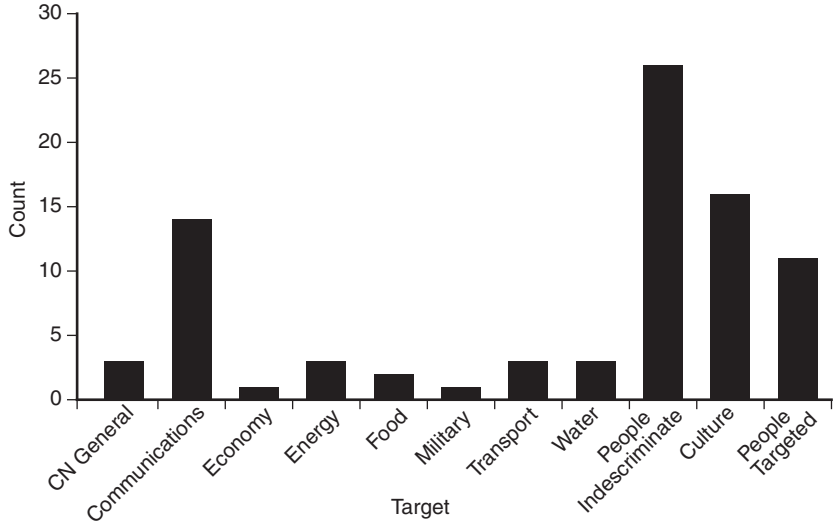
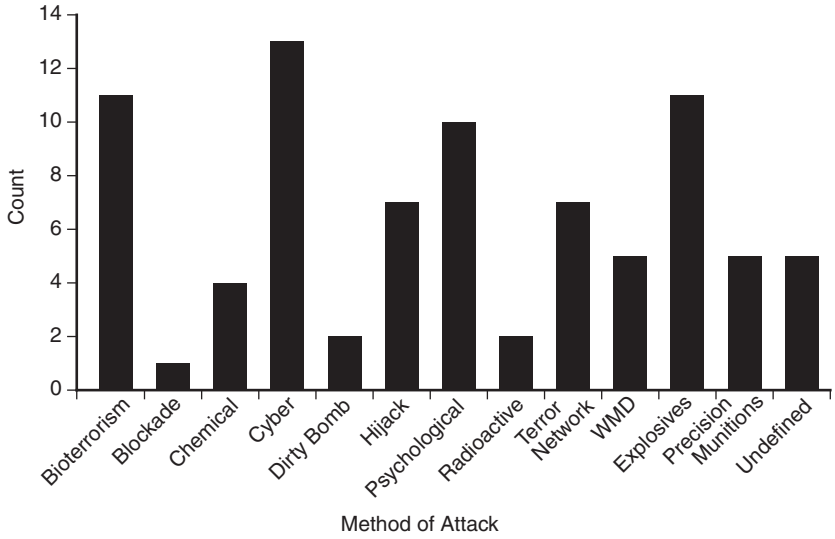


Figure 3. Idea count as a function of method of attack



In terms of method of attack, the most striking finding was the diverse spread of methods indicating that it is no longer possible to build contingency against a single method of attack but that any measures implemented need to be flexible enough to address a multitude of attack methods. Cyber attack and bioterrorism were deemed most likely together with the use of conventional explosives however, psychological attack was also deemed likely through either propaganda or the undermining and abuse of information systems.

Natural emergencies and disasters

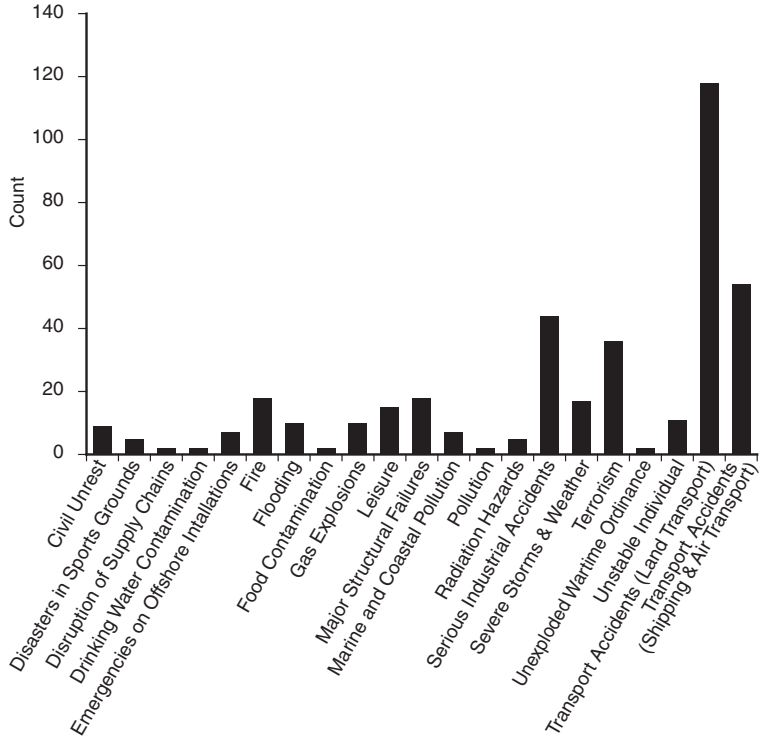
Natural disasters and emergencies come in many shapes and sizes and with different disasters and emergencies being broadcast 24/7 throughout the world it becomes very difficult to perceive the greatest threat. Although not infallible, historic data can greatly aid the realignment of perceptions and indicate where the greatest threats lie. Again there are many methods but the following shows a crude and basic method of the assessment of risks to the UK based on historical data.

Example 2: Natural disasters in the UK

The temperate climate, large industrial base and ageing and congested transportation infrastructure within the UK all pose significant risks and increase the chances of natural and accidental disasters. The dense population also means that such disasters can escalate rapidly and have disproportionate impact in terms of injury and loss of life.

The UK Cabinet Office maintains a database of major disasters.[4] This database includes both man-made and natural disasters both within the UK and overseas since the 1900. Figure 4 shows the incident count as a function of incident type for both man-made and natural disasters recorded within the UK.

Figure 4. Count of UK incidents as a function of type



[4] UK Cabinet Office Emergency Planning College. Major Incidents Database [http://www.epcollege.gov.uk/major_incidents.xls]

Transportation incidents and serious industrial accidents occur most often and response to and recovery from both of these events requires a robust critical infrastructure. Although, food and water contamination and flooding receive much media coverage they are relatively rare occurrences within the UK. Likewise terrorism is often thought of as a rare event but is in fact much more common in the UK than major structural failure.

Threat analysis conclusion

Intuitively one would assume that a nations critical infrastructure is at risk from both man-made and natural threats however, with 24/7 media coverage and a worldwide appetite for sensationalism it is very difficult to reach objective conclusions on the likelihood of particular threats. Nonetheless, such conclusions need to be made so that a nation can invest its scarce resource for protective measures to greatest effect. The above has demonstrated the value of simple future and historical analyses in determining the threats faced by a nation together with their associated probability.

The analysis also quantified the threat to critical infrastructure and highlighted that the most probable threat is not an direct attack in the critical infrastructure itself but from the threat of it being used a platform for man-made attacks designed to cause mass fatalities on a grand scale. With respect to natural disasters and emergencies the transport infrastructure is historically the place where most likely to occur.

Vulnerability Analysis

Having ascertained that the critical infrastructure faces a multitude of threats defensive measures cannot be taken unless the vulnerabilities of the system can be understood. As a starting point it is instructive to define what we mean by critical infrastructure.

The UK Government views the Critical National Infrastructure (CNI) as "those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could:

- cause large scale loss of life
- have a serious impact on the national economy

- have other grave social consequences for the community
- be of immediate concern to the national government"[5]

In the UK, the CNI is categorized as ten interdependent sectors; communications, emergency services, energy, finance, food, government & public service, health, public safety, transport and water.

Such a definition is not inconsistent with that of the United States where it is defined as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[6]

The US also defines a number interdependent sectors that include: the national electric power grid, oil and natural gas production, transportation and distribution networks, telecommunications and information systems, water systems, the banking and finance industry, the chemical industry, agriculture and food systems and public health networks.

Whichever definition chosen, although people often look to their Governments to take the lead in the security of the critical infrastructure, there is no single entity, either within the public or private domain, with sole responsibility and accountability for the system as a whole. Minor outages and disruptions can often be dealt with in isolation by infrastructure service providers however, infrastructures do not exist in isolation—telecommunications require electricity, transport networks requires fuel and in the case of the major emergencies and disasters that may arise from the threats discussed above key vulnerabilities exist at the interfaces and interdependencies between infrastructure service providers.

Governments have recognized the importance of such interfaces[7] and have adopted various approaches to reduce the vulnerabilities

[5] UK Security Service [http://www.mi5.gov.uk/output/Page76.html]

[6] USA Patriot Act, Public Law 107-56, October 26, 2001.

[7] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The White House, Washington D.C., February 2003, pp. 33-34. And *Critical Foundations: Protecting America's Infrastructures*, President's Commission on Critical Infrastructure Protection, Washington D.C., 1997.

both within the infrastructures at the interfaces. Discussed below are US and UK examples.

Example 3: Modeling and simulating critical infrastructures and their interdependencies

Modeling and simulation are particularly useful for large complex problems, especially when there exists little or no historical experience on which to base policy decisions. Recognizing their importance, the US has set up a National National Infrastructure Simulation and Analysis Center (NISAC).[8]

The work concentrates on the four primary classes of interdependency described below:[9]

1. *Physical*: When the state of an infrastructure depends on the output(s) of another.

2. *Cyber*: When the state of an infrastructure depends on information transmitted through the information infrastructure.

3. *Geographic*: If a local environmental event can simultaneously create a change of state in two or more infrastructures.

4. *Logical*: When the state of an infrastructure depends on the state of another through a policy, legal or regulatory connection.

A number of tools and techniques have been developed to address all aspects of infrastructure modeling and simulation and the cross-cutting programme calls for six main activities:

- Integrate modeling, simulation and analysis activities into national infrastructure and asset planning and decision support activities.

- Develop economic models of near- and long-term effects of terrorist attacks.

---

[8] Wimbish, W. & Sterling, J., "*A National Infrastructure Simulation and Analysis Center (NISAC): Strategic Leader Education and Formulation of Critical Infrastructure Policies*" Centre for Strategic Leadership, US Army War College, August, 2003.

[9] Rinaldi, S "*Modeling and Simulating Critical Infrastructures and their Interdependencies*" Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.

- Develop critical node/chokepoint and interdependency analysis capabilities.

- Model interdependencies among sectors with respect to conflicts between sector alert and warning procedures and actions.

- Conduct integrated risk modeling of cyber and physical threats, vulnerabilities, and consequences.

- Develop models to improve information integration.

Simple in theory—but very difficult to achieve in practice. It is well recognized throughout the infrastructure community that modeling and simulation are very powerful techniques and there exist many well developed commercial simulations of individual infrastructures that help owners develop, operate and manage their systems. However, the modeling and simulation of multiple, interdependent infrastructures is immature. Although the technical challenges are vast, this immaturity is not driven by technology but by the challenges associated with obtaining the data needed to accurately represent the infrastructures.

Much of the critical infrastructure is owned and operated by the private sector and the information required is propriety. Likewise there are significant barriers to the sharing of information between the private and public sectors such as the Freedom of Information Act, antitrust laws, confidentiality and privacy issues and access to national security information. Much work is underway to overcome these barriers by legislation;[10] however, data remains the crucial issue.

In the meantime it is possible, for example, to consider the approach of a major hurricane and project its track over land and determine the elements at risk, such as electric power generating facilities and approximate the outage areas. However, in the absence of a complete economic dataset for the communities affected it is difficult to ascertain where the break points in critical infrastructure provision are.

[10] See *Homeland Security Act of 2002*, Public Law 107-296, November 25, 2002. And *Procedures for Handling Critical Infrastructure Information; Proposed Rule*, Department of Homeland Security, Washington D.C., Federal Register, 6 CFR Part 29, April 15, 2003.

Example 4: UK Key Capabilities Programme

Rather than identify specific vulnerabilities through extensive modeling and simulation the UK has adopted the approach of identifying a number of capabilities that are frequently required during an emergency and disaster and exploring the vulnerabilities around them. Although this means that the UK is often planning for the last emergency rather than the next it does provide a framework around which public private information sharing can occur. The Key Capabilities Programme[11] aims to provide a framework for building resilience across the UK and its objective is to provide a "robust infrastructure of response" by developing "key capabilities" where the term "capability" refers to personnel, equipment, training, doctrine and operational concepts. Tables 1, 2 and 3 outline the key capabilities being built and the associated lead government department with responsibility and accountability.

Table 1. Capability Workstreams—the three structural workstreams

Workstream	Lead Department	Aim
Central Response	Cabinet Office	To enhance, improve the resilience of and, where necessary, further integrate central Government's crisis management arrangements.
Regional Response	Office of the Deputy Prime Minister	To ensure that the current state of resilience in each of the English regions is fully understood; to identify gaps in resilience; and to put work plans in place to ensure that such gaps are filled.
Local Response	Cabinet Office	To ensure sound structures are in place to support a local response to emergencies and disruptive challenges.

[11] UK Civil Contingencies Secretariat [http://www.ukresilience.info/contingencies/capabilities.htm]

Table 2. Capability Workstreams—the nine functional workstreams

Workstream	Lead Department	Aim
Chemical, Biological, Radiological and Nuclear (CBRN) Resilience	Home Office	To ensure that the country is capable of responding quickly and effectively to deal with and recover from the consequences of incidents involving chemical, biological, radiological or nuclear material, particularly those caused by terrorism.
Site Clearance	Office of the Deputy Prime Minister	Clearance, removal and disposal of large volumes of rubble and other debris after a catastrophic disaster.
Infectious Diseases —Human	Department of Health	To build an effective capability to vaccinate and treat people as part of an emergency response to an infectious disease such as smallpox or a flu epidemic.
Infectious Diseases —Animal and Plant	Department for Environment, Food and Rural Affairs	To ensure that plans exist and are regularly tested to respond to and minimise the impact of the spread of infectious diseases.
Mass Casualties	Department of Health	To build on the current preparedness and response arrangements already in place for dealing with major incidents and mass casualty incidents through the establishment of appropriate UK doctrine and an associated operational framework for the NHS.
Mass Evacuation	Home Office	To ensure UK-wide mass evacuation arrangements are in place in the event of a major disruption following a CBRN or other catastrophic incident.
Assessment of Risks and Consequences	Cabinet Office	To enhance the current capability of the centre to collect, assess and share across Government information concerning the likelihood and impact of challenges with the potential to disrupt UK life or the operation of UK Government.

Table 2. Capability Workstreams—the nine functional workstreams (continued)

Workstream	Lead Department	Aim
Warning and Informing the Public	Cabinet Office (Government Information and Communication Service)	To educate the public about current and new threats without causing panic; to develop mechanisms to alert members of the public of the need to take action, and to ensure that broadcasters can get timely, accurate and authoritative information to the public, in the event of an incident.
Dealing with Mass Fatalities	Home Office	To deal with fatalities resulting from a major or catastrophic incident; to identify the dead, to investigate causes of death and to dispose of bodies and body parts in a safe and decent manner.

Table 3. Capability Workstreams—the five essential workstreams

Workstream	Lead Department	Aim
Health Services	Department of Health	To ensure that plans exist to maintain continued Health Services in England in the event of a catastrophic incident.
Environment	Department for Environment, Food and Rural Affairs	To ensure that plans exist to maintain continued provision of water supplies, food supplies and flood and coastal defence in England in the event of a catastrophic incident.
Transport	Department for Transport	To ensure that plans exist to maintain continued provision of transport services, including public transport and supply chains and freight haulage capacity in England in the event of a catastrophic incident.
Utilities	Department of Trade and Industry	To ensure that plans exist to maintain continued provision of utilities (e.g. gas, telecommunications, and postal services among others) in England in the event of a catastrophic incident.

Table 3. Capability Workstreams—the five essential workstreams (continued)

Workstream	Lead Department	Aim
Financial Services	HM Treasury	To ensure that plans exist to maintain continued provision of financial services (information clearing house; market information; telecommunications; physical infrastructure; back-up arrangements (private sector); authorities' contingency response) in England in the event of a catastrophic incident.

Each of these workstreams is different in structure but all aim to bring together stakeholders within the private and public sectors to build a national capability. However, as with the US model information sharing between the public and private sectors is the key issue and although the programme seeks to set boundaries on collaboration the sorts of information sharing required to fully penetrate the extent of the infrastructure vulnerabilities is still a long way off.

Vulnerability analysis conclusion

Infrastructures do not exist in isolations—transport depends on power, telecommunications depends on electricity etc. Additionally the interdependencies are *bidirectional* meaning that something happening in one infrastructure will result in and effect on another and that effect will in turn result in an effect on the first. This means that unless the system is considered as whole and information freely passes between infrastructures a key vulnerability will exist at the interfaces. However, there appears to be an intractable problem surrounding information exchange between the public and private sectors which means that this infrastructure vulnerability will remain key and can be exploited. Much of a nation's critical infrastructure is owned and operated within the private domain and information on vulnerabilities is propriety and would constitute valuable market intelligence for competitors. Likewise the sharing of information about those assets within the public sector presents problems associated with national security information. The US example attempts to demonstrate the benefits of

this information sharing by using modeling and simulation and the UK approach attempts to build trust within public and private sector teams around common issues. There is value in both approaches and perhaps a combination approach would allow nations to surmount the information impasse that they are currently facing.

Consequence Analysis

The third and final part to quantifying risk lies in understanding the downstream consequences of a particular emergency or disaster. Typically there will be both near- and long-term political, environmental, social and economic impacts together with human casualties and potential national security implications. Due to the interdependencies and the difficulties in obtaining relevant and timely information outlined above these can be hard to predict for known events but even harder for rare and extreme events for which historical consequence data is scant.

There exist many different types of models and a combination of simulation tools may provide insight into all of the likely consequences. However, it is important to note that such simulations will provide information and guidance but will rarely be predictive in that they describe the exact consequences. They are therefore a useful guide for policy and strategy and in the case of rare or extreme events such as terrorism or catastrophic prolonged multiple infrastructure failure may provide the only guidance available.

The six most common types of modeling and simulation used for infrastructure consequence modeling are:[12]

- *Aggregate supply and demand tools*: An evaluation of the total demand for infrastructure services in a region together with the ability to supply those services.

- *Dynamic Simulations*: Modeling the generation, distribution and consumption of infrastructure commodities and services as flows and accumulations.

[12] NISAC Capabilitis Demonstrations, Portland OR, March 26-27, 2003, and Seattle WA, April 1-2, 2003.

- *Agent-based models*: The modeling of physical components of infrastructures as agents to allow the analysis of the operational characteristics and physical states of infrastructures. Agents can also be used to model decision and policy makers involved with the infrastructure operations, markets and consumers.
- *Physics-based models*: Analyzing physical aspects of infrastructures with standard engineering techniques.
- *Population Mobility Models*: The examination of entities through urban regions and their interaction with each other.
- *Economic models*: Including Leontief input-output models of economic flow.

Although many of these are standard simulation and modeling techniques used "within" many infrastructures the challenge is to expand their use to incorporate the interaction of infrastructures. Until this happens many consequence analyses assume an additive effect of consequences from the infrastructures as discrete entities rather than the force multiplier effects that happen in reality.

Historical analysis of disasters and emergencies shows that three core systems must remain in operation in order for the rest of society to function; power, banking/ finance, and telecommunications. The failure of any of these three systems will cause the failure of the other two within a matter of days or weeks. The loss of power would render banks and phone companies useless. The loss of telecommunications would render power companies and banks useless. And the loss of banking would eventually render power companies and telecomm companies useless. The impact of September 2000 fuel price protests on UK critical infrastructure serves to indicate the power of the force multiplier effects and our reliance on the energy sector.

Example 5: Impact of September 2000 fuel price protests on UK critical infrastructure

In September 2000, British farmers and truck drivers launched a campaign of direct action to protest about fuel duty. They blockaded fuel refineries and distribution depots, and, within days, created a fuel crisis that brought the UK to a virtual halt. The impact of the protest was much deeper than anticipated because it struck at a particularly

vulnerable point of the economy—the oil distribution network, which is organized along just-in-time delivery principles. This, combined with anticipated shortages by fuel consumers and consequent panic buying, magnified the impact of the protests on practically all sectors.

The disruption in the energy sector created a chain reaction among other sectors such as transportation, health care, food distribution, financial and government services due to their interconnectivity and interdependencies. The financial impact of the week-long fuel drought was estimated at close to £1 billion.

Conclusions

A nation's critical infrastructure is not a single entity owned and controlled by a single unit but comprised of interdependent sectors spanning both the public and private domain. In terms of defence this means that you need to know what the threat is, which vulnerabilities can be penetrated by that threat and the consequences of such a penetration. In terms of allocating scarce security resource to achieve maximum benefit you also need to know who has responsibility for the reducing which vulnerabilities and how the various sectors interact with each other.

These are non-trivial ,tasks. However, this paper has shown that there are a number of tools and techniques available that can be useful in adding a degree of objectivity to the analysis. Although a combination of historical and future analysis techniques can help to understand the threats we face, nations are finding a full vulnerability analysis difficult to achieve in practice: not because of technical difficulties in the modeling and simulation of the system but because of the difficulties encountered in information exchange between the public and private sectors. The problem of information exchange is also hampering the third and final part of the jigsaw which is consequence analysis. Without knowing how the system reacts as a whole it is very difficult to predict the chain reactions that can occur within the system due to a relatively small disruption in a single element. The example of the UK fuel protests of 2000 demonstrates how, what starts as a small event, can quickly spiral out of control.

Acknowledging the trans-national and public-private interdependency nature of critical infrastructure there have been a number of policy initiatives, both within Europe and the US. The EU Commission

plans to create a Critical Infrastructure Warning Information Network (CIWIN), which will bring together EU member state CIP specialists to assist the Commission in drawing up a programme to facilitate exchange of information on shared threats and vulnerabilities and appropriate counter-measures and strategies. Likewise, the US has a similar system known as Critical infrastructure Warning Information Network (CWIN) which has been operational since 2003.

However, as a final thought, it is worth noting that information exchange, simulation and modeling, and the cataloguing of critical assets are not the sole domain of those wishing to defend a nation—they are also available to those wishing to harm a nation. Accurate, timely and complete information is key both sets of modelers and the above networks are designed to tip the information balance in the favor of the modeler trying to defend the nation. Their success is therefore an imperative.

Chapter 9

Intelligence Cooperation and Homeland Security

Yves Boyer

Intelligence cooperation and homeland security issues are tricky matters and remain largely marked by secrecy making analysis an almost impossible task with which to grapple. Intelligence cooperation is indeed a matter of high confidentiality in a scene where shadows matter as much as light. People involved in that business will certainly not expose the nature, the purpose, the scope, the channels and the depth of their cooperation. To such opacity, one has to add the very nature of what is at stake. It is about using the means offered by international cooperation for exchanging very sensitive information in order to identify, deter, prevent and act against terrorism. In that sense international intelligence cooperation for protecting the nation, the homeland, is about linking the local[1] to the global.

The local is where the attack occurs, inflicting death on an innocent population. In that respect, it is the first responder that ought to deal with the many consequences and trauma caused by terrorist action. In this case, the only provider of protection and reassurance is the nation-state. This is also the level at which intelligence cooperation, inward and outward, could be organized and can bring its anticipated benefits. This does not mean, however, that other levels should be neglected or ignored, particularly the European Union level and the global level.

Even if the suffering, the pain and the costs resulting from terrorist attacks are essentially local, and even limited to a tiny area (train, metro, discotheque, buildings), the impact of any terrorist's action is immediately projected world-wide on the "global village." This is where terrorists seek primarily to draw the "best value" from their contemptible action in propagating fears that, they hope, will lead

[1] The local is at the same time the precise location where the attack occured and the level where citizens are expected to find help and protection, i.e. the national level.

governments to be more amenable to their objectives. Countries are thus being led into being constantly vigilant about terror and terrorists when, at the same time, in a very cynical way, casualties resulting from terrorists activities, although unacceptable, remain low in comparison to other sources of death, such as diseases. In 2004, for example, domestic accidents caused the death of around 20,000 people in France,[2] a figure roughly similar in Germany or in Britain. That same year, 38,253 people died in the USA from car accidents[3], a figure which exceeds by 15% world wide casualties (32,864) provoked by terrorist actions between January 1968 and November 2005.[4]

Nevertheless, terrorism represents a high risk not only for the reason of the casualties and the destruction it inflicts to innocent people but also because it could affect, in certain circumstances, the social pact existing within democratic countries where multiculturalism is expected to become part of a new covenant. If the state, at the national level, appears to guarantee safety and security, its authority could be defied by groups seeking revenge from terror attacks allegedly attributed to members of minorities that may be, in return, subject to violent reactions. Consequently, if security of the homeland has to be assured, this is also in order to protect social and political stability in countries susceptible to being the victim of indiscriminate attacks. Here lies one of the very challenges to nations, compelling them to use every means at their disposal in fighting terrorism. Intelligence cooperation is naturally one of them. To be efficient, such cooperation presupposes many mechanisms tailored to the need, particularly in allowing rapid reaction for transmitting urgent and very sensitive information within the right decision time. In order to build such mechanisms and define adequate procedures it is important to have clarity about the nature of the threat.

---

[2] "4,5 millions de victimes d'accidents de la vie courante," *Le Monde*, November 10, 2005. Reported by Agence France Presse.

[3] US statistics are borrowed from the National Center for Statistics and Analysis. As a matter of morbid comparison according to statistics provided by the National Policy Agency of Japan, 89,677 people died of car accidents in Japan between 1995 and 2004, a figure that dwarfs the deaths from terrorists' attacks: 12 people died after the sarin gas attack in the Tokyo metro in 1995; 24 Japanese citizens were lost in the World Trade Center during the 9/11 attack.

[4] The figure is taken from MIPT Terrorism Knowledge Base (MIPT stands for Memorial Institute for the Prevention of Terrorism). Even if those figures can be discussed, they however are very indicative.

In the US the terrorist threat is defined according to Title 22 of US code: "*Terrorism means premeditated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents*." Another very similar definition is given by the French Military Joint Staff (*Etat-Major des Armées*): "*terrorism is the illegal use or threat of use of force or violence against people or goods in order to constrain or intimidate governments or public opinions in order to reach political, religious or ideological goals*."

Despite its ephemeral nature, it is commonly agreed that terrorism:

- concentrates its action against innocent people, against non-military targets in order to propagate fear among public opinion; as such those cowardly actions are attacks against democratic values;
- is mainly the action of non-state actors even though until the 1980s it was also state-sponsored (examples include the bombing of Pan Am flight 103 with Libyan involvement; the simultaneous bomb attack against French paratroopers and US Marine Corps installations costing the lives of 58 paratroopers and more than 241 marines in Beirut in October 23, 1983, of largely Syrian origin; and the bombing in Paris in 1986, which traces back to Iran[5]);
- can take different forms in the sense that one can talk about: biological terrorism (anthrax in the USA), chemical terrorism (Aum Shinrikyo attack in Tokyo metro subway with Sarin gas in March 1995 which killed 12 people and severely injured 5000 others), conventional terrorism using explosives combined with suicide attacks to maximize the precision of that attack, narco-terrorism or even cyber-terrorism;
- is increasingly the domain of loosely organized, self-financed, internationally networked people and rarely the result of "one man actions" with the exception of serial killers, such as the snipers in Washington DC during the fall of 2002 or the "Unabomber" (the nickname of Theodore Kaczinski, then a professor at the University of California at Berkely).

[5] In February, March and September 1986, a series of Islamic terror attacks in France provoked the death of 13 people while injuring 267 others.

Those networks of individuals use non-conventional means of destruction which are usually relatively cheap. The cost of 9/11 has been estimated at about half a million dollars for the nineteen men involved. With the exception of few groups like ETA (*Euzkadi ta Askatasuna*, the movement for the liberation of the Basque territory), the *Liberation Tigers of Talim Eelam* in Sri Lanka, and the Kurdish extremists, they cannot be identified with a territory. There is no front; terrorism is at home everywhere on the global village; no country in the world can consider itself immune. There is indeed a growing cross-national link among different organizations which may involve combinations of military training, funding and technology transfer. The group to whom Mohammed Bouyeri (the man who killed the Dutch film-maker Theo Van Gogh) belonged, had contacts with the terrorists who perpetuated, in May 2003, the bombing attack in Casablanca killing 45 persons and later in Madrid in March 2004; the same group failed to implement an attack against the then Portuguese prime minister and current chairman of the EU commission, José Manuel Barroso. Terrorist movements are also protean in the sense that they can act as an international movement (FPLP—*Front Populaire pour la Libération de la Palestine*) or in a single country (former Irish Republican Army, IRA). They can pretend to defend a separatist cause (ETA). They can be motivated by religious faith such as radical Islamism or being millenarian such as the Earth Liberation Front (ELF), an international underground organization consisting of autonomous groups of people spread throughout the UK, USA and Canada.

Hence, it remains very challenging to characterize modern terrorism in a full comprehensive way and accordingly set up "universal" mechanisms to eradicate its financing, its recruiting, its networks and prevent its operations. A distinction between "terrorism of resistance" fighting against a totalitarian regime or foreign occupation using unacceptable means but having a political agenda, and "terrorism of hatred" aimed at destabilizing countries by killing innocent victims without having any coherent agenda has, however, to be established in order to define specific requirements for intelligence cooperation at the international level. The latter type of terrorism which appears like a "black hole" constellation, a loose organization like a "franchising system" without a single authority, more easily generates international cooperation since a general consensus exists about the need for its total and absolute eradication. Sometimes, however, the boundaries

between the two types of terrorism are blurred. To add to that complexity, Islamist terrorism can be understood as a system of concentric circles. The first one is the core of Al-Qaeda, or what is left of it. Then one finds regional organizations, which are still structured for now. For instance, the Chechen independence movement seems to be linked to Al-Qaeda which also seems very active in networking terrorist groups in an arc of crisis ranging from Chechnya to South-East Asia. The third circle is comprised of a loose and informal conglomeration of radical Islamic militants—"freelance" jihadists[6]— most of them being citizens of the countries in which they live. Intelligence cooperation against such diversity of networks has to be appreciated at three levels of "operation."

The first is the national level. At that level, a huge diversity of situations exists. National organization varies according to historical experience, administrative structure and political architecture. Organizations range from centralized structure to more decentralized which gives local power (*Länder*, states, regions etc.) a certain capacity to mobilize police resources against terrorist activities. Despite these differences, a common set of problems has to be solved internally to produce efficient and mutually fruitful intelligence cooperation at the international level. Besides traditional national inter-service rivalries, one key issue is about giving coherence to the intelligence processes at the national level. Traditional police forces, *gendarmerie* (in certain countries) and customs agents interact with many other agencies such as the counter-intelligence apparatus (the Federal Bureau of Investigation in the US; DST, *Direction de la Surveillance du Territoire* and *Renseignements Généraux* in France; MI5 in Britain, and the BND *Bundesnachrichendienst*, in Germany, etc.). There are obvious difficulties in synchronizing and pooling intelligence products efficiently among those many different services which have their own history, code and behavior. Sometimes the issue is essentially technical. For example the National Security Branch of the FBI supervises the establishment of common standards for exchanging data among US counter-terrorist organisations. Interoperability is sought through a common information system build around the TWPDES (Terrorist Watchlist Person Data Exchange Standard) which should harmonize

[6] On the "fabric" of jihadists see: Jean-Luc Marret, ed., *Les fabriques du jihad* (Paris: Presses Universitaires de France, 2005).

data from the NSA, National Security Agency, the FBI and from the Justice Department.

At other times the issue is not technical, but structural. In order to enhance the whole effectiveness of national organization the need may also call for creating new bodies with the task of coordinating the many efforts done at the national level in fighting terrorism. In France, for example, the Cilat (*Comité interministériel de lutte antiterroriste*), an inter-ministerial structure chaired by the Interior minister, is coordinating the works of other ministries regarding protection against terrorist activities; the UCLAT (*Unité de Coordination de la Lutte Anti-Terroriste*) was created in 1984 to coordinate and spread intelligence information among French specialized services. UCLAT has liaison officers in Germany, UK, Italy, Spain, Belgium, Holland and the USA. In Britain, a structure that is in charge of synthesizing intelligence materials about terrorist activities for political leaders also exists, the JTAC (Joint Terrorism Analysis Center). Under the leadership of the Director General of the MI5, the JTAC comprises representatives from eleven government departments and agencies. At the Home Office level, terror activities are coordinated by the Counter-Terrorism and Intelligence Directorate (CTID).

The second level of intelligence cooperation is the European and allies level. At the level of the EU the recognition of the need to deepen cooperation to fight terrorism has been the result of the trans-borders activities of terrorist cells. As early as in 1975, the European Council decided to organize an internal security group called TREVI (Terrorism, Radicalism, Extremism, Violence, and Internationalism). The TREVI group was then set up among the nine European Economic Community (EEC) members to deepen police cooperation notably in relation to extremism, radicalism and terrorism at that time identified with the *Rote armee fraction* in the Federal Republic of Germany (FRG), Red brigades in Italy and *Action Directe* in France. 9/11 has considerably modified the EU perspective in fighting terrorism with the adoption on September 21, 2001, of a Plan of Action to Combat Terrorism encompassing legislative measures, the strengthening of operational cooperation among security services, police and customs, the improvement of the effectiveness of information systems with new functions added to the Schengen Information System (SIS).

- *Europol* has thus seen its anti-terrorist activities significantly increased with the establishment of a counter-terrorist task force.
- A European Arrest Warrant has been agreed upon even though only 17 out of the 25 members had included this European Arrest Warrant in their respective national laws by June 2004.
- A new structure, Eurojust was created in order to develop judicial co-operation within the EU.
- Cooperation agreements have been signed with the US such as, for example, in April 2004 the agreement to strengthen maritime container security.
- The High Representative for the Common Foreign and Security Policy (CFSP) is able to use the Situation Center (SitCent) to provide synthesis of intelligence materials (provided by the member states) to the EU presidency and to the various member states. Although the role of SitCent should not be overestimated. It receives rough analysis from other sources of intelligence. For example, Europol is not allowed to give personal related data but only broad strategic analysis.[7] Similarly, exchanges of sensitive information are still made on a bilateral basis among the EU member states and only among key players in Germany, France, the UK and very few others countries members of the Union.
- This arsenal of measures was improved after the Madrid bomb attack in March 2004. At the European Council of June 2004, a "EU Plan of Action on Combating Terrorism" was endorsed in accordance with UN Security Council resolution 1372 of 2001 which established the Counter-Terrorism Committee, made up of all 15 members of the Security Council.
- Surveillance of land borders of the Union (6,000 km) or its maritime borders (85,000 km), a European Borders Agency is to be set up by January 2005.
- The position of a Counter-terrorism Coordinator, Gert de Vries, has been established to co-ordinate the work of the Council in combating terrorism.

[7] Interview of Max-Peter, Europol Director, *Jane's Intelligence Review*, November 2005.

Cooperation within the EU is, however, still limited by some factors such as differences, for judicial reasons, in the organization of the legal systems and in the strategic conceptions of the threat. The French were already confronted with Islamist terrorism in the 1980s, which led them, since 1986, to put the legal system at the center of the struggle against terrorist activities. This has led to the development of a proactive policy, which means doing away with the distinctions between prosecution and prevention as carried out by the intelligence services. According to Jean-Louis Brugière, a judge in charge of anti-terrorism: "*the advantage of this is that the legal system is more credible and less contested. By working more closely with the secret services the legal system is reinforced. Our system is much more flexible as it is civil law rather than common law. The source of the law are legal texts, not jurisprudence of previous decisions. We don't have to bow to legal precedents, as in the UK or US, which prevents their system from evolving.*"[8]

A second factor bearing on more comprehensive intelligence cooperation is about risks of increasing intelligence sharing among governments. This risk has been raised by the head of MI5, Dame Eliza Manningham-Buller[9] after Charles Clarke, Britain's Home Secretary, called for the European Union's twenty-five member states to enhance intelligence sharing about terrorist suspects. Dame Eliza declared she was concerned that such sharing—as well as the use of intelligence in prosecutions—would jeopardize sources "*it comes from human sources who risk their lives and whom we have a high moral duty to protect, and from technologies whose effectiveness can be countered by skilled opponents. That is why there can be no coercion to share intelligence and why its use in open courts needs to be carefully handled.*" Dame Eliza said co-operation was important given the international threat. But European agencies "*should focus on implementing existing initiatives rather than producing a fresh raft of them.*"

Among allies, outside an EU framework, one has to mention the elusive role of the so-called "Alliance Base,"[10] which is a network of

[8] "The FT's Martin Arnold talks to France's top anti-terrorist judge," *Financial Times*, August 26, 2005. See also: French Push Limits in Fight On Terrorism, Wide Prosecutorial Powers Draw Scant Public Dissent," Craig Whitlock, *Washington Post*, November 2, 2004.

[9] "MI5 chief warns on increasing intelligence sharing," Stephen Fidler, *Financial Times*, September 9 2005

[10] "La CIA et la DGSE auraient établi une structure secrète antiterroriste," *Le Monde*, July 4, 2005; "Help From France Key In Covert Operations. Paris's 'Alliance Base' Targets Terrorists," Dana Priest, *Washington Post* July 3, 2005.

intelligence services working together on matters related to terrorism and having their "secretariat" located in Paris. The members of "Alliance Base" are similar to those participating to the MIC, Multinational Interoperability Council. The MIC is a kind of a "reinforced cooperation" in military affairs established between the US, France, Britain, Germany, Australia, Canada and, since 2005, Italy. MIC is working at a very high level to develop new military concepts and doctrines.

The third level of intelligence cooperation is related to the world level. At the UN level, Resolution 1373 (September 28, 2001) established the Counter-Terrorism Committee (CTC) made up of all 15 members of the Security Council. The CTC monitors the implementation of resolution 1373 by all states and tries to increase the capability of states to fight terrorism. Resolution 1373 imposes binding obligations on all states, with the aim of combating terrorism in all its forms and manifestations. The resolution requires member states particularly to "share information with other governments on any groups practising or planning terrorist acts" (paragraph. 2b, 3a, b, c) and "*co-operate with other governments in the investigation, detection, arrest and prosecution of those involved in such acts*" (p. 2b, f, 3a, b, c). These statements are useful attempts to push intelligence co-operation between states when terrorism is concerned, although there are obviously no constrains associated with such claims.

There is a worldwide co-operation in intelligence which is now going on. This type of cooperation is made more and more on an ad hoc basis and is essentially bilateral. Even countries with political divergences may be led to exchange pertinent intelligence information. For example, during a visit to London in the fall of 2005, Vladimir Putin was accompanied by Anatoly Safonov, special envoy of the Russian president for international co-operation against terrorism. Despite tensions between Europeans and Russians on human rights abuses in Chechnya, the Russians discussed anti–terrorism with their British counterparts. A working group on that matter will be developed between the two governments.

More generally, we are witnessing the multiplication of bilateral or multilateral contacts among security and intelligence services throughout the world. This sort of gathering now encompasses meetings between many different internal security services. For example, in

October 2005, the head of the Japanese Public Service Investigation Agency (KOANCHO), Takashi Oizumi visited his French counterpart at the DST. Discussions now encompass not only terrorism but also organized crime, which represents a growing challenge for many states. International meetings also are places where countries at odds on many other topics can still gather to talk about international terrorism. Such meetings occurred, at least openly, twice in 2005. At a meeting in February in Saudi Arabia, among the many participants were the head of Pakistan's intelligence service (SIS), Britain's MI5 head Dame Eliza Manningham-Buller, the head of French's UCLAT, president Putin's special envoy on terrorism Anatoly Safonov and president George W. Bush's advisor on homeland security, Frances Townsend. A few weeks later in March in Novossibirsk another such meeting happened where many heads or representatives of services committed to fight terrorism from the EU, NATO, the G8, and the CIS, etc., gathered again.

The global fight against terrorism thus calls for new ad hoc cooperation sometimes far away from the traditional channels inherited from the Cold War. Realism and efficacy make virtue out necessity. If Western government have sometimes expressed concerns about human rights abuses in some countries, they, however, are led to increase police and anti-terrorist cooperation with those same countries. Hence, to global disorder corresponds a globalization of the fight and the hunt against terrorist activities throughout the world.

Chapter 10

Homeland Security and the Role of Business

Pauline Neville-Jones and Neil Fisher

At a conference of the Confederation of British Industry in Birmingham, England, in November 2004, the Head of Britain's Security Service, Dame Eliza Manningham-Buller, said "There is a serious and sustained threat of terrorist attacks against UK interests at home and abroad. The terrorists are inventive, adaptable, and patient; their planning includes a wide range of methods to attack us. Be under no illusion, the threat is real and here and affects us all." The implication was that the threat was not just from abroad, but home grown too. The accuracy of the warning was demonstrated on July 7, 2005, and again, precisely two weeks later, on July 21, 2005, when UK nationals perpetrated, or tried to carry out a linked series of suicide bombings in the mass transit systems of London. Their first attack took place as the world's media assembled in Gleneagles, Scotland, for the G8 Heads of Government meeting, causing the host, the British Prime Minister, to have to break off to make an emergency flight to London.

Though people were conscious of the fact that this was the first taste in Britain of a new kind of terrorism, there was no panic. Despite the loss of life and the considerable damage done to the Underground system, the impact on the daily life of the city was marginal. The aim of instilling fear failed and the population proved to be resilient. The competence and effectiveness of the first responders and of the blue light services generally in the immediate aftermath of the attack were crucial in providing reassurance that the government was well prepared and would provide leadership to get on top of the crisis. London remained open for business. Though prevention had failed, resilience had been demonstrated. Had this not been the case, the political and economic impact of the attack would have been infinitely more damaging. The role played by private sector organizations in recovery, though not especially obvious to the external observer, had nevertheless been central to speedy and successful recovery.

In current political conditions, the corporate sector faces new challenges in ensuring operational continuity and resilience. These consist partly in changes in the external political, economic and physical environment which have generated new threats—including, but not only, terrorism—over which companies have no direct control, but for which they must prepare; and partly in secular changes taking place in the way companies themselves operate and are managed which have created new vulnerabilities. During the Cold War, there the risk of the annihilation of organized society existed which, however, became increasingly remote with time. In current international conditions, western societies face much a greater likelihood of attacks which, though more localized in their immediate impact, are capable of causing much broader damage indirectly via the networks that characterise modern economies. There is thus transformation in both threats and vulnerabilities and a new focus on prevention and recovery. This chapter will focus on both aspects, on the interaction between them, on the need for the corporate sector to make itself more resilient, thereby contributing to a more resilient society overall. It will draw on British experience, but the authors believe that the issues and experience described has wider application in modern industrialized societies.

Transformation of the economic and social context

It has been much remarked that the experience acquired by UK authorities during the period of IRA terrorism have been important in the response and recovery techniques on display on July 7, 2005. As significant, but less remarked, were the lessons learnt by government during the UK trucking industry strike of September 2000 which took the form of coordinated picketing almost all fuel depots. Retail petrol supplies dried up. Within 24 hours, hospitals, deprived of their staff, were near closure. Within 48 hours, supermarket shelves were bare of staple foods. The country ground to a virtual halt. The vulnerability of an intensively populated "just in time" economy with its tight dependencies lacking in any surplus capacity, had been alarmingly revealed. "Local" could rapidly become "global." The crisis also showed that events other than terrorism could offer serious threats to the national livelihood and that planning was needed to cover a wide range of civil contingencies, including natural as well as man made disasters.

UK public authorities were galvanized by the summer of 2000 experience of near national shut down into a serious study of recent, but ill understood, changes during the last two decades in the critical national infrastructure (CNI). Three changes stood out: first, there had been changes of ownership through privatisation of such things as public utilities which meant government had lost direct control of many basic services. Secondly, in the name of increased efficiency, many companies and organizations had outsourced or decided to share processes essential to their operation, thus further complicating control and planning. Thirdly, the widespread use of digital technology had ushered in the phenomenon of the globalized organization which operated across the world with decreasing reference to time or geography and without obvious central points of overall control. This combination of ideological change, technological revolution and dramatic corporate expansion in the wake of the Cold War had in turn driven two secular transformations. First, there had been a major shift in the structure of power in society between the public and private sectors in which government now found itself much less able to call the shots without reference to the private sector. Secondly, within the private sector a massive change was also taking shape, fundamentally affecting the way companies were managed. Both parties had to understand and adapt to the consequences of change within and between them.

In the new threat environment, government and private sector found themselves forced to take close account of each other. On the one hand, government has had to redefine the scope of national security very broadly to cover key aspects of civilian daily life—not just government and the utilities but also communications, transport, health and retail distribution systems among other things. The task is to maintain the connectivity of a networked society. This has meant forging new relationships with the many private sector owners of a significant proportion the key assets. The private sector owners have in turn had to incorporate public interest considerations into their planning and into ensuring the existence of adequate management controls.

Government response

The approach taken by government has varied according to subject and sector. Broadly speaking, the government has the choice of compulsion of, or cooperation with, the private sector. In a number of cases, it has chosen the regulatory route—as in the obligations on financial institutions to report financial transactions in an effort to combat threats to national security such as money laundering and the evils associated with it like drugs and gun running and people trafficking. In more instances however, such as protection of the CNI, it is choosing the cooperative- or variants on, the cooperative route. This is partly in recognition of its relatively weaker position (who, after all, produces and possesses the CCTV pictures or the telephone records so vital to the police in an emergency?) which involves a two way flow of information about the threat to and the preparedness of the CNI and the private sector generally. It is also because government does not wish to pay all the costs and would not in any case know how to apportion responsibility between, for instance, private sector companies sharing facilities. There are also other ways to the same end: it is, for instance, open to government to incentivize the attainment of minimal security standards by setting them for companies wishing to tender for government contracts. It can licence or create tax benefits relating to the attainment of agreed security standards and, in relation to those risks where insurance is available, it can look to the insurance industry to police the adequacy of mitigation by the rates charged.

In the UK case however, it has to be said that these techniques have yet to be used in any systematic way. Government still has to complete work out the standards it wishes to attain internally, as well as require externally. The setting of standards would also require the promulgation of a strategic framework so that those organisations being asked to meet them could understand their relevance and purpose. In the UK, government needs to reveal much more than it has yet been willing to do about its attitude to risk. Its reluctance to do this may be related in part to the obscurity of the budgetary process—it is impossible to know how much homeland security is costing or how the money is being spent—and out of a desire to keep governmentally borne costs down. Over the long term however, agreeing on the acceptable levels of risk in different sectors and the distribution of the costs of mitigation will be one of the keys to successful provision of security.

Policy making also needs to emerge more form the shadows. The UK government's national strategy for countering terrorism, known as CONTEST, is classified. While bits of it have been released when the government has felt the need to convince the public of the reality of the threat to the United Kingdom, the strategy has not been made available to business or the public as a single document even in unclassified form. Such secretiveness is counterproductive to good government leadership. Adequate, consistent and continuous communication on the part of government is essential as one of the techniques needed—along with adequate exercising-to ensure that the strategy actually works in a crisis. London did well in July 2005. But the UK also needs to ensure it is prepared to withstand a bigger hit still.

Business response

In responding to the new external environment, business has simultaneously faced a task of internal adaptation rather greater than that undergone by government—hardly surprising, perhaps, as it is the corporate sector which has been the main driver and beneficiary of change. Transformation has become a continuous process without resting point. Technology has enabled a huge increase in the velocity of activity within and between companies to take place. In consequence there have been productivity gains—sometimes massive—resulting from much more efficient use of labor and plant which however depend for their realization upon the utter reliability and invulnerability from disruption of business activity. In management, decision making has been speeded up and hierarchies flattened. The customer has gained power. Increasingly, with less reliance on process, quality and reliability of staff lies at the heart of corporate success. Trust has become a vital commodity. The more highly geared the situation, the less the distance between ensuring business continuity and business survival. The security and survivability of the company's assets, whether physical or intellectual, becomes a top priority.

Companies have had to accommodate the consequences of these changes in their management and governance structures and practices. Not all have been equally successful. Evidence about business awareness of and sentiment about security in the UK was provided in a survey conducted in November 2004 by QinetiQ, a leading British defense and security company. It revealed that while there was a wide-

spread high level of concern about security and a consequent increase in some companies in security spending and in the development of continuity plans, there was at the same time declining confidence in the effectiveness of these efforts. QinetiQ termed this phenomenon business insecurity. It seemed clear that business leaders were confused about the risks and threats they faced and what they should be doing about them.

The evidence indicates that risk management is taken increasingly seriously and gets much more of a hearing round the Board table than it used to. Senior management is less inclined than previously to view security as a purely technical matter to be left to middle managers. Even so, risk assessment frequently remains unimaginatively narrow in scope--covering only those risks specifically directed at the company or those within its control when the threat may lie beyond this—and badly directed. Focusing on the likelihood of a given risk rather than on the extent of the vulnerability of key dependencies can give the wrong answer. Beyond monitoring, the attitudes displayed are often still too passive. A company culture of security is too seldom cultivated and taking active measures to increase security is too often seen purely as a route to extra costs, rather than as a business enabler. The reputational as well as financial cost of a loss of function is too frequently disregarded.

Such behavior is increasingly risky and destroys trust. It also undermines partnership between government and the private sector over security. Companies' several security roles depend for their success on maintaining trust. In consuming homeland security from government—which uniquely has the resources to provide threat assessment—they must inspire confidence in their ability to protect sensitive information. In providing security within their own domain, they must aim to maintain trust through total reliability and, as suppliers of security expertise to the public sector, they need to be trusted partners. Many of the technologies, services and security products which government will need to procure are only to be found in the private sector. The multiplicity of roles offers industry opportunities, but they carry with them obligations to ensure effective risk management internally and good value for money when contracting externally to provide security services.

Conclusions

Being secure unavoidably involves cost for companies. But it is also good business. Companies already have big obligations in the area of risk management and those which already take them seriously should not find it difficult to take in their stride management of those which arise specifically in the context of homeland security. For those companies with inadequate risk management, the increased risks and vulnerabilities arising from the new threats to society and the economy should act as a wake up call. Your business, and those of your suppliers and customers, can be destroyed.

Government is aware of its fundamental obligation to its citizens to provide them with protection. The way it goes about this has however to change. It can no longer do this effectively—if it ever could—on its own or behind a wall of secrecy about the level of the threat or the measures it plans to take in emergency. The breadth of the task and the government's dependency on the private sector to provide solutions is now too great for an approach lacking in transparency to have any chance of working in the long term or of commanding popular support among an informed electorate. While it is legitimate for government to expect the private sector to pick up a significant proportion of the costs, it too will have to budget for the long term and help plug any important market failures that may arise such as the absence of adequate insurance. A start down the road of public private partnership in making the country more resilient has been made though there is a still a long way to go. The interests of government and companies will not always be aligned and compromises will be necessary on the way. Failure is not, however, an option.

About the Authors

Dr. Sandra Bell is Director of the Homeland Security & Resilience Department at the Royal United Services Institute. Sandra Bell received a BSc (Hons) in Mathematics and Physics from the University of London before studying for a doctorate at the Royal Military College of Science, Cranfield University. She received a PhD in Military Science with a thesis in "Personnel Blast Protection." In 1991 Sandra took up an appointment as a scientist at the Defence Research Agency, which subsequently became QinetiQ, Europe's largest Defence and Security science and technology organization. Sandra initially specialized in personnel protection and acoustic stealth for ships and submarines and subsequently became Technical Director (Innovation & Strategy) where she was responsible for technology management and strategy within QinetiQ. Prior to joining RUSI, Sandra headed QinetiQ's Technology & Business Strategy Consultancy Business with a suite technology strategy consulting services to help organizations, both corporate and government, harness technology for business benefit. Sandra is now the Director of the Homeland Security & Resilience Department at the Royal United Services Institute in Whitehall. Her department provides integration and coherence for the new security environment by being a professional forum for decision makers, solution providers and system integrators.

Dr. Heiko Borchert directs a business and political consultancy specializing in strategic management and security and defense policy. He has worked with different military and national security organizations in Switzerland, Austria, and Germany on issues like scenario-based security policy planning, security sector evaluation, organizational reform, and defense science and technology. Besides lecturing at different universities and military schools in Europe, he is Director for Security and Defense at the Düsseldorf Institute for Foreign and Security Policy (DIAS) and co-winner of the 2003 Transatlantic Essay Competition sponsored by the Foreign Policy Association and the Richard C. Welden Foundation. Heiko Borchert studied international relations at the University of St. Gallen, Switzerland, where he also received his Ph.D. His research focuses on transformation, homeland security, Europe's security architecture, and

the transatlantic relationship. He is co-editor of a series of books titled *Vernetzte Sicherheit* [Network-Centric Security] and has published many articles, among others, in *Contemporary Security Policy*, *Orbis*, *European Security*, and *Connections*.

Dr. Esther Brimmer is Deputy Director and Director of Research at the Center for Transatlantic Relations at the Paul H. Nitze School of Advanced International Studies at The Johns Hopkins University. From 1999-2001 she was a Member of the Office of Policy Planning at the U.S. Department of State. She also served as a Senior Associate at the Carnegie Commission on Preventing Deadly Conflict and as a Special Assistant to the Under Secretary of State for Political Affairs. She has worked for the Democratic Study Group in the U.S. House of Representatives and for the management consultancy firm McKinsey & Company. She has written several articles and book chapters on international security issues. She is the editor of three Center volumes, *The Strategic Implications of European Union Enlargement*, *The EU's Search for a Strategic Role: ESDP and Its Implications for Transatlantic Relations*, and *The European Union Constitutional Treaty: A Guide for Americans*. She received her D.Phil. (Ph.D.) and master's degrees in international relations from the University of Oxford.

Prof. Yves Boyer is deputy director of the Fondation pour la Recherche Stratégique in Paris. He is also chairman of the Société Française d'Etude Militaire and an associate professor at Institut d'Etudes Politiques de Paris.

Dr. Anja Dalgaard-Nielsen is Senior Fellow at the Danish Institute for International Studies (DIIS) and non-resident Fellow at the Center for Transatlantic Relations, Johns Hopkins University School of Advanced International Studies (SAIS), Washington DC. She holds a Ph.D. from Johns Hopkins University SAIS. Dr. Dalgaard-Nielsen has published on a number of topics including homeland security, counter-terrorism, transatlantic relations, American foreign policy, and German security policy. She is a regular commentator on issues of foreign and security policy in Danish electronic and printed media.

Mr. Neil Fisher is Director, Business Development and Security Solutions, Security and Intelligence Division at QinetiQ. He joined QinetiQ's Security Macro-Capability in 2002 and has responsibility

for driving QinetiQ security products and capabilities into the global commercial and government agency security market. For three years Mr. Fisher held the position of UK managing director of a US critical infrastructure security subsidiary, also supporting a start up company in US specializing in biometrics and authentication, post September 11, 2001. His experience in Counter Terrorist technology and Information Assurance is extensive and spans 34 years in senior managerial and advisory/consultative roles. He currently holds the honorary role as Vice Chair of the UK's Information Assurance Advisory Council.

Dr. Gerd Föhrenbach is the Deputy Head of the Law/Politics Division at the Bundeswehr Transformation Center. He studied political science, history and English at the University of Freiburg (Germany) and at the University of Massachusetts in Amherst (USA). From 1997-1999 he was a Junior Fellow at the Center for European Integration Studies, Bonn. During 1998-1999 he was the Chancellor Kohl Research Associate at the Center for German and European Studies, Georgetown University, Washington, DC. Gerd Föhrenbach received his Ph.D. in political science at the University of Freiburg. His various publications include works on U.S. foreign policy, transatlantic relations, European security and the Baltic Sea region.

Dr. Daniel Hamilton is the Richard von Weizsäcker Professor and Director of the Center for Transatlantic Relations at the Paul H. Nitze School of Advanced International Studies (SAIS), Johns Hopkins University. He also serves as Executive Director of the American Consortium for EU Studies, a consortium of five U.S. universities designated by the European Commission as the EU Center of Excellence Washington, DC. He is the publisher of the Center's bimonthly magazine, *Transatlantic: Europe*, *America & the World*, and principal advisor to the Congressional Caucus on the European Union. He has served as Deputy Assistant Secretary of State for European Affairs, Associate Director of the Policy Planning Staff, and U.S. Coordinator for Southeast European Stabilization. He has authored many articles and books on transatlantic relations, most recently *Transatlantic Homeland Security* (with Anja Dalgaard-Nielsen, eds., 2005); *The New Frontiers of Europe* (ed., 2005); *Deep Integration: How Transatlantic Markets are Leading Globalization* (with Joseph P. Quinlan, 2005); *Partners in Prosperity: The Changing Geography of the*

Transatlantic Economy (with Joseph P. Quinlan, 2004); and *Transatlantic Transformations: Equipping NATO for the 21st Century* (ed., 2004).

Gen. Gustav Gustenau has been deputy director of management and the bureau of security policy in the Austrian Ministry of Defense since 2000. He has been the liaison to the Austrian National Security Council since 2002. He studied political science, history and philosophy at the University of Vienna. He has published many papers regarding security and defense policy.

Dr. Lawrence J. Korb is a Senior Fellow at the Center for American Progress and a Senior Adviser to the Center for Defense Information. Prior to joining the Center, he was a Senior Fellow and Director of National Security Studies at the Council on Foreign Relations. From July 1998 to October 2002, he was Council Vice President, Director of Studies, and holder of the Maurice Greenberg Chair. Prior to joining the Council, Mr. Korb served as Director of the Center for Public Policy Education and Senior Fellow in the Foreign Policy Studies Program at the Brookings Institution, Dean of the Graduate School of Public and International Affairs at the University of Pittsburgh, and Vice President of Corporate Operations at the Raytheon Company. Mr. Korb served as Assistant Secretary of Defense (Manpower, Reserve Affairs, Installations and Logistics) from 1981 through 1985. In that position, he administered about 70 percent of the Defense budget. For his service in that position, he was awarded the Department of Defense's medal for Distinguished Public Service. Dr. Korb served on active duty for four years as Naval Flight Officer, and retired from the Naval Reserve with the rank of Captain.

Dr. Gustav Lindstrom is a Senior Research Fellow at the European Union Institute for Security Studies (EUISS). His research areas include terrorism, transatlantic relations, non-proliferation, and space issues. Dr. Lindstrom also contributes to the Institute's ongoing work on ESDP related matters. Recent publications include *EU-US burdensharing: who does what?*, Chaillot Paper No. 82 (2005) and "On the Ground: ESDP Operations" in *EU Security and Defence Policy: The first five years* (ed. by Nicole Gnesotto, 2004). Dr. Lindstrom holds a Doctorate in Policy Analysis from the RAND Graduate School and a Master's degree in International Policy Studies from Stanford University.

Dame Pauline Neville-Jones has been Chairman of the Information Assurance Advisory Council (IAAC) since 2003. From 2002 to September 2005 she was Chairman and compliance Director of QinetiQ Group plc, a UK defense and security technology company. From 1998-2004 she was the International Governor of the BBC. From 1996-2000, she was a member of senior management of the NatWest Group. Prior to that she was a career member of the British Diplomatic Service. She was a foreign affairs adviser to Prime Minister John Major, Chairman of the Joint Intelligence Committee in Whitehall (1991-1994) and, as Political Director in the Foreign and Commonwealth Office, leader of the British delegation to the Dayton peace conference on Bosnia in 1995. She is a graduate of Oxford University and was a Harkness Fellow of the Commonwealth Fund in the United States (1961-1963).