Transforming Homeland Security: U.S. and European Approaches

Esther Brimmer, Editor

Defending societies and providing for homeland security make new demands on national security structures. How should countries organize their civilian and military assets to meet the challenges? What are the roles of the private sector or the place of intelligence operations? How can these security measures be crafted in ways consistent with our ideals and political cultures?

In this book, European and American experts analyze efforts to manage civilian-military relationships in the field of homeland security on both sides of the Atlantic. Authors discuss possible roles for armed forces in supporting homeland security; elicit lessons to be learned from ongoing transformation programs for homeland security; and outline possible joint action to overcome shortfalls and to improve the interplay between military and civilian capabilities commensurate with the new security risks. The book includes a joint road map for immediate and long-term policy action at national, European and transatlantic levels. The volume features contributions by:

Sandra Bell
Heiko Borchert
Yves Boyer
Esther Brimmer
Anja Dalgaard-Nielsen
Neil Fisher
Gerd Föhrenbach
Gustav Gustenau
Daniel S.Hamilton
Lawrence J. Korb
Gustav Lindstrom
Pauline Neville-Jones

The Center for Transatlantic Relations engages international scholars, students, government officials, parliamentarians, journalists, business executives and other opinion leaders on contemporary challenges facing Europe and North America. The goal of the Center is to strengthen and reorient transatlantic relations to the dynamics of a globalizing world. It is an integral part of the Paul H. Nitze School of Advanced International Studies (SAIS), one of America's leading graduate schools devoted to the study of international relations. Center activities include seminars, policy study groups and research projects, media programs and web-based educational and policy efforts. The Center also serves as the coordinator for the American Consortium on European Union Studies (ACES), which is a partnership among five national-capital area universities—American, George Mason, George Washington, Georgetown and Johns Hopkins—to improve understanding of the European Union and U.S.-EU relations. The Consortium has been recognized by the European Commission as the EU Center of Excellence in Washington D.C.

ISBN 0-9766434-4-8
90000
9 780976 643449

Washington SAIS Bologna Nanjing

Johns Hopkins University

Center for Transatlantic Relations

Transforming Homeland Security: U.S. and European Approaches

Esther Brimmer, Editor

CTR

Transforming Homeland Security

U.S. and European Approaches

Politisch-Militärische Gesellschaft

Danish Institute for International Studies

Esther Brimmer, Editor

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
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

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.

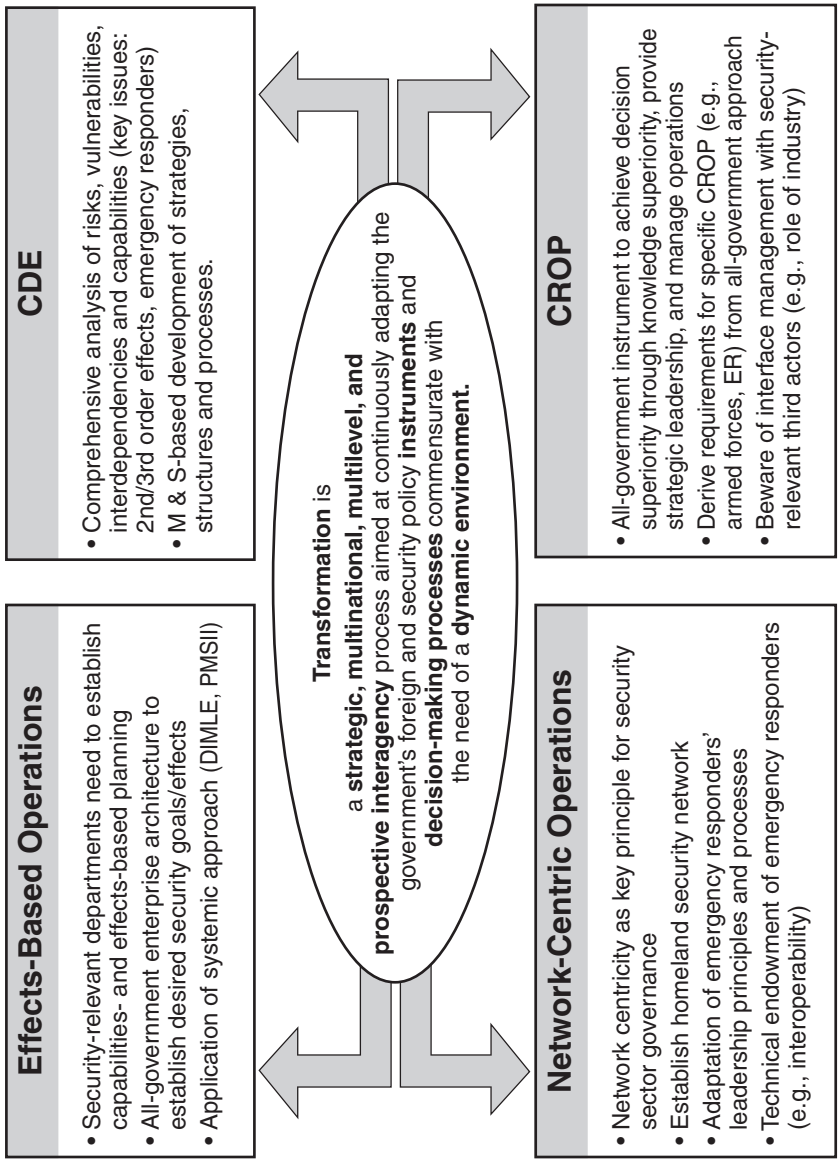
- containing the impacts/effects of a catastrophic event, managing its consequences, recovering, and facilitating the return to pre-crisis conditions.

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.

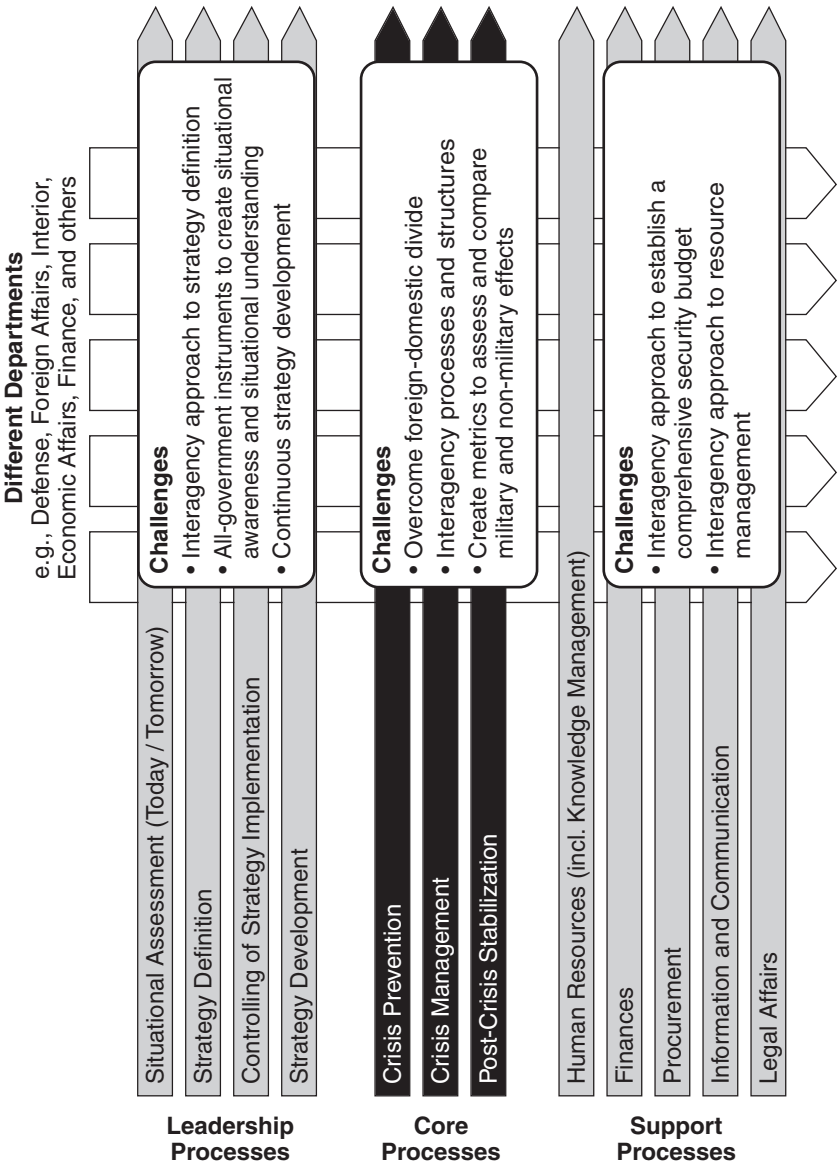
The realignment of security tasks described by the three security core processes referred to above will be seriously hampered without overcoming the structural dichotomy in organizing military and non-military capabilities. At the strategic level it will thus be crucial to implement joint instruments 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.