INFORMATION & SECURITY

An International Journal

Volume 17, 2005

Homeland/Societal Vulnerability and Security

Edited by
Peter Faber and Valeri Ratchev

ProCon Ltd., Sofia 2005

Content *I&S*

I&S Monitor

HOMELAND / SOCIETAL VULNERABILITY AND SECURITY

A decade after the end of the Cold war the world found itself in the face of security challenges, risks, and threats that cannot be countered effectively by traditional security organizations. The security systems of many countries are in the process of transformation, while other countries create entirely new organizations.

To reflect the respective conceptual and organizational developments and to facilitate doctrinal, organizational, technological, and educational innovation, the Editorial Board of *Information & Security: An International Journal* (I&S) decided to prepare a special I&S issue on vulnerabilities of modern societies and the search for higher levels of security.

Technical discussions of Homeland Security cannot occur in a void; they require both structural and cultural contexts if they are to be understood properly. Given this truth, the first two articles in this special issue of *Information and Security* deliberately seek to provide these contexts. Peter Faber's article provides the most "global" view of the topic, while Bengt Sundelius analyzes the societal dimensions of security today and provides a glimpse into proper organizational arrangements.

Christian Lanz then continues the general discussion by looking at homeland security from the viewpoint of a largely self-reliant neutral nation (Switzerland). Lionel Ponsard provides a Russian perspective on the subject, while Valeri Rachev presents the main problems in adapting security establishments of democratic countries to the challenges of spreading terrorism in a globalized world. He focuses on often neglected problems facing post-communist countries and the cultural impediments to the transformation of the security sector, as understood by Western analysts.

A research team from the Center for National Security and Defense Research in the Bulgarian Academy of Sciences assesses then the status and prospects ahead of Bulgaria's system for protection of population and critical infrastructure. The fundamental principles of the Concept for Civil Security of the Republic of Bulgaria have been formulated within the context of increasing integration of the security sector.

The following two articles provide a comprehensive treatment of another very important subject – critical infrastructure protection. Eugene Nickolov examines the consequences of attacks on specific elements of the infrastructures, as well as the initiatives and problems that arise with their protection on national and international level. Finally, Klaus Niemeyer's article considers the crucial role of modeling and simulation in critical infrastructure protection and thoroughly presents his research and development efforts in this area.

This special issue provides also a comprehensive, up-to-date list with on-line resources on Homeland Security related journals, institutions, resource repositories, events, as well as some milestone publications.

The reader will not find answers to all related questions in this issue. We believe, though, that this I&S volume will provide clear description of novel concepts, analysis of approaches and experience, and advanced modeling and analysis tools, that will be of service on the thorny path of creating systems for increased security in the Twenty First century that are both effective and preserve the values of democracy.

Information & Security

- Homeland Security: General Templates and Options for the Future
- A Brief on Embedded Societal Security

Structural and Cultural Context of Homeland Security

HOMELAND SECURITY: GENERAL TEMPLATES AND OPTIONS FOR THE FUTURE

Peter FABER [1]

Abstract: Homeland Security (HLS) encompasses the combined efforts of government agencies, non-government organizations, and the private sector to protect a nation-state, either offensively or defensively, against violent attacks. If attempts at protection fail, HLS then focuses on the management of and the response to such attacks. This generic, two-part definition of Homeland Security may be accurate enough, but it should not obscure a contradictory truth – HLS strategies invariably fluctuate by country and by region even though the era of exclusively national defense in Greater Europe is over, as is the era of narrowly designed national defense strategies themselves. Slowly but inevitably, all security strategies in the area, including Homeland Security strategies, will have to become "layered" if they are to account for the growing security roles of multiple actors operating on multiple levels. One user-friendly example of layering is the Pyramid Model of Strategy. This model attempts to be as reality-inclusive as possible by working from the bottom up – i.e., by working through 5 successively specific rungs (or types) of strategy. By adapting to and reflecting the influence of the first four rungs, the top-most national HLS strategy can maximize its potential for success in ways that otherwise might not be possible.

Keywords: Homeland Security, Southeast Europe, Strategy Pyramid, Civil-Military Combination Strategies, US Global Strategy, Regional Strategies, US-Europe Security Issues.

Introduction and General Framework

To most observers, Homeland Security (HLS) encompasses the combined efforts of government agencies, non-government organizations, and the private sector to protect a nation-state against violent attacks. If attempts at protection fail, HLS then focuses on the management of and the response to such attacks. This generic, two-part definition of Homeland Security may be accurate enough, but it should not obscure an additional truth – definitions of HLS invariably fluctuate by country and by region.

In Eastern and Southeastern Europe, those who try to define HLS inevitably confront a series of difficult questions. How narrowly should one define Homeland Security?

Should it remain the primary responsibility of Ministries of Defense? Within those ministries and/or others, what level of influence and oversight should civilians have over their uniformed colleagues? And perhaps most importantly, should security establishments attempt to provide a "full menu" of HLS capabilities, even if the attempt itself dilutes (and perhaps even dooms) their effectiveness? These are not trivial questions in a part of the world where significant portions of the military establishment continue to insist on preserving their institutional autonomy from the "interference" of what they see as civilian "amateurs."

The interrelated reasons for this backwards-looking and military-dominated attitude towards security include the following.

- 19th and 20th century concepts of military professionalism, which encouraged officers to believe that national defense is the exclusive responsibility of "scientific" experts.
- A less philosophically supportable desire to preserve institutional freedoms and prerogatives, if not outright bureaucratic self-survival.
- A lingering suspicion of post-Cold War security sector reforms (and Western-driven reforms in particular), which appear to demand that military leaders jettison the doctrines and practices that once defined their professional lives.
- An unwillingness to commodify military thought – i.e., an unwillingness to treat strategy and doctrine development as an entrepreneurial activity where different concepts collide and compete with each other in a free marketplace of ideas, and thereby help determine which options are best suited for the future.

The above reactions, although understandably human, remain Sisyphus-like in their futility. The great "No" they represent provides only a meager defense against what is the overarching theme of this article – *the era of exclusively national defense in Greater Europe is over, as is the era of narrowly designed national defense strategies*. Slowly but inevitably, all security strategies in the area, including Homeland Security strategies, will have to become "layered" if they are to account for the growing security roles of multiple actors operating on multiple levels. Figure 1 not only represents what this strategic layering means in practical terms, it also provides a user-friendly template for future Homeland Security strategy development at the national level.

If strategy developers decide to use the Pyramid Model presented in Figure 1 to create HLS-centered security strategies that are as reality-inclusive as possible, they will first have to start from the bottom up – i.e., they will have to work from the broad to the specific. Additionally, they will have to assume that only a minority of security strategies will be strictly military in the future. The majority of them, including HLS

Figure 1: The Pyramid of Strategy Development.

strategies, will actually involve a combination of military and non-military means, but to a degree that is historically unprecedented. (See the discussion of Combination Strategies later in this article.)

Second, the Pyramid Model requires planners to craft strategies that at least minimally account for America's security interests in their part of the world. No devotee of a robust European Security and Defense Policy can ignore the following existential facts – 1) for the foreseeable future the United States will remain a military colossus unequaled by any other military power, alliance, or union in the world; 2) this unipolar military power has growing strategic interests in NATO's rimlands, including the Wider Black Sea Area, and 3) virtually all of NATO's newest members are loath to spurn the security protections provided by the United States for those promised, at some theoretical point in the future, by politically motivated European Union (EU) members (especially France) who want to curtail America's security role in a Greater Europe. Given these facts, national and HLS-level strategies must account for local American interests, even if cursorily, if they are to be effective.

They must also account for a third level of strategic activity – a multi-organizational level that will only grow in importance over time. If the UN will not bring added "hard" power to the security table anytime soon, its "soft" power capabilities will

certainly remain in place, as will those of the OSCE. NATO and the EU, in turn, will continue to add to their hard and soft power capabilities, and will almost certainly attempt to "proliferate" them through other organizational means – for example, through a revitalized Maghreb Arab Union, or the (Persian) Gulf Cooperation Council, or a Wider Black Sea Security Cooperation Group, etc. The exact composition of these transnational overlays is not the issue here. What is the issue is that neither organizations like NATO nor individual states like Bulgaria can rely solely on inward-looking strategy development processes in the future. These processes will have to adapt to hybrid civil-military strategies, they will have to consider the interests of a dominant unipolar military power, and they will have to reconcile themselves with security strategies developed (and operating) across inter-organizational lines. In short, Homeland Security strategies created at the national level cannot ignore this layered or Pyramidal approach if they hope to be effective. The attention they pay to each level of the Strategy Pyramid may wax and wane depending on the circumstances, but strategic incoherence will be the price they pay for ignoring any rung along the way.

The fourth and next rung of the Strategy Pyramid requires planners not only to consider the mutual impact of regional inter-organizational strategies on their work, but also the impact of *intra*-organizational strategies. In terms of HLS, this unavoidable step means accounting for intra-NATO and intra-EU concepts of operations, organizational schemes, capabilities, etc. With a firm grasp of Alliance and Union-level crisis management practices in hand, for example, the local strategist can finally climb to the top of the Strategy Pyramid and develop national-level and/or HLS-centered strategies that rest on the firm conceptual foundations provided by the four rungs below them.

In closing this section, it is appropriate to restate that Figure 1 is nothing if not a multi-dimensional template for developing security strategies now and in the future. It provides a comprehensive approach that begins by deliberately orchestrating civilian and military security practices together, and then focuses on increasingly narrow multi-regional, inter-organizational, and intra-organizational strategies. These increasingly narrow foci then shape the final creation of Homeland Security strategies that are not "tone deaf" at the nation-state level. In order to illustrate just how this approach works, this article will now turn to highlighting several rungs of the Strategic Pyramid in greater detail.

The First Rung of Strategy – Civil-Military Combination Strategies

To describe this foundational level of strategy development properly, it is important to accomplish two tasks – 1) trace briefly how the global strategic environment has changed, and thereby explain why civil-military combination strategies are necessary;

and 2) provide an example of this type of strategy that planners might want to use in their development of specific HLS options.

A Paradigm Shift in the Strategic Environment

When discussing broad strategic environments, there is the "then" of the Cold War and the early-to-mid-1990s, and the "now" of today. Changing demographic and migration patterns, ethnic and religious tensions, environmental degradation, the instability exported by failing or failed states, and increased weapons proliferation are only a few of the problems that have exacerbated the differences between "then and now" security, as has post-9/11 transnational terrorism. But since "now" security has readily identifiable features, it permits the development of general axioms. And since these axioms provide the conceptual foundations for *all* forms of strategy development (including HLS strategies), it is worthwhile to highlight some of them here.

- *First:* Globalization is both a boundary broadening and boundary weakening process. In other words, internal and external threats are increasingly becoming indistinguishable from each other and interchangeable with each other.
- *Second:* We live in a unipolar world militarily (dominated by the United States), a multipolar world economically (dominated by the US, Europe, Japan, and increasingly China and India), and a transnational world (dominated by international/regional organizations, non-government actors, and multinational corporations that increasingly limit what nation-states can do in terms of their own security.) These parallel and yet overlapping worlds represent a "variable geometry" that all HLS planners must account for in their work.
- *Third:* The concepts of transnational and human security have seriously trumped traditional concepts of national defense, especially in Western Europe. Consequently, what was once seen as the narrow and exclusive domain of Ministries of Defense is now seen as the responsibility of multiple organizations and agencies, both official and unofficial. This broadening of security as a concept and as a responsibility is not necessarily a bad thing – it represents its "debelicization" and therefore provides an opportunity for more sophisticated and multifaceted responses to today's threats (see below).
- *Fourth:* The sources of conflict today are "rational" and "irrational" – i.e., they involve traditional political cost/risk calculations and emotional acts of negation. Given this duality, HLS strategies must concentrate both on prevention and consequence management in order to be effective.
- *Fifth:* Nation-states have forever lost their monopoly on generating and using mass-effects violence. In other words, politically motivated violence has been

"privatized" into the hands of sub-state or non-state actors. As a result, this type of violence is appearing in human domains historically protected (at least partially) from the ravages of armed attacks.

- *Sixth:* Given the above trends, one can say that security institutions today have to cope with a security space that is everywhere and yet nowhere. Their opponent is now an abstraction (the "spectrum of conflict") rather than a specific, readily identifiable foe. And the "combatants" they face, many of whom are civilians, are networked, modular, borderless, transnational, ephemeral, and asymmetrical.
- *Seventh:* As a result of the above changes, using balanced or symmetrical means against others can now be inherently self-defeating. Instead, it is better to use flexible civil-military strategies (including their hybrid means) to obtain desired effects. But what would one of these types of strategies look like, especially given their importance in the first rung of the Strategy Pyramid?

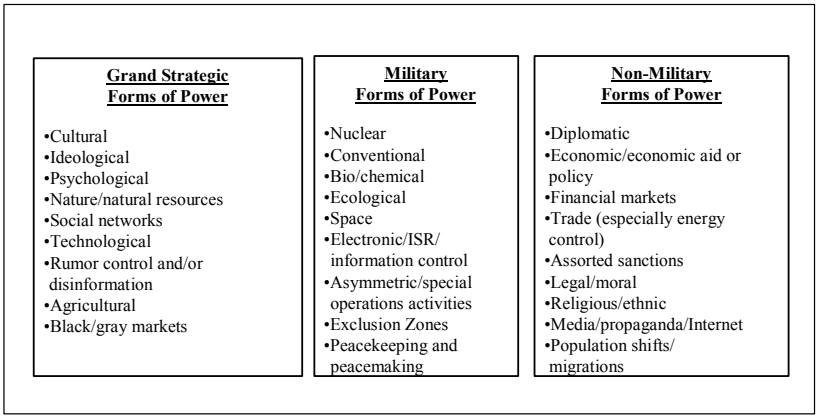
Civil-Military Combination Strategies – One Possible Example

Because they emphasize the interconnectedness of threats (from terrorism, to civil wars, to extreme poverty), civil-military combination strategies are naturally broad and comprehensive in their approach. For these strategies to work effectively, however, the institutions that use them must overcome their own parochialism and learn to work *across* broad organizational and conceptual lines. They must also understand that when they speak of using *all* available sources of national power, particularly for homeland security, they should not mean just using political, economic, military, and informational forms of power, which is usually the case. As Figure 2 illustrates, in civil-military combination strategies there are at least 27 forms of power one can use, either offensively or defensively, on an interchangeable or "horizontal" basis.[2] It is these numerous forms of power (and more) that should provide the foundation for today's Homeland Security strategies and not the limited options used in the past.

The forms of power in Figure 2 may or may not be already familiar, but what is certainly new is the potential ability of HLS planners, while working with multiple agencies and/or organizations, to mix and match them in unprecedented ways. But how does the above template actually work, one might ask? Basically, it works through bundling – i.e., to defeat or de-fang shadowy or traditional threats, those who practice civil-military combination strategies should mix and match the listed forms of power as necessary. The latter are basically "LEGO pieces" that planners can use to construct any type of HLS strategy that they see fit. Additionally, the level of emphasis given to each LEGO piece could (and should) change as circumstances demand. A particular combination of pieces may be vital in a counter- or anti-terror campaign for X amount of time, but their importance may wane given new circumstances. There-

A Security–Centered, Non–Compartmentalized Combination Strategy

You have political, economic, military, and informational forms of power that you can use, but you should use additional forms of power as well



"A better means used alone will not prevail over multiple means used together"

Figure 2: Forms of Power in Civil-Military Combination Strategies.

fore, as the situation changes, so should the pieces of the "jigsaw puzzle" or "mosaic" that make up civil-military combination strategies, and so should the relative weight of the pieces themselves. This approach would go far beyond current notions of integrated planning and use national strengths much more precisely, widely, and economically. In fact, by adopting civil-military combination strategies, security-minded nations would be able to 1) encourage inter-agency cooperation, 2) rely on a variety of pre-existing strengths, 3) avoid having to maintain full-service militaries (the bundling of different forms of power would obviate the need for that), 4) improve their security sectors in potentially low technology ways, and 5) save money (because of the efficiencies provided by the first four options).

But what about working within the 27 forms of power themselves? What HLS-friendly templates might be useful there? As illustrated in Figure 3, one possible approach is to develop assorted prevention, protection, and response options against non-state international adversaries, nation-state adversaries, and domestic foes. With this template in hand, the HLS planner would not only have a civil-military combination strategy to shape his or her planning, but also a methodical way to develop different forms of individual power. The planner's ability to operate within the first rung of the Pyramid of Strategy would thus be complete.

HLS—Working Within the Forms of Power

Homeland Security Components	Homeland Security Threat Environment							
	Non-state International Adversaries		Nation-State Adversaries			Domestic		
	Terrorism	Drug Trafficking	Terrorism	Drug Trafficking	Military Attack	Terrorism	Civil Disturbances	Natural Disasters
Overall	Command and Control							
	Planning							
	Training							
Prevention	Border Control							
	Intelligence Collection, Analysis and Dissemination							
	Diplomacy/Shaping							
	Cooperative Engagement with Domestic Law Enforcement Agencies					Cooperative Engagement with Domestic Law Enforcement Agencies		
	Community-based Anti-drug Programs		Community-based Anti-drug Programs					
	Arms Control and Non-proliferation							
Protection	Cooperative Engagement with Domestic Law Enforcement Agencies				Cooperative Engagement with Domestic Law Enforcement Agencies			
					National Missile Defense			
	Air Sovereignty							
	Countering Foreign Intelligence Collection							
	Critical Infrastructure Protection							
	Cyber Security/Computer Network Defense							
Response	Consequence Management							
	Support to Continuity of Government Operations							
	Crisis Management							
	Cooperative Engagement with Domestic Law Enforcement Agencies					Cooperative Engagement with Domestic Law Enforcement Agencies		

Figure 3: HLS – Working within the Forms of Power.

The Second Rung of Strategy – Accounting for a Global US Strategy in the Wider Black Sea Area

If we assume that 1) today's external and internal threats are increasingly interchangeable, and 2) American security interests will continue to grow in the Wider Black Sea Area rather than diminish, then the HLS strategies developed in that part of the world should not be exclusively local in character. Instead, the strategies must account for the interests and preferences of outside actors, even if only cursorily. In practical terms, this means the United States and regional political-military organizations like NATO and the EU. In the case of the US, there are two major points HLS planners need to remember.

First: Unlike NATO or the EU, the US has global interests rather than broadly regional ones. These wider interests might inspire it to make what appear to be eccentric or abrupt decisions, at least when seen from a regional or sub-regional perspective. What if, for example, the US chooses to take the following steps in the future?

- Redoubles its efforts to transform the Middle East and tie it to the global economy.

- Actively attempts to reunify Korea and promote internal Iranian reforms.
- Rejects (or accepts) the emergence of China as a geopolitical equal.
- Attempts to create other "NATOs" in other parts of the world.
- Attempts to link these "NATOs" together into a wider security network.
- Significantly expands its geopolitical and economic activities in Central Asia, Africa, etc.
- Formally federates itself with other states in the Western Hemisphere and/or elsewhere.
- Attempts to develop an alternative or parallel organization to the UN (made up of democratic nations, for example).

The above possibilities are admittedly speculative and even fanciful. However, they illustrate that the logic of a global actor is distinctly different from the logic of a regional one. And if that actor has interests in a Greater Black Sea, no local HLS strategy can ignore the potentially helpful or disruptive effects of that actor's policies and/or behavior. That is why effective HLS strategies need to account for and build upon the first two rungs of the Strategy Pyramid.

Second: Nations in the Wider Black Sea Area may have to factor in US preferences into their HLS strategies, but 1) they are part of greater Europe, 2) a number of them aspire to NATO and/or EU membership, and 3) a militant minority in the EU want to substitute their security umbrella for that provided by the US (and they want to do it sooner than later). Whether the latter desire is politically mature or not is not what matters here. What does matter is that HLS planners must premeditatedly (and therefore effectively) balance the security imperatives represented by the second rung of the Strategy Pyramid with the imperatives represented by the third and primarily fourth rungs. More specifically, the planners should account for at least six security-related stress points between the US and specific NATO-EU members at this time.

- The role of morality in foreign policy – When compared to their European counterparts, American administrations are more comfortable with the need for and the possibility of moral judgment in world affairs. As far as the Americans are concerned, different circumstances may require different methods, but they do not justify different morals. In turn, conflict is not merely attributable to miscommunication, inadequate education, or justified rebellion against unjust circumstances, as transatlantic progressives have long argued. It is also attributable to the very structure of the international system and to diseased political cultures that should be condemned for what they are. Because of their tragic common history, European governments often disagree with this doctrinaire moral view (as they see it).

- The role of universal values – American leaders rightfully tout the importance of human dignity and democratic values. However, they also assume that these values, as expressed by the US, are universal and transportable – i.e., that they can work everywhere and that they should be spread as far as possible. Once again, European elites are less sanguine about universal values – they doubt their actual universality, their transportability, and their naturally assumed connection with democratic politics.
- Thwarting peer competitors – The current American *National Security Strategy* argues that the US needs to prevent the rise of a peer military competitor. The unselfconscious assumption behind this belief is that America uses its hard power benignly and in balanced ways. In other words, by maintaining its national selfishness *and* selflessness in rough equilibrium, it blends power and principle together. Critics quarrel with these beliefs, which they argue lead to ambiguous reactions to ESDP and other beneficial forms of European burden sharing.
- The War on Terror – The current American government believes that they are at war with international terrorists and the largely theological program they represent. The terrorists are therefore not criminals. They are 1) shadow warriors, 2) irregular troops warring against perceived apostates and infidels, and 3) indifferent to enhancing their power within the existing international system (they actually want to replace the system outright). In contrast, there are transatlantic critics who claim that the war against terror is a self-perpetuating fiction. To characterize on-going counter- and anti-terror activities as a war runs the risk of 1) needlessly militarizing anyone's foreign and domestic policies, 2) fixating on the symptoms of terror rather than on its sources, and 3) undervaluing alternative legal or law enforcement options that are still appropriate and available.
- The roots of terror – What causes international terrorism? According to the current American *National Security Strategy*, anti-Western terror is not necessarily a product of poverty or even injustice. Instead, it is a product of political oppression – of authoritarianism and despotism. If you want to solve this particular problem then, you need to solve it through democratization. Critics may or may not agree with this particular solution for terrorism, but they do agree that it is insufficient. Terrorism has multiple causes, they argue, including the very ones the *National Security Strategy* rejects.
- The need for proactive/anticipatory defense (including preemption) – Since it believes time is not on the side of those who merely react to catastrophic attacks, the current US administration claims the historical right to anticipatory or proactive self-defense. In doing so, however, it has mixed the traditional

> definition of *prevention* with a nontraditional definition of *preemption*, which now claims that a history of hostile behavior, the ownership of certain capabilities, and the pursuit of destabilizing objectives can constitute an "imminent" threat by others. This looser, with-doubts standard for proactive defense is at odds with those who want to preserve the traditional (and stricter) one, which they consider far less destabilizing.

To summarize then, there are still a myriad number of commonalities between the US and its European allies on security matters. But as the above examples illustrate, there are also points of friction that planners in the Wider Black Sea Area (and elsewhere) need to consider. Furthermore, they need to de-conflict these points of friction as much as possible, especially when they build pyramidal HLS strategies that account for America's singular global power on the one hand and alternative regional models on the other (including ESDP).

The Fourth Rung – Regional Security Strategies

It is appropriate to skip over a discussion of multi-organizational strategies here (the third rung of the Pyramid of Strategy) because of their conceptual immaturity and lack of definition at this point in history. When speaking of the fourth rung, however, there are two brief but important points to make.

First: When HLS planners in Europe attempt to harmonize regional security strategies with local strategy-building processes, they are basically trying to harmonize their efforts with NATO and EU strategies. However, since ESDP remains a work in progress, the primary strategy-building requirement vis-à-vis the EU is studied vigilance. In the case of NATO, however, the requirement is to remember that it is no longer just a mutual defense alliance. Instead, through a relentless process of role diffusion over the last 10-15 years, NATO is now a collective security organization, a political alliance, a preventive diplomacy instrument, a builder of civil societies, a democratization tool, a protector and partner for non-ethnically-based governments in the Balkans, an intervention tool, a "housekeeping device" for a largely stable continent, a counter- and anti-terrorism tool, a regional organization with an increasing area of responsibility, an important part of growing transnational "interlocking dimensions," a laboratory for military transformation, and so much more. Any attempt to accommodate local HLS strategies with NATO's Strategic Concept and Strategic Vision must note just what a "multi-foliate rose" the Alliance has actually become.

Second: This article has repeatedly referred to a Wider Black Sea Area (WBSA), but this admittedly artificial geopolitical construct is a work in progress (and an immature one at that). HLS planners in Southeast Europe must not only take note of it, they perhaps need to help define and institutionalize it too. Otherwise, alternative regional

and sub-regional geopolitical models might compete with the WBSA as a concept, crowd it out, and leave local planners with follow-on regional strategies that are difficult to reconcile with their own. Some of these alternative models include Sir Halford Mackinder's indestructible Heartland Model, political Islam's Transnational Caliphate Model, the Greater Danube Basin Concept, a New Hapsburg League Concept, the Greater Middle East Concept, and more. Again, since none of these alternatives may be better than the Wider Black Sea Area Concept itself, the fourth rung of the Strategy Pyramid is one place where Southeast European planners may not merely adapt, orchestrate, and/or reconcile different strategies with each other, but proactively shape the regional context for the fifth and final rung of the Pyramid – National (HLS) strategies.

The Fifth Rung – National Security Strategies (with an Emphasis on HLS)

As Figure 4 illustrates, Homeland Security is indeed an amorphous challenge. It has international and domestic components, it focuses on broader security and narrower defense issues, and it includes specific problems that traverse all boundaries.

HLS's intrinsic amorphousness also means that one-size-fits-all Homeland Security strategies are not realistic. Local conditions demand local strategies (influenced and adjusted by the above four rungs, however). Having said that, there are generic preparatory steps that all HLS planners can take to populate their national HLS strategies properly. These steps would naturally involve a multi-agency process (remember our discussion in the first rung) and could include the following:

- Conduct vulnerability analyses.
- Develop remedial plans.
- Create warning centers.
- Develop a response system.
- Develop a reconstitution system.
- Develop education and awareness programs.
- Pursue research and development.
- Enhance intelligence collection and analysis activities.
- Pursue international cooperation.
- And establish legislative and budgetary requirements.

With these broad preparatory steps accomplished, the local HLS planner could then focus on specific Ministry of Defense-oriented activities in order to populate their HLS strategies even further. These activities could include the following.

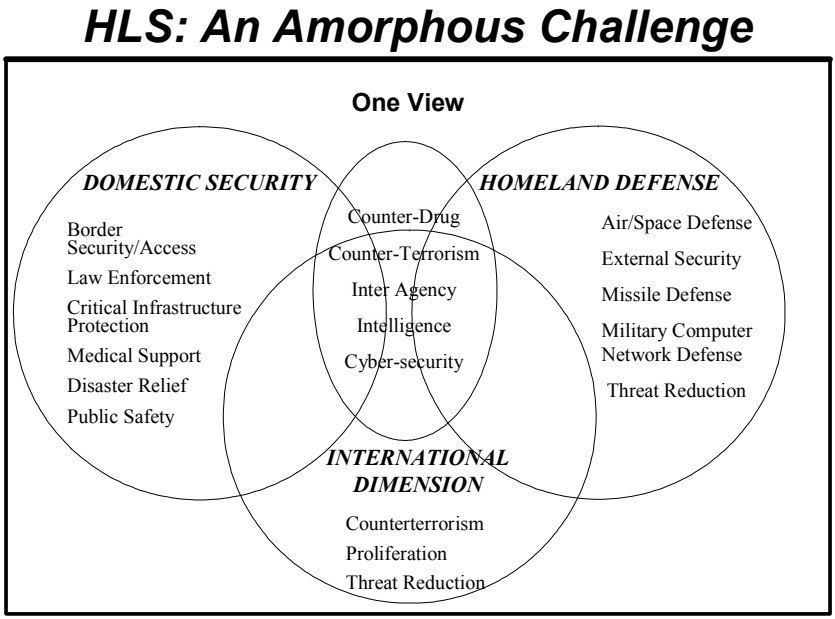


Figure 4: Homeland Security as an Amorphous Challenge.

- Detection, surveillance, and intelligence.
- Plans, training, exercises, evaluation.
- Law enforcement and investigation.
- Weapons of Mass Destruction (WMD) consequence management.
- Key asset, border, territorial waters, and airspace security.
- Domestic transportation security.
- Research and development.
- Medical and public health preparedness.
- Domestic threat response and incident management.
- Economic consequence management (cost sharing).
- Public affairs.

The above basic steps may be generic, but they are also widely applicable. They also close the conceptual loop of this article. After all, the fundamental point of the article is that for HLS strategies to be successful they cannot be insular – i.e., in terms of strategy, they have to work from the broad to the specific; they have to rely on LEGO-like civil-military combination strategies; they have to account for the poten-

tially helpful or disruptive military power of the United States; they then have to account for the strategic orientations found between and within transnational organizations; and they need to do all this while remaining responsive at the national level. In short, HLS strategies need to be three-dimensional, which is why a Pyramidal approach to strategy may be an HLS planner's best friend.

Notes:

[1] The views expressed by the author of this article are solely his own and should not be attributed to any governmental institution or political entity.

[2] For a military-centric discussion of this concept, see James Callard and Peter Faber, "An Emerging Synthesis for a New Way of War: Combination Warfare and Future Innovation," *Georgetown Journal of International Affairs* III, no. 1 (Winter/Spring 2002): 61-68.

PETER FABER is a faculty member and researcher at the National War College, National Defense University, Washington, D.C. From 2002-2005 he was a Research Associate at the NATO Defense College, Rome, Italy. He holds 5 advanced degrees and his main research interests are theory and strategy development, military transformation, and Euro-Atlantic relations. *E-mail:* faberp@ndu.edu.

A BRIEF ON EMBEDDED SOCIETAL SECURITY

Bengt SUNDELIUS

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

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

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

There is a paradigmatic shift in Europe from the national defence systems of the Cold War to the evolving notion of *embedded societal security*. The member states of the EU are developing novel practices for dealing with security challenges from abroad,

at home and not least *within its intermestic sphere.* The latter domain becomes a primary playing field for the pursuit of embedded societal security in and by the Union. Several types of actor-focused and structurally-based threats can be faced in Europe in the foreseeable future. These developments will affect both the security challenges faced and our abilities to meet them in effective and legitimate ways.

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

Security Challenges Ahead

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

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

Europe has a legacy of violent terrorist attacks going back to the days of the multinational empires of Russia, Austria-Hungary, and Germany. In the 1960s, and particularly in the 1970s, a number of terrorist attacks were again experienced on this conti-

nent, including in Sweden.[1] In the United Kingdom, Spain and France terrorist bombings occur at regular intervals.[2] In many ways, armed attacks by "another" manifest traditional challenges to national and international security. This form of violent protest against the established political order will be with us for a long time.

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

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

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

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

This challenge can be illustrated with two threatening types. The first is a collapse of neighbouring systems, where nobody is at fault in a direct sense. There is no culprit. There is no evil Other.[5] A nuclear plant is destroyed through malfunctions. Something serious goes wrong in Chernobyl or in Ignalina. Energy shortfalls or power blackouts, they just happen and they are with serious safety consequences. Deadly epidemics of

various kinds may brake out and spread quickly. Consequences are often widespread and deadly like in violent attacks by some Other.

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

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

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

Trends Affecting Embedded Societal Security

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

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

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

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

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

Naturally, antagonists wishing to inflict harm upon a society have interests in finding the critical points, where various infrastructures connect. A major task in planning for societal security is to transform potential vulnerabilities linked to this technological

complexity into high reliability systems.[12] This is an open-ended process involving many societal sectors and numerous government agencies. It cannot be accomplished without the active participation of those that actually own and control most of these infrastructure networks, i.e. the private business sector.

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

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

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

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

care often rise very quickly.[18] Cascading effects evolve in uncontrollable ways when some dormant risk contingency suddenly becomes a reality.

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

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

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

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

Public expectations of government performance remain high in the face of a wide spectrum of threats to state security and to individual safety. At the same time, the

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

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

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

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

It is important to build knowledge about societal security in all EU countries, as an analytical underpinning for the implementation of the Solidarity Clause. New requirements are levied on think-tanks to develop such knowledge in partnership with

policy agencies and operatives. One needs knowledge about security threats and strategies that is both based on scientific research and on practical experience. Such centres of knowledge production and transfer need to be linked in trans-national and co-operative networks. This knowledge-building enterprise should extend across the Atlantic as well as to other global centres.

Domains of Societal Security

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

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

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

Figure 1: Concepts and Domains of European Security.

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

focus of the defence sector. In both tracks, collaboration with partners or allies abroad is well developed.

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

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

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

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

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

In Figure 3 an additional EU domain is added in between the domestic sphere and the international setting. In the *intermestic sphere*, the necessary trans-boundary linkages across the domestic and the international levels are highlighted. Drawing on the discussion of trends affecting embedded societal security in the previous section, it is

clear that this intermestic sphere is an important security domain for the Union. Its importance is symbolized in the Solidarity Clause of the proposed Constitution. In this statement of a common political commitment to embedded societal security, both a concern with state security and the requirements of human safety are included. The solidarity pledge cuts across these distinct professional tracks and it fuses the domestic-international nexus. The intermestic domain becomes a primary playing field for the pursuit of societal security in and by the Union.

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

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

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

Toward Embedded Societal Security across the Atlantic

Yet, preparations for European societal security cannot be conducted in splendid isolation. This demanding collaborative effort must be multi-continental in approach in order to be effective. The societal security paradigm must bridge across the Atlantic to the USA, as well as to other global partners. Steps can be taken to transform the existing, alliance based Atlantic security community into a secure trans-Atlantic So-

cietal Security Community. The question remains how to link the novel European notion of embedded societal security with the US Homeland Security program?

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

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

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

One cost effective means to open up entrenched rigidities would be to plan and execute several interactive training workshops. Responsible policy makers and elected officials from several nations would in workshop settings deal intensively with some scenario-based trans-Atlantic threat situation. A shared contingency awareness and a

mutual learning process would develop through such experiences with concrete decisional security dilemmas. An excellent example of such learning tool was the *Atlantic Storm* simulation that was conducted in Washington on January 14, 2005. The scenario-based game engaged prominent former statesmen and active policy shapers from a sample of European governments and from North America. The lessons learned from this exercise were widely noted in media.[27] The format was tested in March by members of the new House Homeland Security Committee of the US Congress. Similar multilateral workshops ought to be convened in Europe.

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

Notes:

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

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

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

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

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

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

[7] Paul 't Hart "Symbols, Rituals and Power: The Lost Dimensions of Crisis Management," *Journal of Contingencies and Crisis Management* 1, no. 1 (1993): 36-50.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Perceptions and Approaches

- Is Neutrality an Appropriate Instrument for Domestic Security? A European Perspective
- Homeland Security and the Russian Approach
- The Growing Threat: Homeland Security Issues of Bulgaria
- Civil Security: Architectural Approach in Emergency Management Transformation

IS NEUTRALITY AN APPROPRIATE INSTRUMENT FOR DOMESTIC SECURITY? A EUROPEAN PERSPECTIVE

Christian LANZ

Abstract: Can the Law of Neutrality, as still practised by various countries in Europe today, still prevent or protect from a war or a conflict? How compatible, if at all, is neutrality with affiliation to supranational organisations, e.g. the UN or the European Union and other international security organisations and agreements, and finally, can it contribute to domestic security? Even if the TV station Al-Jazeera broadcasted excerpts of a videotape of Osama Bin Laden addressing the American people by quoting: (…) "Let him (President Bush) tell us why we did not strike Sweden, for example." (…) we have to look at features, relevance and history of neutrality and at today's actual security situation. The analysis of the European security situation reveals a manifold range of threats and risks, which has developed particularly through the creeping dissolution of the monopoly of national power, e.g. unresolved conflicts in the South-Eastern flank of Europe, the phenomenon of organised crime trying to integrate itself into the economic operation, the constantly growing willingness of terrorists to commit suicide attacks, the spread of WMD, etc. It can be noted that the danger of conventional military threats has clearly diminished. It is, however, evident that the new conflict potential and its forms are characterised by ethical, religious and also economically motivated actors (usually non-governmental) and that they considerably affect the safety environment of Europe. So a question must be asked, to what extent neutrality is still of use in such an environment.

Keywords: Law of Neutrality, Hague Conventions, Charter of the United Nations, Prohibition of War, Integration of the European States, Creeping Dissolution of the Monopoly of National Power, Blurring Borders between External and Internal Security, Networking.

The term "neutrality" is defined by the international community as non-participation in armed conflicts between other states. A distinction must be made, however, between the Law of Neutrality and the policy of neutrality.

The Law of Neutrality is that area of International Law containing those provisions which neutral states have to observe in times of international armed conflict and to which the parties of the conflict must adhere in the same context. For the most part, these concern the right of the neutral states to be left undisturbed during such conflicts and their obligations of impartiality and non-participation. In practice, such obligations do not interfere greatly with the freedom of action of neutral states. The sources of the international Law of Neutrality are customary International Law on one hand and the 1907 neutrality agreements of The Hague on the other.

The policy of neutrality concerns all measures that a neutral state decides to adopt of its own free will, above and beyond its legal obligations, so as to ensure the credibility and effectiveness of its neutrality. Neutrality policy is flexible enough to adapt to each case, taking into account the foreign and security policy situation of the day.[1]

Can the Law of Neutrality—as still practised by various countries in Europe today, among others Switzerland, Finland, Austria and Sweden—still prevent or protect from a war or a conflict? How compatible, if at all, is neutrality with affiliation to supranational organisations, e.g. the UN or the European Union and other international security organisations and agreements?

The increasing interdependence of trade, economics, and, above all, information (globalisation) present a further challenge for neutrality as the existence of a society or even a state can increasingly be threatened by more than foreign armed forces alone. Europe, in particular, currently faces no direct military threat any more. Of course the question arises here too, what or whether neutrality can contribute to domestic security. Therefore, the neutrality question will have to be judged with particular regard to the risks and dangers facing Europe. These are the central questions to be discussed in this article.

Features and Relevance of Neutrality

The right of neutrality contains those regulations of International Law that must be considered by states in the event of international armed conflict. The general regulations of the Law of Neutrality were contractually codified (land and naval warfare) in 1907 at the Hague Peace Conference. Until today, there have been no further written additions to this Law of Neutrality; it has only been augmented and extended by unwritten International Law. The Law of Neutrality is only applicable to inter-governmental conflicts, not however to internal conflicts or civil wars. The neutrality right is also not applicable if the United Nations takes action to preserve international peace and security, for example when a state has violated the Charter of the United Nations. So the right of neutrality can principally not be applied to coercive measures of the UN due to the fact that according to The Hague Conventions [2] a conflict between the

UN and a lawbreaker does not constitute a military conflict between states. Consequently, one could also say that with the Charter of the United Nations neutrality no longer exists since the Charter foresees no neutrality at all, as war is principally prohibited and peace is regarded as the normal condition.

A short review of history must be made to better comprehend the nature of neutrality. The international policies of the years 1648 to 1900 can be also designated as the "Westphalia order," since certain aspects of that policy were upheld more or less continuously. Three of these components are thereby of special importance:

1. The neighbourhood of sovereign and independent national states;
2. The acceptance of war as instrument for regulating conflicts, thus no general prohibition of war;
3. Tolerance of non-involvement in wars.

These components are no longer compatible with today's order since after the two totalitarian World Wars a complete reorientation of the international order developed. From there on, wars were no longer accepted as legal means for resolving a conflict, with the exception of the coercive measures already mentioned in the context of the United Nations and the more or less clearly defined right of self-defence. So, we can conclude that neutrality in the classical sense had already lost its legal basis after 1945.[3] For the first time, the conditions between the European states were no longer determined by war, but through cooperation and collaboration.

Apart from the obligations of neutral states, it remains to be mentioned that the neutral states still have rights.[4] If it is embroiled in a war, the neutral state is allowed to join alliances or make use of foreign military support. Neutrality obligations become obsolete, if neutrality fails to fulfil its function. Here, however, the question arises, for how long war preparations (today: threats of terror?) of a foreign power, for example, must be tolerated, even when these are also directed against a neutral state without affecting its territorial sovereignty. Which preparations or cooperation arrangements can be made by the neutral state in times of peace without compromising state's neutral status?

Since the end of the Cold War, there have been interventions not only in international conflicts, but also in cases of humanitarian disasters or severe violations of human rights, such as these in former Yugoslavia, Somalia, Kosovo, etc. This results in the fact that even states no longer enjoy unlimited sovereignty and that they can very well forfeit their sovereignty if they are universally seen to violate International Law. This universal view of right and injustice, however, is of greatest importance for the success of such an intervention. The partly independently conducted pre-emptive strikes [5] of the United States of America (USA), particularly in the case of the Iraq

intervention in the aftermath of 9-11, demonstrated an even greater restriction in the sovereignty of a state. A universal consensus that Iraq had committed a breach of law did not exist as many states like France, Germany, China and Russia among others did not support the view of the United States. States involved in the intervention and in the subsequent pacification of Iraq, such as Spain and Italy, have already painfully had to find out what it means to have participated in an action that was not legitimised by International Law or was only legitimised later (abduction of citizens and assassinations some of which were even carried out in the home country). States not participating in this war, i.e. those European countries that remained neutral, so far have been spared attacks and encroachments (see also next section on this). *At the present time, we may thus say that a certain degree of restraint or in other words taking a clearly neutral stance during a military dispute can certainly produce some security.*[6]

However, the question must be posed, to what degree a state can remain neutral in the face of today's security policy integration.

Tolerance towards neutral states has, however, clearly diminished with the creeping dissolution of proper national states in Europe. Besides the UN and NATO, the European Union has also constantly developed further with regard to its Common Security Policy. Hardly any other region of the world knows such a high degree of integration and organisation between states. This is not only the case in the field of security but also in the economic sector with the European Union, European Fair Trade Association (EFTA), Organisation for Economic Cooperation and Development (OECD), etc.[7] A central goal of the European Security and Defence Policy (ESDP) is to strengthen the Union's ability to act as an entity at the international level by establishing civilian and military capacities for conflict prevention and crisis management. The ESDP forms a part of the Common Foreign and Security Policy of the European Union and functions according to the principle of inter-governmental cooperation. With the 2004 Headline Goals passed by the European Council in July 2010, the creation of such crisis management capacities enters a new phase. Already by 2007, an intervention capability is to be established with 13 planned rapidly deployable units.[8] The operational readiness of the ESDP has already been demonstrated with the conduct of several civilian and military operations. The first began on 1 January 2003, when the European Union Police Mission of 500 officers took over in Bosnia-Herzegovina from the UN's International Police Task Force. The mission, which will remain for a period of three years, is training local police officers and establishing sustainable policing arrangements in line with European standards and practice. The second operation followed later in 2003, when a small NATO force in Macedonia was replaced first by an EU military force, and subsequently by a 200-strong EU police mission, which is still in place. The largest of the three started in December 2004, when an EU military force (EUFOR) took over from the previous NATO-led Security

Force (SFOR) in Bosnia-Herzegovina. SFOR has been in place since the end of hostilities in 1995. EUFOR has a total of 8,000 troops.[9]

These developments show the increasing integration of the European states and their assumption of responsibility in all areas of crisis and conflict management. The holistic approach of transferring sovereignty and independence to a supranational organisation that is better able to act seems to have found acceptance. *Respective non-involvement (neutrality) indirectly weakens these efforts and will probably meet with little understanding.*

Security Policy Challenges

When examining the practicality of security policy, the definition of political goals must be kept in mind and those threats considered that challenge them. The aims and goals of the European states are, both nationally and in the context of the supranational community, fairly congruent due to quite balanced cultural, political and social homogeneity. Their integration is also becoming more and more intricate through industrialisation, urbanisation and growing international trade.[10] As example the author refers to the goals of the Union enumerated in the preamble of the European Constitution:

> The Union's aim is to promote peace, its values and the well-being of its peoples.
>
> The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, and an internal market where competition is free and undistorted.
>
> The Union shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment. It shall promote scientific and technological advance.
>
> (…) [11]

The analysis of the European security situation reveals a manifold range of threats and risks, which has developed particularly through the creeping dissolution of the monopoly of national power and simultaneous privatisation:

- Yet unresolved conflicts, the instability and the failure to establish a new national order in the south-eastern flank of Europe, in particular in Kosovo. Long-term solutions of the economic, social and socio-political problems in the former Yugoslav area are not apparent yet. The zones, in which military and political instability is latently present, already are or will probably increasingly become opportune retreat areas for clusters of organised crime, war criminals as well as radical Islamic fundamentalists.

- The phenomenon of organised crime, which develops best against a background of reduced national power, economic deterioration (unemployment), poor social climate (isolation of refugees and displaced persons) and also a lack of perspective among young people.[12] Here, organised crime tries to integrate itself into the economic operation of the states through money laundering, corruption and the purchase of company stocks, entire enterprises and real estate. But even the states themselves and their powers are affected as police and jurisdiction may also constitute infiltration targets. According to recent findings, we can also assume that terrorist networks collaborate closely with organised crime syndicates. The past distinction between ideologically motivated terrorists and organisations of organised crime driven by financial greed seems to be fading more and more. The merging of financial greed and terrorist ideology could breed a new dimension of danger to democratic states and systems of collective security and collective defence.[13]
- The spread of weapons of mass destruction is very likely to continue despite all international efforts. Recent examples are North Korea's declaration to possess nuclear weapons, as well as the unveiling of the proliferation network of the Pakistani nuclear scientist Abdul Qadeer Khan. According to official data, Khan, for example, transmitted nuclear modules to Iran.[14] Apart from various nuclear programmes, chemical and biological weapons are also still being developed. The spectre of having no national control over these weapons will therefore probably continue to haunt us.
- The threat of terrorism, as primarily practised by Islamic fundamentalists, has sharply increased over the last years. The USA and/or their citizens all over the world, but also other states that are connected with the USA are most threatened. Various factors are responsible that the terrorist threat has reached to a hitherto unknown dimension: the constantly growing willingness of terrorists to commit suicide attacks, the readiness to cause even a great number of casualties (Madrid, Beslan, Iraq, etc.), the absolute refusal to distinguish between guilty and innocent people and the innovative use of civilian technologies (e.g. car bombs).
- Apart from political, economic and social changes, technological developments may increasingly add to the range of threats. Today, the relevant technological results of research and development come mainly from the private sector and can, therefore, also be all the more easily obtained by non-governmental players. Developments in nano-technology, genetics and biotechnology could cause great changes with implications also for future warfare and conflict management.

- Illegal migration: continuous instability causes a constantly growing flow of emigrants to Europe. Most of them are economic migrants who have no prospect of obtaining a refugee status and thus generate social risks, imbalance on the job market, wage pressure and promote xenophobia among the inhabitants of the host countries.

In summary, it can be noted that the danger of conventional military threats has clearly diminished. It is, however, evident from the enumeration above that the new conflict potential and its forms are characterised by ethical, religious and also economically motivated actors (usually non-governmental) and that they considerably affect the safety environment of Europe. So the question must be asked, to what extent neutrality is still of use in such an environment.

Conclusion and Evaluation

The trends make clear that terms such as internal and foreign security used so far are noticeably merging. *The borders are blurring between domestic security* (*internal security*) *and foreign threats on the one hand and between respective defence, precautionary measures and competencies on the other*. Europe has become a technologically highly advanced, specialised, globally networked and service-oriented society with a highly specialised industry. Already for quite a long time, the borders of the national state no longer correspond to network boundaries or to security areas. Even large distances offer no protection any more. The effects of violent conflicts are rapidly noticeable world-wide. Because of continuous domestic conflicts, this can express itself, for example, in streams of refugees, who rapidly set off crises in neighbouring countries.

If we intend to fight these new risks and dangers as well as their often forgotten causes, it becomes evident that here too, many new areas of cooperation will be necessary. The following areas will primarily have to be dealt with to enhance security:

- National and international interoperability (standardisation);
- Information exchange and common use of information ("from information sharing to information awareness") of the security services (intelligence) and the emergency organisations (first responders);
- Increased and coordinated approach against organised crime syndicates and possibly also operations against small crime by reinforcing police forces and paramilitary forces, e.g. Gendarmerie;
- Protection of critical infrastructures (integration of civilian authorities and their responsibilities) and the population;

- Crisis management, particularly with regard to conflict prevention (cultural dialogue, economic cooperation and integration, privatisation, fight against corruption, etc.);
- Improvement of information (IT) security;
- Increase of the quality of sensor technology, monitoring and identification, particularly with regard to biometrics;
- Last but not least: calming down and reassuring the population. We should inform the public that terrorists are best defeated when people aren't afraid of them.[15]

During the latest international stabilisation operations it has also become evident, that apart from their classical combat missions, the armed forces will also have to increasingly carry out protective and preventive tasks. The result will thus be an increased mixture of military and police tasks. But this is a grey area, as basic legal conditions are still missing or inadequate. The sharp separation between military, political, economic and social resources for resolving conflicts has become increasingly difficult, since all means are inter-dependent in various ways during the different phases of conflict management. Only a continuous, trans-national, inter and intradepartmental dialogue (up to networking) and the resulting joint analysis will guarantee purposeful action in the future, economic use of resources and means as well as effective security provisions.[16]

The concept of integrated (networked) conduct of operations, not only in the military field will probably play a substantial role – whereby the armed forces could well play the role of a pioneer. Attention must be paid to the fact that the extended areas of interest can be agreed upon as a stable field of cooperation. In this respect neutrality is no longer a practicable instrument for achieving these goals, because:

> *Whoever is or wishes to remain neutral in the face of today's security policy challenges and global integration has already taken sides.*

Notes:

[1] <http://www.eda.admin.ch/sub_dipl/e/home/thema/intlaw/neutr.html> (22 June 2005).

[2] <http://en.wikipedia.org/wiki/Hague_Conventions_(1899_and_1907)> (22 June 2005).

[3] Jürg Martin Gabriel, "Die Gegenläufigkeit von Neutralität und Humanitären Interventionen" (Zürich: Center for Security Studies, Swiss Federal Institute of Technology, 1999) <http://e-collection.ethbib.ethz.ch/cgi-bin/show.pl?type=incoll&nr=32> (22 June 2005).

[4] <http://www.vilp.de/Depdf/d198.pdf> (22 June 2005).

[5] See Prof. Dr. Armin A. Steinkamm, "Der "Irak-Krieg:" Eine Herausforderung an das Völkerrecht," *Wissenschaft & Sicherheit* 10 (December 2004), <www.sicherheitspolitik.de/PDFs/WuS_10_2004_Steinkamm.pdf> (24 June 2005). From the military and political point of view, the pre-emptive strike has been considered not to be a fully-legitimised preventive attack. The legal dimensions of pre-emptive and preventive warfare will, however, not to be discussed here.

[6] BBC News, 29 October 2004: Arabic TV station Al-Jazeera broadcasted excerpts of a videotape of Osama Bin Laden addressing the American people: (…) "Let him (President Bush) tell us why we did not strike *Sweden*, for example." (…)

[7] Gabriel, "Die Gegenläufigkeit von Neutralität und Humanitären Interventionen."

[8] Dr. Thomas Hajnoczi, *Europäische Sicherheits- und Verteidigungspolitik* (*ESVP*), Österreichische Gesellschaft für Landesverteidigung und Sicherheitspolitik, Mitteilungsblatt 56 (Wien, 2004).

[9] <http://europa.eu.int/pol/cfsp/overview_en.htm> (24 June 2005).

[10] Kurt R. Spillmann, *Von der bewaffneten Neutralität zur kooperativen Sicherheit*, Bulletin 1995 zur Schweizerischen Sicherheitspolitik (Zürich, 1995).

[11] <http://europa.eu.int/constitution/en/ptoc2_en.htm#a3> (24 June 2005).

[12] Gheorghe Fulga, "Rumänien und die regionale Sicherheit," *Europäische Sicherheit* 4 (April 2005).

[13] IHT, *Terrorists and organized crime join forces*, 25 May 2005.

[14] Reuters, 10 March 2005.

[15] <http://de.wikipedia.org/wiki/Verkehrstote>: according to world-wide collections and estimations about one million (World Bank) up to 1.2 million (WHO 2003) humans die annually at the consequences of traffic accidents. The number of road casualty lies thereby far over victim numbers of war, genocide or terrorism.

[16] Heiko Borchert, "Vernetzte Sicherheitspolitik" (Büro für Sicherheitspolitik, Wien, 2004).

CHRISTIAN LANZ, LTC (GS), was born in July 1971. In 1998, he graduated the Military Academy at the Swiss Federal Institute of Technology Zurich (ETH Zurich) as a Swiss Federal Diploma Professional Officer VBS/ETH. From 1998 until 2001 he was Company Instructor at the Anti Tank Recruit School (Pzaw RS 16/216). Then he was appointed at the Intelligence Directorate, Military Analyst Strategic Intelligence Service, and since 2004 LTC Lanz has been Project Manager for Doctrine Research and Development. *Address for correspondence*: Armed Forces Planning Staff, Military Doctrine, Doctrine Research and Development, Swiss Department of Defence, Civil Protection and Sports, Papiermühlestrasse 20, CH-3003 Bern, Switzerland; *Phone*: ++41 (0) 31 324 19 05; *Fax*: ++41 (0)31 322 54 45; E-*mail*: christian.lanz@vtg.admin.ch; *Web*: www.vbs-ddps.ch.

HOMELAND SECURITY AND THE RUSSIAN APPROACH

Lionel PONSARD

Abstract: Homeland security remains a vague notion in the Russian understanding, but essentially refers to the safeguard of key national interests, the struggle against global threats, with a strong focus on international terrorism, and eventually the fight against transnational organized crime. Homeland security tasks are usually performed in the Russian Federation by several security agencies distributed among three different ministries, i.e. the Interior Ministry, the MOD, and the Ministry for Civil Emergencies (EMERCOM). However, this trilateral structure is perhaps not sufficient to ensure concrete results in Russia's attempts to fight against organized crime. Although having repeatedly stated the need to re-establish the rule of law, the current Russian government appears to deal with oligarchs in a discretionary way. It would therefore be rather utopian to expect any real improvement without a radical change of attitude from the top leadership. Russian approach towards homeland security is rather close to the European standards in terms of structural implementation, but much closer to the U.S. approach in terms of response and the preference for the use of force. The analysis of Russia's security concepts demonstrates that security threats to the country are assessed as having clearly increased in the last ten years. A gloomier worldview combined with a reduced influence on the international scene obviously calls for more assertive security documents. In the same logic, the Russian perception advocates force as the preferred solution to deal with asymmetric threats, such as international terrorism. This became even more apparent in the wake of the 11 September attacks on the United States and the renewed strategic partnership between Moscow and Washington. The recognition of Russia's key role in the fight against international terrorism did indeed bring Russia back into the Western security community. On the Russian side, the Russian leadership soon understood that Russia was too weak to counter these new threats on its own and would lose any prospective benefit by openly confronting the West.

Keywords: Homeland Security, Asymmetric Threats, Russian Transnational Organized Crime, Russia's Security Concepts.

One of the most difficult issues facing governments today is the question of how to address new threats to national security. Gone are the days of the Cold War when intelligence agencies dealt essentially with a conventional threat that was rather pre-

dictable. These new threats have become increasingly global and asymmetric, following no rules or expected timelines. These observations suggest that these non-traditional threats pose risks to all countries including Russia. Needless to say that these threats would better be defeated through a coordinated and collaborative response among states. And yet, all countries do not see themselves "at war" against these new amorphous threats.[1] As a consequence, Europeans, Americans and Russians do not necessarily perceive the struggle against transnational threats in the same way. Interestingly enough, the widely held belief in the United States that force is the preferred solution to deal with transnational threats such as terrorism does find some echo among the Russian people. It is even commonly admitted that the odd couple of Bush and Putin was brought dramatically nearer by the terrorist assault. To grasp the Russian perception of these new threats, we will first explore some definitions pertaining to the concept of "homeland security," with a particular focus on their practical implementation in the Russian ministerial structures. We will then look into domestic threats of transnational nature, in particular criminal activities also defined as "organized crime." But in the Russian view, homeland security also includes the fight against global external threats. In order to better apprehend Russia's current perception of outside threats to its national security, we will review the evolution of Russia's security concepts. This analysis will also be put in parallel with Russia's position on the international scene in the aftermath of September 11. In so doing, a number of traditional security parameters and concerns will be highlighted.

Homeland Security Concepts and Russian Practice

"Homeland security" remains a rather vague concept, but basically suggests a security against an ill-defined threat or enemy.[2] The various components of homeland security notably include vital national interests, counterterrorism, counter proliferation, and international crime. The task of securing the homeland is most often described by European equivalents such as "domestic" or "internal" security. We should note however that the U.S. Department of Homeland Security strongly differs from a typical European ministry of the interior. Most important, the Department of Homeland Security essentially focuses on dealing with the threat posed by catastrophic terrorism, while the responsibilities and the tasks of a European ministry of the interior are much broader and include most if not all of a state's law enforcement elements. As for Russia, "Homeland security" essentially refers to the protection of national interests, the fight against global threats such as international terrorism, and eventually the fight against transnational organized crime. In practice, most of the functions of the American Department of Homeland Security are actually spread across a range of ministries in Russia. First and foremost, the Ministry of the Interior of Russia (MVD) heads the system of the bodies of internal affairs (police forces) and internal troops (equivalent to the French gendarmerie) and has jurisdiction over public administra-

tion in the sphere of protection of the rights and liberties and law enforcement.[3] In the aftermath of the Beslan tragedy, the Russian Interior Ministry has taken over a larger security role. Its new responsibilities now include the control of an additional 440 sites throughout the Russian Federation, many of which are viewed as potential targets for terrorists. Such reforms aim obviously at enhancing Russia's protection against terrorist actions.[4] Apart from the Interior Ministry, the Ministry of Defense and the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters (also called EMERCOM) are also responsible for homeland security tasks. The Russian MOD controls all military activities including the operational control of the army on a daily basis, but also retains a monopoly on military information and military intelligence. Last but not least, EMERCOM directs the whole Civil Defense apparatus, including Civil Protection Troops. These troops are armed with specialized equipment, such as engineering, medical, radiation, chemical and biological protection.[5] However, this trilateral structure is perhaps not enough in order to ensure an incremental improvement to Russia's internal security and its efforts in combating transnational threats such as organized crime.

Russia's Fight against Transnational Organized Crime

There has been a major increase in organized crime in the Russian Federation since the disintegration of the Soviet Union. The collapse of the Communist Party removed former mechanisms of social, political, and economic control and created a very permissive environment for criminal enterprise. The transition to the market economy was also made without any well-established rules or regulations. We might identify several major kinds of criminal activities, including drug trafficking, arms trafficking, trafficking in nuclear material, human trafficking, and money laundering. These activities are transnational since it is clear that the Russian Mafia has also spread its activities to other countries.[6]

Russian organized crime poses a direct threat to security at a national and international level. Internally, it challenges the state by providing a rival authority structure ready to use violence in order to enforce its actions. It also infiltrates and eventually corrupts public and private officials in order to neutralize law enforcement resources. The aim is usually to prevent any governmental initiative designed at fighting criminal groups. Organized criminal groups also try to invest in the potential of economies in transition. By disrupting social and economic institutions, they encourage inflationary pressures and undermine economic equilibrium. Furthermore, the implementation of a black economy inevitably affects economic growth. Most important perhaps, the people might opt for a hard-line government that promises to restore order. In this kind of scenario, the potential for a reversal of the trend towards democratiza-

tion and the reinforcement of autocratic tendencies is very considerable. Externally, it penetrates territories without respecting the sovereignty of national borders. While these threats are of great concern in Russia itself, the failure to deal with transnational organized crime from a global perspective merely provides further opportunities for their growth and development. Therefore, the international community should find ways to cooperate in preventing the expansion of the phenomenon of Russian organized crime.

In these circumstances, Russia has initiated more stringent measures against organized crime and the different ministerial security agencies have engaged in more comprehensive and effective inter-state cooperation. Different studies have been conducted and aim at understanding the conditions that are conducive to the rise and growth of transnational criminal organizations. However, there is so far no guarantee for success although the current government has often announced the return of the rule of law. The fact is that legislative power is united with executive power in the person of President Putin. The power over the life and liberty of the citizens is arbitrary since the judge is also the legislator.[7] Oligarchs and other typhoons currently are part of this strategy aiming at centralizing the maximum amount of power. They have a certain *marge de manoeuvre* as long as they respect some basic principles such as the absence of any real ambition in the realm of domestic politics. Khodorovsky tried to play this risky game. He finally lost and has recently been sentenced to 9 years in prison. Problems such as organized crime also provide the Kremlin with additional arguments that require the ceding of more liberties. Indeed, for the time being, most of the Russians are happy to cede more power and freedoms to the government. It is of major significance that in the view of most experts, Russia always appeared to have a low view of human nature, always believed in strong leadership, and always put primary reliance on coercion and repression orchestrated by the ruling administrative elite. Obviously, better coordination between security agencies remains fundamental, but we might also draw some parallel between the decision to strengthen security structures, the need to safeguard national interests, and the evolution of Russia's security concepts.

The Evolution of Russia's Security Concepts

On 21 April 2000, President Putin signed a decree approving a New Military Doctrine. The document, which replaces the one approved by former president Yeltsin in 1993, is a revised version of the blueprint published in the official Defense Ministry newspaper *Krasnaya Zvezda* on 9 October 1999. In this document, the military security of the Russian Federation rests upon strategic, political and economic factors. Therein, the threats to the security of the country are assessed as hav-

ing clearly increased since 1993. The document also refers to the expansion of military blocs and alliances as detrimental to Russia's military security.[8]

In sum, the New Doctrine reflects a gloomier and more militarized worldview than the previous one. This more assertive doctrine can be regarded as a reaction to the continuing decline of Russia's standing in international politics. This is particularly apparent in the paragraph addressing the lowering of the deployment threshold of nuclear weapons, which states that "the Russian Federation reserves the right to use nuclear weapons in response to an attack on itself or its allies by nuclear weapons or other weapons of mass destruction, and also in response to large scale attack by conventional weapons in situations critical to the national security of the Russian Federation."[9] This new nuclear policy can also be found in the New National Security Concept [10] approved by president Putin on 10 January 2000 in replacement of the National Security Concept [11] signed by president Yeltsin in December 1997. While recognizing that the threat of large-scale aggression against Russia in the foreseeable future is practically absent, the document underlines that Russia has to conduct its policy from a position of relative weakness. In other words, the weakening of the Russian Federation justifies the repositioning of the nuclear aim as the only guarantee of security.[12]

In this context, nuclear deterrence becomes the most important task of the Russian armed forces. One of the major changes in Russia's declared nuclear posture is probably the reconsideration of the long disregarded option of nuclear first strike.[13] However, the new nuclear policy does not define clearly the use of nuclear weapons, nor does it specify whether nuclear weapons are to be considered instruments of war-prevention or war-fighting.[14] Indeed, according to the New National Security Concept, "all forces and facilities available, including nuclear weapons, will be used if necessary to repel armed aggression, if all other means of resolving the crisis have been exhausted or have proved to be ineffective." In the 1997 version of the National Security Concept, this article read differently: "Russia reserves the right to use all forces and means at its disposal, including nuclear weapons, in case an armed aggression creates a threat to the very existence of the Russian Federation as an independent sovereign state." This means that nuclear weapons are no longer reserved solely for extreme situations as in the event of a threat to Russian national survival, but can also potentially be used in a small-scale war that does not necessarily threaten Russia's existence. These formulations thus show that Russia tries to compensate its conventional weakness by moving beyond a nuclear doctrine based exclusively on deterrence.

In both documents, military force is still presented as by far the most relevant instrument of power in international relations. As a consequence, the level and posture of the military potential of the state is to be enhanced to a sufficiently high level. Thus,

while the 1993 Military Doctrine mainly consolidated the view of Russia as a regional hegemon, the New Military Doctrine and the New National Security Concept both reflect a consensus on the imperative to preserve Russian interests on issues of vital strategic concern and to re-assert the Russian position on the international scene.

Russia's Fight against Global Threats after September 11

The terrorist attacks on the United States demonstrated once for all that no single entity—state or organization—could address these new threats to security and that their defeat required a coordinated response among states. In particular, the Russian leadership was very much aware of the fact that Russia was too weak to counter all these threats on its own and to achieve its long-term goals by openly confronting the West. Joining the West in the global campaign against transnational threats was therefore a sort of survival strategy at a time when the country had to concentrate on its domestic economic revival. Russia had neither the means to nor the interest in engaging into a very costly foreign and security policy and direct rivalry with the West. Only a sound economy would permit Russia to rebuild its military power necessary to the conduct of a realist policy aimed at rehabilitating the country's status on the international scene. The 11 September 2001 terrorist attacks on the United States thus brought about a shift in both Russian and Western policies, which were both conducive to greater rapprochement and interaction in the struggle against international terrorism.

From the outset, Russia actively and positively participated in the anti-terrorist coalition, not only providing diplomatic support to the campaign, but also sharing intelligence on sources and methods used to finance terrorist groups, and applying sanctions against the countries harboring terrorists. This cooperation gave rise to frank exchanges on the entire spectrum of the terrorist threat—including the risk of nuclear, biological and chemical proliferation—and included joint exercises addressing the consequences for the civilian population of a large-scale terrorist attack. When the United States initiated a campaign against the Taliban and Al-Qaida in Afghanistan,[15] Moscow opened Russian airspace to US planes and enhanced military assistance to the Northern Alliance.[16] Considering Russia's key role and military experience in Central Asia and Afghanistan, its participation was paramount to the success of the coalition against terrorism and the post-11 September international order.[17] Indeed, Russia's endorsement of U.S. Operation "Enduring Freedom" facilitated the provision of practical support by the former Soviet Central Asian states. Furthermore, reluctant states like China, India, and Iran finally decided to follow the Russian stance and to offer political support.

No need to say that this support and Putin's strongly pro-western rhetoric soon faced criticism amongst Russian political and military representatives,[18] as well as within large sections of the public. Apparently, many did not share his "confidence in the

American and European commitment to reward Moscow for its support."[19] In their perception, the US still viewed Russia as an obstacle to its interests in a number of issues: missile defense;[20] NATO enlargement; spread of US influence in Central Asia; relations with rogue states like Iraq, Iran, North Korea, etc. They also wanted Putin to avoid repeating the mistakes of Gorbachev and Yeltsin who had made concessions to the West and received very little in return.[21] Their position was further reinforced by severe U.S. blows to Russian interests on issues of vital strategic concern: U.S. withdrawal from the ABM Treaty and NATO's expansion to the East. In addition, the prospect of a long-term US military presence in the near abroad Central Asia was strongly opposed, not least by the Russian military.

Putin's decision to maintain a pro-Western line was in fact a way of showing that Russia belonged to the same security community. In other words, the attacks on the U.S. helped Russia to complete the building of what is now named the "threat bridge to the West."[22] By embarking on the campaign, Russia succeeded in imposing itself on the post-11 September order. The very recognition of common security concerns with the West, and shared vulnerability to threats such as global terrorism—and more particularly Sunni Islamist extremism—was another reason that comforted Putin in his decision. The fact that the U.S. were so preoccupied with building an international anti-terror coalition in which Russia ought to play a central role improved seemingly Russia's chances to regain some influence in international politics and to be treated as an almost equal partner by the US administration.

Indeed, the success of the U.S. operation against the Taliban in Afghanistan largely depended on the position of Russia, both in terms of its possible participation in the coalition and with regard to its influence on such neighboring countries as Tajikistan, Kyrgyzstan, and Iran. Not only does Russia possess military bases and units in the area close to the Afghan theatre, and does exert strong influence on at least some of the local Central Asian regimes (Tajikistan), but it also has strong personal interest in containing the Taliban threat.[23] Given its tense relations with Iran and Pakistan, Washington could hardly dispense with Russian facilities in the region. For its part, Russia's strategy was dictated by the perspective of several benefits.

A major benefit for Moscow included the Western endorsement of Russia's war in Chechnya [24] and the recognized legitimacy of this official anti-terrorist campaign.[25] Many Western political representatives soon put the Chechen rebels on par with organizers of 11 September attacks.[26] In this context, the West took up a new attitude towards Russia, and this change has confirmed, in the eyes of the Russian public, that the Russian policy in Chechnya, for example, has been a right one. Of course, Western human rights campaigners had expressed their concern about a softening of criticism towards the conduct of Russia's military operations in Chechnya.[27]

Another important element was Russia's desperate need for Western investment. Although Russian economy recovered rapidly from the massive rouble devaluation of August 1998—largely due to high oil and gas prices—there was still a strong need for further economic reform and restoring international investors' confidence in the Russian market. In return for its cooperation in the fight against terrorism, Putin expected U.S. and European support for Russia's economy. In this context, the importance of oil and energy resources did not go unnoticed in Russia's decision to join the anti-terrorist coalition. Indeed, the campaign against terrorism in Central Asia risked placing Russia as an alternative and a more reliable source of energy to the West. In other words, while not expecting short-term economic or political benefits from its cooperation with the West, Russia could expect future western investments and gains from the sale of oil and gas to the West, and could then potentially dominate its main Arab competitors—who were definitely more reluctant than Russia to join the anti-terror coalition—on the global energy market. Among the Russian people, however, there was widespread resignation and disillusionment regarding any Western support for Russia's economic difficulties.

We should bear in mind that, in so acting, Russia did not look at democracy and market economy as goals *per se*, but the best available instruments in making the Russian state stronger and more efficient. By becoming a member of the western community through cooperation against global threats, Russia would be able not only to save money the country would otherwise have spent on building a strategic parity or at least a credible and sufficient anti-western defense. Russia's choice meant a significant departure from traditional Soviet and—to a very large extent—post-Soviet thinking on Russia's place in the international system. In other words, it implied the end of Primakovian policies designed at counterbalancing the western influence by building strategic anti-western alliances with alternative centers of power in a multipolar world.

Conclusion

Russia's land stretches across both Europe and Asia. Its immensity provides the country with natural strategic interests throughout Europe, the Middle East, the Indian subcontinent, and the Far East.[28] However, this immensity was also the cause of scores of invasion of the Russian territory, from the Mongols to Napoleon to the Nazis. At the same time, it is a country whose brutal weather has often repelled these same foes with equal power. At the end of the Soviet Union, the loss of superpower status and the sudden emergence of new states on Russia's periphery were sources of considerable unease and confusion.[29] This post-imperial frustration was exacerbated by the fact that Russia's position with respect to a number of traditional security parameters—such as access to the high seas and availability of critical resources, etc.—

had significantly deteriorated with the disintegration of the former USSR a decade ago. In Russia's security documents, the motives of the West with respect to NATO enlargement, Kosovo, or missile defense were—at least implicitly—condemned and as a consequence, the level and posture of the military potential of the state was to be enhanced to a sufficiently high level.

The changing security environment following the 11 September 2001 attacks on the United States presented an unprecedented opportunity for Russia, not only to review its partnership with the West, but also to recognize their interdependence concerning the safeguard of vital security needs that none can meet alone. Both sides had good geopolitical reasons to cooperate at least at the outset. Obviously, it is fairly easy to misinterpret the changes of the Russian position by disregarding crucial nuances. Indeed, it should be observed that, regardless of what has been the real motivation of President Putin and his team, the main trend in the wider discourse has been not towards greater solidarity with the United States and the West as a whole, but about a re-assertion of the Russian position on the international stage.

While Russia's perception of Homeland security undoubtedly includes the fight against external threats and the safeguard of national interests, it also refers to domestic threats, in particular organized criminal activities. Russia, especially in its larger metropolitan areas, always had "big city" crime problems. In the Soviet period, however, crime was hidden and repressed by a totalitarian regime. Beginning in the mid-1980s, criminal activity became more visible with the arrival of perestroika and its associated political, social, and economic reform. These circumstances were then exacerbated by the diminished standards of living that came with the wholesale economic changes in post-Cold War Russia. At a state level, the interplay between organized crime and government officials is nothing short of subversion of the Russian state itself. This would obviously require immediate and decisive action at the highest levels of the executive, legislative, and judicial branches of the Russian government. However, experts tend to believe that one man only currently exercises these three powers in Russia and uses oligarchs to his own benefit. Obviously, more coordination among the different security agencies is also paramount, but no major improvement can be expected without a radical change of attitude from the top leadership.

Notes:

[1] John L. Clarke, "Securing the European Homeland," *Journal of Homeland Security* (September 2003): 1.

[2] Chris Seiple, "Homeland Security Concepts and Strategy," *Orbis* 46, no. 2 (Spring 2002): 259-273.

[3] See the official site of the Ministry of the Interior of Russia, <http://eng.mvdrf.ru>.

[4] Roger McDermott, "Russian Interior Troops Expand Security Role," *Eurasia Daily Monitor* 1, no. 146 (14 December 2004).

[5] See the official site of EMERCOM, <http://emercom.gov.ru>.

[6] Phil Williams and Ernesto Savona, *The United Nations and Transnational Organized Crime* (London: Frank Cass, 1996), 16.

[7] Charles de Secondat, Baron de Montesquieu, *The Spirit of Laws* (Cambridge: 1995), 157.

[8] See inter alia Henrikki Heikka, *Beyond the Cult of the Offensive. The Evolution of Soviet/Russian Strategic Culture and its Implications for the Nordic-Baltic Region* (Helsinki: The Finnish Institute of International Affairs, 2000), 79.

[9] See "Voyennaya Doktrina Rossii" (Russia's Military Doctrine), *Rossiyskie Vesti*, no. 224, 18 November 1993. For the New Military Doctrine, see "Voyennaya Doktrina Rossiyskoy Federatsii" (Military Doctrine of the Russian Federation), *Rossiyskaya Gazeta*, 25 April 2000. For the Draft of the New Military Doctrine, see "Voyennaya Doktrina Rossiyskoy Federatsii" (Military Doctrine of the Russian Federation), *Krasnaya Zvezda*, 10 September 1999. See also Vladimir Yermolin, "Military Signs a New Doctrine," *Izvestiya*, 13 October 1999; Andrey Korbut, "Draft Military Doctrine," *Nezavisimaya Gazeta*, 13 October 1999; and V. Chugunov, "We Discuss the Draft Military Doctrine. With Consideration for the Potential of the Country," *Krasnaya Zvezda*, 19 October 1999.

[10] The text may be found at the official site of Russia's Security Council, <www.scrf.gov.ru>. See also *Nezavisimoye Voyennoye Obozreniye*, 14 January 2000.

[11] See *National Security Concept of the Russian Federation*, <http://www.acronym.org.uk/43nsc.htm>. See also "New Look at National Security Concept," *Rossiyskaya Gazeta*, 6 October 1999.

[12] See Viktor N. Pavliatenko, "Russian Security in the Pacific Asian Region. The Dangers of Isolation," in *Russia and East Asia. The 21st Century Security Environment*, eds. Gilbert Rozman, Mikhail G. Nosov, and Koji Watanabe (New York: M. E. Sharpe, East West Institute, 1999), 20.

[13] See Andrei V. Zagorski, "Traditional Russian Security Interests in the Caucasus and Central Asia. Perceptions and Realities," in *Russia, the Caucasus, and Central Asia. The 21st Century Security Environment*, eds. Rajan Menon, Yuri E. Fedorov, and Ghia Nodia (New York: M. E. Sharpe, East West Institute, 1999), 62.

[14] See Heikka, *Beyond the Cult of the Offensive. The Evolution of Soviet/Russian Strategic Culture and its Implications for the Nordic-Baltic Region*, 82.

[15] Moscow supported UNSC resolution 1373 which in effect endorsed the US military action against the Taliban.

[16] It is important to note that Russia viewed Afghanistan under the Taliban rule as an acute source of destabilization in the region and a key exporter of Islamic terrorism to Chechnya. From 1996, Russia was the main supplier of military support to the Northern Alliance, and provided it with large quantities of weapons and war equipment in the aftermath of 11 September.

[17] Anatol Lieven, "The Secret Policemen's Ball: The United States, Russia and the International Order after 11 September," *International Affairs* 78, no. 2 (2002), 245-259.

[18] This confrontational stance was mainly advocated by Vladimir Zhirinovsky, leader of the Liberal Democratic Party LDPR (nationalist extremist); and Gennady Zyuganov, leader of the communist party KPRF.

[19] Oksana Antonenko, "Putin's Gamble," *Survival* 43, no. 4 (Winter 2001-2002): 49-60.

[20] From a Russian perspective, the building of more substantial defenses on the U.S. side would erode Russia's deterrent and pose serious impediments to further reductions in missiles (cf. START agreements).

[21] See Lieven, "The Secret Policemen's Ball: The United States, Russia and the International Order after 11 September."

[22] Boris Piadyshev, "After the Terrorist Attacks," *International Affairs* (Moscow) 47, no. 5 (2001), 6.

[23] See Jakub M. Godzimirski, *11 September 2001 and the Shift in Russia's Policy towards NATO* (Oslo: The Norwegian Atlantic Committee, Security Policy Library, 7-2002), 13.

[24] We should bear in mind that Putin's popularity and his political ascension were based on his uncompromising stance regarding the conflict in Chechnya.

[25] See Nodari Simonia and Vladimir Baranovsky, "What is in Store for the World," *International Affairs* (Moscow) 48, no. 1 (2002), 15.

[26] NATO Secretary General Lord Robertson, for instance, in his interview published in Russia on the day of the Rome Summit, described the Chechen rebels as a branch of the global terrorist network.

[27] See Antonenko, "Putin's Gamble."

[28] George Vernadsky, *A History of Russia* (New Haven: Yale University Press, 1961), 10.

[29] See also Joseph L. Nogee and R. Judson Mitchell, *Russian Politics: The Struggle for a New Order* (Boston: Allyn and Bacon, 1997), 163.

LIONEL PONSARD is currently a Research Advisor at the NATO Defense College in Rome. He first studied at the Universities of Louvain and London, and earned his PhD in Political Science at the University of Leiden. Dr. Ponsard started his professional career as an Assistant Lecturer at the University of Namur, Belgium. In 1999, he joined the Belgian Ministry of Defense as a Political Adviser. He later held several management positions at the Belgian General Staff, mainly in the area of political, security and defense issues related to the former Soviet Union and traveled extensively to the region. He was at the time mainly responsible for the preparation and the follow-up of bilateral and multilateral cooperation programs with east-European countries, particularly in the field of Defense reform. During his assignment, he also worked as Belgian Representative for specific NATO Economic, Political and Military Committees. On the academic side, he was Lecturer at the Belgian Royal Military Academy and the Belgian Royal Institute for Defense Studies. Dr. Ponsard is regularly invited to lecture at different academic institutions such as the National Defense University in Washington, the Russian Academy of Science in Moscow, the University of Louvain, the University of Namur, the NATO School, the NATO Studies Centre in Bucharest, the Ukrainian Military Academy, the Belgian Royal Military Academy, and the Belgian Royal Institute for Defense Studies. He is member of different associations such as the Belgian Association for Political Science and the Belgian Institute for International Relations. He has also published a number of articles in English, French, and Russian on post-Soviet issues and transatlantic relations in different academic journals including the *NATO Review*. Dr. Ponsard is perfectly fluent in no less than six foreign languages including Russian.

THE GROWING THREAT: HOMELAND SECURITY ISSUES OF BULGARIA

Valeri RATCHEV

Abstract: This article presents the main problems in adapting security establishments of democratic countries to the challenges of spreading terrorism in a globalized world. The focus is on problems facing post-communist countries. The author argues that, both during the early stages of democratization and in the ongoing security sector reform, the emphasis is on democratic civilian control and too little attention is paid to operational effectiveness. Furthermore, all democratic countries face the problem of achieving effectiveness of the security organizations while preserving and protecting democratic values. The concept of homeland security, among others, may be used to strengthen international and interagency cooperation in dealing with the security challenges of the Twenty First century.

Keywords: Homeland Security, Human Security, Societal Security, Terrorism, Security Sector Reform.

Among the huge and still growing number of key issues discussed by the security experts in the aftermath of September 11 is the extent to which transnational terrorism has become 1) *number 1* security threat, 2) threat to the liberal democratic world *as a whole* and not only to the US, and 3) *how long* will this threat remain dominant in the international and national security context. Let us all bear in mind the deeply emotional headline 'We are all Americans,' which appeared in one of the French newspapers on the day after the tragic events of September 11; two years later it was followed by 'We are all Spaniards,' which, however, left a touch of bitterness not so much due to the withdrawal of Spain from the coalition in Iraq but because of the inability of democrats to address their people in a democratic manner (i.e. directly and frankly). These were followed by the somber 'We are all Londoners' during the two-minute silence on July 15, when thousands of people throughout Europe paid tribute to the victims of the latest terrorist attacks. It was amidst these emotional responses that we initiated the war against terror, replacing with spread of democracy as a way of curtailing terrorism (no longer 'killing the mosquitoes with a newspaper,' but 'draining the swamp they breed in'), as President Bush emphasized in his second in-

auguration address. We have also completed the operation in Afghanistan with the total support of the entire international community and, in terms of rebuilding the nation, ended up with results which highly exceeded our expectations. We took part in the US-led campaign against Saddam Hussein, the outcome of which will become clear not within the next months or even years, but after decades.

Practically, the terrorist attacks in London mark a new chapter in this drama of the century. First, leading experts on transnational terrorism reached the conclusion that the search of its origin in the swamp of poverty, quicksand of religious fundamentalism or the clash between the 'rich North' and 'poor South' civilizations does not provide an answer to the question where should be the center of gravity in the war against terrorism. The London terrorist attacks show another aspect of the suicide bombers' image – altogether adjusted foreigners, never being subjected to any form of assimilation, brought up in well-to-do families with small business of their own, privileged to use all benefits of the free liberal democratic society and, alas, well acquainted with its flaws and vulnerabilities. According to British intelligence officials, their terrorist mentality takes the shape of blackmail against social and religious discrimination whose victims they think they are. If this assessment is correct, besides the religious motivation there is obviously a strong political factor wrapped in the haze of social injustice (we should keep in mind that Bin Laden himself is a multimillionaire, or at least was one in the wake of terrorism). Moreover, the MI5 experts are probably right when claiming that they are familiar not only with modern means of communication but also with the methods for conducting police investigation, the various obstacles in the relations among the institutions, media coverage and social compassion for suspects until their guilt is proven. There is one main issue which provokes and focuses our attention in regard to terrorism being the foremost threat in Europe (also). In relation to the London attacks, the Italian newspaper *La Stampa* ran an article about a demonstration against Israeli policy in Torino back in 2002, during which groups of Moroccan schoolchildren, educated in Italian schools, marched along dressed as suicide bombers.

Second, all current data, processes and trends confirm that terror will be the main threat to national and international security in the years to come: starting with the recruitment of suicide bombers, selecting the targets and ending with the ease with which all necessary items can be obtained; from oil prices to armament costs and the easy access to nuclear and missile know-how; from the continuous lack of effectiveness of the international organizations, vulnerability of interim coalitions to the lack of any short-term perspective for adjusting international law to real-life issues.

Third, it is quite obvious that the conceptualization of security in the 21st century is bouncing back and forth in a triangle formed by democratic freedoms, transnational asymmetric threats, and efficient security systems.

The highly ambitious US project called 'Homeland Security' turned out to be difficult for implementation by the Americans themselves, almost unfeasible for Western Europe and completely incomprehensible in Eastern Europe. Scandinavian research endeavors on contemporary crisis management systems are closer to the traditional East European models. They, however, cover a limited range of today's threats and do not involve active measures for countering terrorism and other threats beyond the country's national borders. The third principal notion nowadays is the concept of societal security. The reason to include this concept in the system of ideas and procedures was that the traditional concept of state security could not measure up to the inconsistent situation when, in some cases, strengthening of the security of state can turn into a threat to the society. This is typical not only for East European countries, but also for all other societies in which the security environment provokes an expectation for a strong hand, for order and discipline, for threats caused by minorities, etc.

This concept requires a phenomenal consolidation of society together with a strict control over the security sector in order to maintain a steady balance of their relationship in regard to effectiveness – democracy criterion.

Meanwhile, even the concept of the so-called 'Security Sector Reform' seems to be more like an idea for transforming security organizations from totalitarianism to democracy than an approach towards their modernization and optimization. Highlighting the aspect of democracy in the organization and functioning of the security forces—although a must from a political point of view—did little to enhance their efficiency in countering terrorism from an operational point of view. The reforms of the Armed Forces in different parts of the Euroatlantic space, which until recently were implemented in the range from revolution in military affairs to downsizing and modernization, turned out to be inappropriate and were replaced by the concept of transformation. In spite of the great efforts of the NATO's Allied Command Transformation, this concept is facing the extremely difficult task of reaching all member states of the Alliance as well as its potential non-allied partners around the globe. Even the idea for including 'small' states within the framework of developing niche capabilities cannot possibly make up for the lack of clear vision and could not fill in the technological gap and doctrinal deficiencies. Explanations for this vary from lack of mutual threat perception to lack of resources and limited national ambitions. As a result, too many questions arise and various issues, such as the role of the armed forces under the new circumstances and in the strategic future, their integrity as a whole (in terms of national defense and coalition operations) and the need of specific capabilities (necessary for countering terrorism), force planning (capabilities-based, threat-based or mission-based), and politically feasible framework of military acquisition, still remain unresolved. Expectations from the military are on the rise, no matter what they have proven, assumed or demonstrated so far.

On the whole, the surfacing high degree of vulnerability of modern liberal societies along with the obviously inadequate resources of the existing homeland security organizations to cope with the newly emerged risks and threats are becoming a problem which we are not ready to face either from a notional, political or operational point of view. It is possible that the tragic events in London will make the free world more tolerant to police control on free movement (surveillance cameras on main crossroads, in subways), on communications (Internet and cellular), on bank accounts and transactions (for suspects charged with financially aiding terrorists). This will no doubt help the politicians and experts to provide a plausible answer to the question of what liberties we are prepared to sacrifice in order to ensure even an imperfect security. Practically, however, the key political issue concerning homeland security lies in finding the formulae in which achievements of democracy instead of being sacrificed are implemented in countering terrorism.

Conceptual Level: Effective Security Policy Calls for Restricting the Scope of the Notion of 'Security'

In its 1994 Annual Global Human Development Report, UNDP introduced a new concept of security. The ambitious goal was to transform it into a basic conceptual instrument. Due to its comprehensive and fundamental nature, the notion for the so-called '*human security*' will have coordinating functions in many aspects of public life and serve as a basis for a great number of UNDP programs. The major issue in this case is that human security should not be set against national security. Initially we, especially the East European states for which homeland security was a matter of 'fatherland' and 'motherland' security during the Cold War, got the false impression that this is an entirely new level of security. We accepted it as a key element of the political transition and started to restructure many aspects of state security (border control, judiciary, address registration and monitoring, top secrecy on security, intelligence and counterintelligence issues on political presumption, etc.) without having any idea how to enhance human and societal security. With a background involving shock therapy, political and economic catharsis, lack of democratic responsibility and vague strategic environment, this was a very risky undertaking. We are still under the false impression that the traditional type of national security involves higher budget spending for security and defense compared with spending on human and societal security requirements. As the UNDP Report puts it, human security is multidimensional, the key aspects being economic security, food security, health security, environmental security, personal security, community security and political security. However, there is nothing original in this idea. Back in 1987, the UN General Assembly international conference on Disarmament and Development came up with a definition which reflects the new complex approach to security in the changing environment: "… Security is a top priority issue for all nations. It serves as a basis for

both disarmament and social development. Security has not only military but also political, economic, social, humanitarian and environmental aspects."

Basically, the term security has always referred precisely to human security. As Stefan Popov, a Bulgarian analyst, once said, the problem is that "… throughout the Cold War human security was regarded and included in terms such as nation, sovereignty, territory, population. This is by no means substitution of one type of security with another. Providing security to the citizens involves a policy at the level of territorial defense, preparing for a massive attack, etc." Transnational terrorism has changed thoroughly this context, thus shifting the focal point from security of the state attributes (sovereignty, territorial integrity and independence, as guaranteed by the Constitution of Bulgaria) to security of critical infrastructure, information networks, political process, ethnic relations, social balance in all its aspects – economical, psychological, etc. The scope of the term security can be spread on indefinitely. As a result, the initial term security becomes even more vague and wide-ranging. It turns out that the very effort to make human security the target of policy actions has been rendered useless with the introduction of this term. Taking a broad approach to security might become a risky precedent for the management process if the basic concept is not subjected to a certain structural adaptation. The key issues here are at least two: identifying the term 'security' as policy objective and defining the policies needed to reach this objective.

Looking for a New Security Paradigm

Addressing a seminar at the George C. Marshall European Center for Security Studies, Prof. J. Clark emphasized the US efforts to modernize their security system. According to him, '*Homeland Security*' embodies "the preparation for, prevention of, deterrence of, preemption of, defense against and response to threats and aggression directed toward population and infrastructure, as well as crisis management, consequence management and other domestic civil support." He also referred to homeland defense as: "the protection of territory, sovereignty, domestic population and critical infrastructure against direct threats and aggression." It is obviously not easy to initiate policy actions based on these definitions. The US actions in the aftermath of 2001 clearly prove this – highly ambitious at the beginning, focused on the newly established Department of Homeland Security, followed by a continuous search for allocation and balancing responsibilities among institutions, a large-scale project for restructuring intelligence community, huge but dubious defense budget, reassessment of the new social control regime, etc.

The general US approach embodies three more or less separate elements: *protection* against various terrorist attacks; *defense* of territorial integrity and sovereignty; *assistance* in case of disasters, terrorist attacks and other emergencies. This article,

however, is not intended to make any kind of assessment of the existing US practices. A huge setback for Bulgaria and other similar countries is the current identity dilemma in the field of security. It may sound paradoxical, but the challenges to security policy triggered by transnational terrorism should have been even more serious for us than for the West European countries. Political transition within the last fifteen years was based on the collective approach to foreign policy, security, and defense, voluntary renunciation of part of the national sovereignty, and shared obligation. Along with many other issues, transition meant breaking up with the bastion state, with the notion of '*Fatherland*,' whose political survival was more important than the human values, as well as with the notion of '*The War*' in which we had to destroy the enemy.

At present, the discussion of the security paradigm in Bulgaria is focused at several levels of analysis: sense of belonging (or not belonging) to the common Euroatlantic values, threat perception (either shared or not), concept for reaction (determination, wait-and-see, and defense), and collective approach (what we can and what we cannot do on our own).

The sense of belonging to a certain civilization cannot be acquired or destroyed in a couple of decades. In the past, within the boundaries of the Ottoman Empire, Bulgaria managed to preserve its values for five centuries. Returning to the roots of their civilization has never been a problem for Czechs and Hungarians, mainly due to the fact they had never really broken with them. Nowadays, Bulgaria's joining the transatlantic system of values in terms of mentality is based on the presumptions of 'no return,' 'this is our world,' and 'we should share the burden (pay the price).' These are more or less political slogans. However, if they could succeed in motivating also the social expectations and individual actions and gain support by gradual achievements in the field of integration, then the idea of belonging will become a key motivating factor and will result in deep 'sharing of values,' while the cultural identity remains intact.

In regard to national security, the threat perception is undergoing continuous changes as a result of such factors and circumstances as the end of the Cold War, the collapse of the Warsaw Pact, the conflict in neighboring Yugoslavia, the emerging Islamic fundamentalism, the transnational terrorism, and the escalating organized crime in the country and in the region. Clearly, terrorism is just one of the driving factors of the nation's current threat perception. Society's expectations and the actions of the politicians are affected not so much by its pure forms of manifestation but by its combination with other factors and circumstances such as Bulgaria's participation in missions abroad—Bosnia, Kosovo, Afghanistan, Iraq—and the presence of large Muslim communities and thousands of Bulgarian Muslims with dual citizenship, relatively loose residence regime of aliens, and last but not least – organized crime engaged in

'strategic' traffic routes connecting Afghanistan and Turkey with Kosovo, Albania and Colombia, as well as with the West European and the US markets.

It is the nation's historic background that determines the notion about the way security-related issues are tackled, together with the government's determination, the realistic assessment of the country's capabilities, and the maturity level of Alliance mentality.

In Bulgaria, each of these elements is still undergoing thorough transformation. The old Balkan mentality to resolve all issues by means of war is obviously part of the past. However, the flying start of the first nationalist party after the 2005 Parliamentary elections cannot remain unnoticed (Coalition 'Ataka').

The ambitions of the recent Bulgarian governments to escape from the swamp of international isolation (deep enough from the time of Mehmet Ali Agca's assassination attempt of the Pope John Paul II, and the self-imposed isolation during the wars in Yugoslavia in the 1990s) and to demonstrate the qualities of first class-actors in international relations have led to participation in such emblematic events as the NATO operation in Kosovo, the war against terror and driving the Talibans from power in Afghanistan, and the US-led operation in Iraq. Thus, a trend for 'determination' and 'being on the offensive' starts to emerge, which would have hardly happened had the syndromes of demonstrating a sense of belonging, of confirming the breaking up with isolation and of finding proofs for their own value existed.

Another specific issue is to what extent decision makers and society are aware of the real capabilities of the security sector. One of the main difficulties encountered during the pre-mission training for deployment on the Balkans, Afghanistan and Iraq in particular, is that political decisions were made on the presumption that capabilities exist, but only after decisions were made the military started to create the specific capabilities: forming battalions, providing equipment and special training, etc. Considering the different nature of these operations in terms of risk, specific conditions and scale, the issue of existing operational military capabilities for participation in such operations created quite a swell in public interest.

Community spirit in regard to NATO and its member states could not obviously be formed within a year or two, given the difference between NATO and the Warsaw Pact in terms of organizational culture and collective approach. As a result, the spirit of 'collectiveness' is demonstrated mainly on political and professional military level. In order to guarantee political continuity, however, it should be integrated into the nation's system of values.

Apparently, under these circumstances the new security paradigm could no longer be based on the conventional concepts for 'territorial integrity, sovereignty and inde-

pendence of the country' being the focus of the security policy and main objective of the armed forces and being implemented through a 'defensive military doctrine.' Granted that Bulgaria and other countries from Europe and America, regardless of their potential and ambitions, sincerely desire to join the Euro-Atlantic system of values, they have to accept the paradigm that national security should be guaranteed by effective risk management and prevention of risks escalating into threats as early as possible, preferably in a collective manner. This paradigm thoroughly changes the approach to building national security sectors, sets new requirements in respect to the legislative basis for guaranteeing security within the country, within the alliance and in the world as a whole and creates new regulations concerning the transformation of the armed forces and the other security-related establishments.

The Achilles' Heel: Operationalization of the New Security Paradigm

The main reason for the slow and strenuous digestion of the new realities in the security sector most probably is a result of the transition's inertia. For much too long states like Bulgaria had focused primarily on themselves – on the political and economic transition within the country and the corresponding 'reforms.' In our case, for instance, democratic control of the security sector, structural demolition of the 'state within the state' and achieving a certain degree of transparency on an organizational level were much more important than efficiency, competence and rationalism under the 'cost-efficiency' criterion. As a result, the security sector organizations turned into institutions 'in waiting': any immediate military effectiveness was not necessary, or at least was not a priority; the interior organizations were subordinated to the primacy of civil rights; the intelligence and counterintelligence were subordinated to competing political goals.

The issue is to what extent inertia has been brought to a close and replaced with the sober understanding that what we are facing now are growing asymmetric threats, ideological and religious extremism and terrorism with globalized long-arms, which makes the effectiveness of the security apparatus paramount and requires different priorities and trade-offs. Events such as the London bombings of July 7, 2005, will no doubt bring politicians and professionals closer to realizing the rationalism of the new security paradigm than, for instance, to giving up the concept that 'security' is equivalent to 'defense.' However, apparently the problem lies in the ability to generate new operational concepts and turning them into systems of well-functioning tools. The so far unsuccessful efforts in regard to the security sector reform concept are an example of this, but we can hardly expect any conclusions to be made out of them. The situation concerning homeland security is quite similar. In the most recent Bulgarian *Strategic Defense Review* neither of the two concepts was implemented, while modern crisis management systems and human or societal security were not even

mentioned. These are the facts, although Bulgarians were among the most ardent participants in the debates concerning the thorough transformation of the political, legal and operational aspects of the national security system even before September 11.

This article is not intended to make a critical analysis of the existing security concepts or offer a new national security system option. Actually, it is offering a number of ideas and approaches in this regard. However, there are several basic points while discussing the various alternatives. Among them are the perceptions for the new political goals of the security system, the vision for national security's global space, the conviction that global threats should be confronted collectively, and that the quest for more security should not extend beyond democratic values.

Guaranteeing absolute security is no longer a plausible political goal

The architecture and the buildup of the security system used to be based on the presumption that, provided we have perfect organizations engaging the best possible professionals and the state provides sufficient funds, national security is guaranteed. The opposite was quite out of the question both from a political and professional point of view. Therefore, even experts openly declared that either there is or there is no security. Thus, the main issue for the East-European states in the context of their NATO membership was 'To what extent will NATO guarantee our security?', although while analyzing the threat perceptions these same people (mostly politicians and journalists) declared that practically there are no threats for countries like Bulgaria which require NATO protection. Speaking about guaranteed or 100 percent security in our globalized world is pure fantasy. Terrorist attacks in the US and even more the ones in Madrid, Istanbul and London clearly showed that the main issue lies not in 'guaranteeing security,' but in determining the level of insecurity society is ready to accept as normal. The social perception for insecurity is the key decision-making factor as far as security is concerned. The chronically insecure societies are suspicious, irritable and radical in terms of their social and political behavior. Generally speaking, they are prone to making greater cutbacks of civil and democratic freedoms and radical decisions (regulations, budgets, large-scale restructuring, contingency measures) are more easily adopted.

Security can no longer be regarded as internal and external

Reality leaves far behind the current organizational structure of the national security systems. For countries such as Bulgaria not even one of the existing security risks can possibly emerge and evolve only within the country and none of the current threats can be resolved solely on the country's territory. The presumption for 'external' and 'internal' no longer exists in the sphere of security. In spite of the actual breakthroughs within the police and army sectors, most of the security organizations still follow this course both in terms of concept and structure. Roles and missions, legal

frameworks and operational concepts are being created for major options with a 5 percent probability, while those which are 95 percent likely to happen are dealt with on an *ad hoc* basis and from time to time. The Armed Forces consider operations such as the ones in Afghanistan, Kosovo and Iraq as 'non traditional' or 'unconventional.' The system of counter-crime organizations continues to be helpless in regard to internationally-based crime because its notional basis includes the presumption for domestic area of operations and authority. Intelligence and counterintelligence divisions follow the principle of 'external' and 'internal,' although in a world of globalized information technologies, banking, movement of people and commodities this is sheer nonsense.

The capability gap could not be fulfilled on a national basis

NATO and EU will no longer be security organizations aiming to prevent clashes among the member states by means of integration. The institutional politization as a discussion forum on security issues is being replaced by their operationalization into actual policy instruments. Not even a single issue could be resolved by partial measures on a national level such as quitting the *Schengen Agreement* in order to strengthen national border control. They only illustrate that, so far, not enough attention has been paid to the international measures for building up capabilities where required and to interactive programming mechanisms. In view of terrorism and other global threats, the efficiency of the security instruments becomes crucial. Interoperability should be related not only to NATO member states and military establishments. Interoperability is the basis for combined and joint operations of military and interior forces but also for all inter-agency—both national and international—actions. Net-centric operations should also be further developed and implemented as doctrine both internationally and within the national institutions. Advanced multinational research and development and integration of defense industries into a perspective source of coalition security advantage are important components of this approach.

The virtues of democracy should be used as foundations for building up the new security system

Democracy must not be used as an excuse for the lack of efficiency of the security system in our world and this is more than obvious. Democracy's biggest strength lies in the people's concern for the future of the nation and the state, i.e. the lack of principal antagonism between citizen and political authority. This means that key issue of the required new security policy is the authorities' manner of addressing and getting people involved in security measures. This means that attacks on the Euroatlantic democratic system require, more than ever, democracy. Professor Dominique Moissi said in Sofia: "The first answer for us is to be even more democratic than we are. This is what the enemy wants us to become: to close our system, to violate these democratic principles of which we are so proud. The answer to violence is democracy." He

came up with a very important conclusion regarding the 2003 Madrid bombing: the reason for turning the vote in the parliamentary elections in Spain is mainly the failure of the then-government to openly and frankly tell Spanish people: "Well, it may be Al Queda's doing, but it is not because of the war in Iraq. It is because we are liberal democracy and we are to fight it together."

Perfect civil control, transparency in planning and functioning of the security sector organizations, efficiency and competence of parliamentary oversight must be promptly and cleverly modernized in order to meet the challenges posed by transnational terrorism. Being a pillar of civil society and democracy, they could not possibly be questioned or restricted without discussion. The time of closed-type organizations is definitely over. We must keep in mind, however, that even perfect civil control and transparency could easily turn them into ineffective or simple political instrument (especially in the underdeveloped democracies of Eastern Europe). Control and transparency must have a mission and objective. Control and transparency without objective and purpose might make things even worse.

New organizational culture is a must

Practically all efforts so far to conceptualize national security sectors have more or less failed. It is obvious that archaic standards prevail for reserved perimeters, unique obligations, vertical organizations and relationships, etc., whose origin lies in the self-generated presumption that security organizations (and their personnel) are the true patriots and the only saviors of the nation in case of calamity.

No doubt things have changes in the aftermath of the Cold War. Some doubts remain in regard to the ways security sector could be organized and could perform. Analysts from the East have often observed with some envy the existing practices in the USA and other countries to create horizontally organized and manageable structures, declaring that the only way to avoid the destructive effect of hierarchically structured organizational behavior is by creating a real security community. Today, we are witnessing an increasing centralization in the West, intelligence and security services included. This is a serious cultural issue which could be overcome only after thorough social and psychological analyses and decision modeling for defining the true balance between organizational tradition and mentality and modern management procedures.

Legal bases of security must form the nation's future

Many of the reforms in East Europe, both past and present, are or were focused on eradicating atrocious or ineffective legacy from the past. Regulations and mechanisms for their implementation in most of the cases addressed problems, which had already occurred in certain countries, and were intended to prevent their happening again. These regulations were very short-lived. The current Defense and Armed Forces Law in Bulgaria was adopted in 1995 as a reflection of the most serious clash between the

Minister of Defense and the Chief of the General Staff (the most senior military official in the country). The Law's ideology lies in the presumption to 'define and differentiate' the military and civil sectors and limit any possible mutual intervening. Ten years after its adoption, this law still generates a mentality of differentiation which is spreading not only among military and civilian personnel but within the whole society.

In order to function properly, the new security paradigm must be backed up by innovative laws and regulations, shaping the ethos of the experts engaged in the security sector as well as the nation's character as far as broad security sector issues are concerned. They should focus not on past problems but on future demands. The effect of the new legislation, for instance, will become visible after one generation of officers (accounting for the example of *Innere Führung* in Germany).

Remodeling of the security system must boost the democratic political system

The real situation, especially in the East European countries, is that while the democratic political system was practically newly established, the national security systems were subjected to reforms or restructuring. Thus, the new Bulgarian Constitution adopted in 1991 created four power centers – Parliament, President (directly elected by the people), Government (endorsed by Parliament), and independent judicial system (including Constitutional Court ensuring the supremacy of the Constitution). This pattern, along with the distribution of prerogatives, displays the existing at that time concerns about the return of authoritarianism rather than any ambition for creating a simplified and efficient political management system. The distribution of security organizations among the power centers is motivated by the system of checks and balances. Thus, the President has direct control over the National Intelligence Service and the National Guard Service and is Supreme Commander of the Armed Forces although he has no rights to initiate any regulatory acts or to exert influence on their budgeting. Obviously, in a situation like this, the system's efficiency starts to depend on the leaders and how well they work together rather than on hierarchy and formal relationships. In a number of similar cases, one of the possible means for countering terrorism and other unexpected threats is creating a government-affiliated Security Council, incorporating the existing information and analyses, and a corresponding position of National Security Counselor or National Director of Intelligence. These are the so called 'expedient' solutions. Actually, in some cases like the one in Bulgaria, it is a matter of forming up a new center of influence, which might considerably transform the relationships within the system of checks and balances.

Another aspect of this principle is the setting up of a national system for crisis response or for civil protection. So far the approach has been in favor of a centralized model of ministerial type. The resulting effect is that in case of a calamity local peo-

ple regard themselves as doomed while those coming from the so called 'center' look like saviors to them. This definitely does not help direct democracy and undermines the idea for a strong local government.

Conclusions

The nature of global security has changed over the past twenty years or so. Practically, it seems that two dates and one single process are dominating over our present. The dates are November 9, 1989 when the Berlin Wall collapsed, and September 11, 2001 when terrorists wiped out one of the symbols of the free world. The process is globalization – political, economic, cultural, informational and in the field of security. No doubt terrorism is one of the dark sides of globalization coming up to show that besides the free flow of finances and commodities, unfortunately there is a possibility for merging and intermingling of threats and risks. We are now witnesses of a new phenomenon – never before in mankind's history such a small group of people has had the opportunity to threaten so many people. It is just the opposite to the famous quote of Churchill: "Never did so few people do so much for so many."

The present situation could be described in a number of ways, but I believe it is mainly caused by the technological gap and the lack of progress in human ethics. This is a problem we all must face with the awareness that we are living in a totally dependant and globally united world: we have no place to hide or to retreat from the existing problems. It is totally unacceptable to be divided no matter what the reason might be. Like never before we are all in one boat. This is why the quest for a new security paradigm and the subsequent operational models and decisions is like never before a matter of collective effort. One of our biggest challenges is the need of thorough and multivariate analyses as well as prompt actions leading to concrete results. In fact, no one has any time for making experiments and errors. The joint efforts for this edition of *Information and Security* are modest although much needed contribution in the quest for finding constructive solutions. It does not matter whether they will be found within the context of homeland security, crisis management, human or societal security or another conceptual framework. What really matters is the effectiveness of the policy and its implementation so that terrorists are never allowed to set the security agenda.

VALERI RATCHEV is Colonel of the Bulgarian Armed Forces. He is Deputy Commandant of "G.S. Rakovski" Defense and Staff College and Dean of its National Security and Defense Faculty. In this position he is responsible for senior military officers' education and civil-military training on security and defense policy and management. Col. Ratchev has considerable experience in conceptualization and documentation on national security, crisis management, defense doctrine and force reorganization. He has published extensively on international security issues, defense reform and civil-military relations. *E-mail*: ratchevv@yahoo.com.

CIVIL SECURITY: ARCHITECTURAL APPROACH IN EMERGENCY MANAGEMENT TRANSFORMATION

Velizar SHALAMANOV, Stefan HADJITODOROV,
Todor TAGAREV, Stoyan AVRAMOV, Valentin STOYANOV,
Pencho GENESHKY, and Nikolay PAVLOV

Abstract: The article presents the major findings of a comprehensive study (White Paper on Civil Protection) accomplished by the Center for National Security and Defense Research (CNSDR) in the Bulgarian Academy of Sciences (BAS). The research is presently further developed within the framework of a NATO Science for Peace Project SFP-981149 for building new capabilities in Decision Making Support for the Bulgarian Security Sector. The main goal of this article is to assess the status and prospects ahead of the system for protection of population and critical infrastructure. The fundamental principles of the Concept for Civil Security of the Republic of Bulgaria have been formulated within the context of the establishment of an integrated security sector. An institutionalized civil security system is considered "the third pillar" of the security sector in Bulgaria. Three main alternatives for development of civil security system are put forward. The first alternative is a result of a narrow interpretation and application of the newly adopted Crisis Management Act. The second alternative offers a broader interpretation and application of the Crisis Management Act. This alternative envisages maximum interdepartmental coordination – "a quasi ministry, whereas a ministry is not actually established." The third alternative envisages the establishment of a new Ministry of Civil Security. The development of a Center of Excellence in Security Sector Transformation in Bulgaria is proposed to provide scientific support to the effective transformation of the civil security system and the implementation of the Crisis Management Law.

Keywords: New Risks and Vulnerabilities, Emergency Management, Civil Security, System Architecture, Security Sector Transformation.

Introduction: Vulnerability and Security in the New Age

There is a clear shift from military to nonmilitary threats to security and increasing awareness of the vulnerabilities of modern society to disasters and emergencies, terrorist acts and organized crime.

In such a security environment it is more and more important to have an integrated approach to security and an integrated security sector to cope with the new challenges. Participation of civil society and focus on security of the citizen and society as key element of the emerging civil security concept is best visible in the area of emergency management / civil protection.

Different events are possible on the Bulgarian territory, which require rapid reaction of the security system:

- *Natural disasters* – earthquakes, floods, drought, landslides and landslips, stormy winds, twisters, sandstorms, forest and field fires, hailstorms, snowdrifts, ice storms, sea storms, centers of infections and human, animal and plant pandemic diseases;
- *Accidents* – at risk sites operating with nuclear, radiation, explosive and highly inflammable substances, toxic industrial substances and toxic gases;
- *Emergencies* – cosmic, aviation, railway, road, at sea, and premeditated acts;
- *Terrorist acts*, as well as separate acts of organized crime that pose a direct threat to security of civilians and critical infrastructure.

Risks of different nature have been consecutively assessed with the help of the seven expert groups of the National Consultative Council with the Permanent Committee for Protection of the Population against Natural Disasters, Accidents and Emergencies (PCPPNDAE).

The possible causes of risk of radiation contamination are: violation of radiation safety rules; violation of safety rules; incompetence to work with sources of ionizing radiation (SIR); human error; theft; terrorist act. The possible consequences of *radiation risks* are: damages to people – loss of human life within the zone of radiation damage, damage within the repository, damages to a different extent to the people across the entire territory of the country, local damages from SIR; damages to critical infrastructure – loss of huge power capacities in an industrial accident at a nuclear power plant; environmental damages.

Chemical risks come mainly from industrial accidents when highly toxic substances are produced; there is a risk of such accident in more than 350 companies in the pharmaceutical, metallurgic, chemical, textile and oil processing industries. The territory of the country is crossed by *oil* and *gas pipelines*, which together with the compressor stations and the natural gas repository near the village of Chiren are potentially highly inflammable and explosive sites. The territory of the country is also crossed by a major *artery for transport vehicles carrying highly toxic substances*, which, in case of a road accident, may cause environmental pollution or pose a threat to the life and health of the population. Road accidents and *technological accidents at*

sites operating with oil, *oil products and natural gas* may cause pollution and pose a real threat to the population. *Spills of mercury*, *pesticides and other chemicals*, as well as accidents related to the use and transportation of the abovementioned items could also result in pollution and real threat to the population. Oil spills along the Danube River and the Black Sea may have the same effect.

Biological risks leading to severe infections-related morbidity for the period 1950-1959 stood annually at 1402,86 o/$_{oooo}$ (104 135 registered cases). The next period of 34 years (1960-1993) marks a downfall in morbidity rate and eradication and elimination of a number of contagious diseases (hydrophobia, classical typhus, diphtheria, poliomyelitis). The average rate of morbidity for the period stands at 1208,43 o/$_{oooo}$ as a result of improvements in the etiological diagnostics, the expansion of the immunization program, and planned implementation of anti-epidemic and prophylactic measures. In the 1970s, there was immediate risk of importing some very dangerous infections such as smallpox and cholera from neighboring countries (Federal Republic of Yugoslavia and Republic of Turkey). The period 1994-2003 is characterized by a tendency of decreasing morbidity rate from highly contagious diseases – from 1043 o/$_{oooo}$ in 1994 to 648 o/$_{oooo}$ for 2003. The average annual morbidity for that period stands at 910,82 o/$_{oooo.}$

Seismic risks are caused by different natural (and in some cases anthropogenic) factors, suddenly manifested short movements of Earth's surface of different strength. They stand out for: very hard to predict (and only partially) or unpredictable manifestation; very short duration (within tens of seconds) of seismic blasts; different depth of seismic centers; inconstant and huge by rule intensity of seismic energy; regular or irregular recurrence of seismic processes; relative localization of seismic effects in seismic zones and belts on Earth's surface; relation between the earthquakes and the strongly rifted sections of the lithosphere.

The earthquakes of average and big magnitudes may cause many different in scope and nature ecological problems related to: the destructive power of tsunami waves along seacoast areas; damage or destruction of dam walls of artificial reservoirs; damage or destruction of warehouse facilities, reservoirs or earth gas pipelines, liquid fuels or other chemical substances; damage or destruction of electric transmission lines, etc. The heaviest situations could emerge in the most densely built-up central urban part, industrial areas of big cities and the lots of old construction not compliant to the seismic requirements.

Landslide risks are related to some of the major unfavorable phenomena that form the potential geodynamic danger. Landslides are scattered irregularly across the territory of the country and there are regions of higher concentration.

The *climatic*, *meteorological* and *hydrological risks* fall into two groups of risk phenomena: natural and anthropogenic. The "winter" and "summer" smog in cities, the thinning ozone in the stratosphere and the "global warming" are among the highest risk phenomena of anthropogenic nature. A possible climate change is related to potential risks for agriculture and forestry, water resources and healthcare.

Significant and intensive precipitation may cause floods in many possible regions across the country. Considerable warming during the second half of winter and the start of spring, accompanied by rainfalls and fast thawing of snow cover may cause small and medium water basins to overflow and other unfavorable phenomena.

Strong winds, such as foehn, squall, strong turbulent wind, and twister, cause breakdown in communications, damages and collateral difficulties (possibly victims). Probable regions are the entire territory of the country. Meteorological situations leading to fires are the continuous droughts accompanied by high temperature and low humidity.

Risks related to infrastructure have acquired greater significance for civil security. The draft CM Law defines "critical infrastructure" as a system of facilities, services, information systems, whose halting, defects in operation or destruction may have serious negative impact on the health and safety of population, environment, national economy or on the efficient functioning of the state administration.

In some states, the defense system and management of emergencies have been explicitly defined as part of the critical infrastructure. Other countries underscore the critical importance of the functioning of administration, healthcare system and public-order enforcement systems.

These are real risks and they are not only on our territory but everywhere, so we have to be prepared to react as well as to work on reducing vulnerabilities (mitigation), to perform preparedness / prevention activities and to have capable programs for reconstruction.

This article is based on a research project of CNSDR-BAS ordered by PCPPNDAC in order *to assess with the participation of independent experts the current state and prospects ahead of the system for protection of the population and critical infrastructure*, *to develop a concept for its expansion and thus assist PCPPNDAC and the other competent authorities in the application of the just approved Law on Crisis Management and possible drafting of the Law on Population and Critical Infrastructure Protection.*

The research performed is of a *methodological*, *conceptual* and *recommendatory* nature. After the relevant administrative decisions are taken by the competent officials, *a decision may be drafted by the Council of Ministers for the adoption and develop-*

ment of legislation and other regulations, for the organization of training at central and regional levels within the framework of a comprehensive concept for the system for protection of the population and critical infrastructure.

The immediate importance of the presented project is determined by:

- The reform in the security sector has reached the stage of intergovernmental coordination and integration, at which the system for population and infrastructure protection, within the context of the currently drafted Law on Crisis Management, is to play a key role in restructuring of the sector.
- The assessment of the risk environment and particularly of terrorist threat, infrastructure vulnerability, gradual privatization of major infrastructure sectors, increased international commitments, and the cross-border character of modern threats require a modern review of the system.
- The actual NATO membership and the forthcoming EU membership require a high extent of harmonization. In fact, the civil protection system is a top priority area of cooperation between EU and NATO in the Black Sea region.
- The completed Strategic Defense Review makes it possible to reassess and redirected a number of issues related to the use of civil resources, defense industry, strategic partnership, etc., which opens new opportunities for projects for modernization of the system for civil protection within the context of army, police and infrastructure sectors modernization.

The main contributions of the accomplished study are in:

- Definition of the concept of "Civil Security" as the Bulgarian interpretation of the concepts of Homeland Security, Civil Security and Societal Security, discussed within the Euro-Atlantic community in the context of establishing an integrated security sector.
- Application of the architectural approach leading to comprehensive description of alternative crisis management arrangements, assessment of alternatives and selection of a "best" architecture, and, finally, defining main steps of the transition to the future architecture.
- Efficient use of the brain-storming method and optimization methods for decision-making regarding the development of population and critical infrastructure protection system.

Concept of Civil Security as Third Pillar of Modern Security Concepts

The analysis has focused on a number of different notions for naming of the unified system for management of crises caused by natural disasters, accidents and catastrophes and for protection of citizens and infrastructure: civil defense; security of living

environment; public security (*societal security* has been adopted in Scandinavian countries and is considered an analogue of the American *homeland security*); protection of the population (citizens) and infrastructure; security of citizens and infrastructure; civil protection; *human security*; *civil security*.

The most recommended term within the Bulgarian context is "civil security" (adopted, for example, in France and Belgium). The creation of a Bulgarian concept of civil security has sought a balance between the approach of the US and different European countries by taking into consideration the experience and the situation in Bulgaria with the aim to establish the best possible environment for efficient implementation of the Law on Crisis Management.

The civil security system could be established as an independent third "pillar" of the security sector, which is equally important to the other two "pillars" of security – internal security and public order (mainly provided for by the Ministry of the Interior) and external security and military operations (mainly provided for by the Ministry of Defense).[1] Consequently, it should have a well-defined normative regulation and a solid institutional dimension. There is a possibility that social relations connected to civil security can be regulated by the same Law on National Security.

The civil security system is built to a high extent with active civil participation and civil control as compared to the other elements of the security sector. This presupposes also a high extent of transparency, accountability, and, in the long run, democratic quality of this key element of the security sector. The establishment of an efficient civil security system presents an opening for the maintenance of well-balanced civil-military relations and clear-cut distribution of obligations during different types of crises.

The civil security system should be based on the principle of decentralization. Special importance is rendered to the local units of civil security (controlled by the local authorities) that give the initial response at the rise of threats related to civilians and infrastructure. This characteristic of the system for civil security corresponds directly to the process of establishing an electronic government (e-government), including at local level. If the transformation process is well-managed, "security" as a service could be provided along with other administrative services as a "one-stop-shop" service (on the Internet or a single emergency and non-emergency phone number). Much could be borrowed in this respect from the experience of the Emergency Call Centers established at all levels of the administrative-territorial units in the US.

The principle of decentralization does not eliminate the need of an overall coordination and control implemented by the "central units" of the civil security system – the National Centre for Crisis Management, the State Agency for Civil Protection, and the Permanent Committee for Protection of the Population against Natural Disasters,

Accidents and Catastrophes (PCPPNDAC). An important role in the formulation and management of the Plan for transformation of the civil security system could be rendered to the National Research and Coordination Council to PCPPNDAC.

As a novel concept, the Civil Security Concept is emerging on the basis of two main prerequisites. First, the process of globalization is changing the essence and the role of the state as we know it. We are unable to predict how states and nations will look like in 2050, for instance. The transformation of "traditional" states and nations necessitate transformation of the security sector as a core element of the traditional state. Civil security and human security are the answers that we can give to these global transformation processes from a 2005-perspective.

Secondly, it is a statistical fact that much more people are dying as a result of natural disasters, accidents, and catastrophes in comparison to the victims of terrorist acts or organized crime activities. We are unable to stop natural disasters and catastrophes, but we can optimize our emergency management system and minimize the negative effects. Precisely, this is one of the goals of the Civil Security Concept.

As every definition, the definition of civil security is a hard task that can only be achieved by a higher number of experts. Therefore, in this article we can only give some of the guidelines for a definition. Civil security means the following:

- *Better interdepartmental coordination*. If properly implemented, the broad interpretation of the Law on Crisis Management will lead to the establishment of a civil security system that is legally described as National System for Crisis Response. In this respect, the role of the National Crisis Management Center is crucial.
- *Active civil society participation in the provision of security*. The active civil participation is the connecting link between "traditional" civil protection and civil security. Nowadays security cannot be provided by the state itself. The engagement of civil society becomes indispensable. Civil society structures, NGOs, voluntary local formations as well as business organizations and the scientific community are the potential resource for the establishment of a third pillar of the security sector.
- *Good governance and effective democratic civil control over the security sector*. Participation is the best opportunity for proactive control.
- *New strategic culture of civil society*. The establishment of a civil security element of the security sector is a challenge to the maturity of civil society. The ability of civil society to fill in the vacuum left by the diminishing traditional state fast before organized crime is vital.

The successful transformation of the population and critical infrastructure protection system into a civil security system will be both a test and a major step towards the establishment of an integrated security sector. Even in the case when the civil security system is not developed as a "separate pillar," the Civil Security Concept could become the conceptual basis for a successful security sector transformation process. In this sense, the Civil Security Concept could be interpreted as an upgrade of the Security Sector Integration Concept. Moreover, transcending beyond "national security," the Civil Security Concept gives the opportunity to formulate a Security Sector Maturity Model applicable in the whole Euro-Atlantic geopolitical space.

Implementation of the Architectural Approach to Transformation Planning of Civil Security

Implementation of the concept of civil security requires serious transformation of the existing system for emergency management around the State Agency for Civil Protection and partner organizations as MoD, MoI, and other ministries (transportation, healthcare), local authorities, civil society, and business. A new architecture is needed and an enterprise governance mechanism to manage it. This is the reason to use the methodology of the architectural approach to provide comprehensive analysis, description of the existing system, development of alternatives and their assessment, selection of the end-state model, and planning of the needed steps for transformation.

Transformation planning requires the drafting of a model, goal, and criteria for the assessment of alternatives for the system for population and critical infrastructure protection. This general model is the starting point for the questionnaires for research on the current status, collection of data for future development and selection of a method for qualitative and quantitative optimization of the architecture of the system. The definition of the general model (an "empty" object-oriented model based on the architectural approach) of the system has to begin with a general description of the environment for development of the system at present time – political, economic, social and technological, as well as with an assessment of system's current status (SWOT (strengths, weaknesses, opportunities, threats) and PEST (political, economic, social, technological) analyses). The second step should be the development of alternatives for improvement of the system, selection of a basic alternative and an action plan (or transformation plan) for attaining the target status (or the desired alternative).

The presented study has offered a number of alternatives differing in principle in the major parameters in the description of the two main aspects (layers) of the unified architecture of the system for population and critical infrastructure protection:

- Operational architecture – major risks, goals, working elements, links, information exchange;
- System architecture – main systems for surveillance, monitoring, early warning, alerting, decision-making and management, coordination and planning, reconstruction and prevention, as well as major logical building elements of these systems.

The main areas where different parameters for the alternative models are sought are: risk environment and types of operations of the system for population and critical infrastructure protection; main capabilities necessary for population and critical infrastructure protection; system structure and distribution of obligations and the necessary operational capabilities in compliance with the elements of this structure; partnership among the organizations within the system for population and critical infrastructure protection and international cooperation; system management and forms of public-private partnership; establishment of technical systems – development and use; financial model of functioning of the system for population and critical infrastructure protection.

The optimization should be taking place at three levels:

- Formation of a full range of alternatives and expert screening for plausible options in order to establish a range of differing in quality and internally non-contradicting alternatives;
- Quantitative optimization of each alternative;
- Assessment of the alternatives (quantitatively optimized) and selection of a range of preferred (basic) alternatives.

Qualitative optimization of a mixed alternative could be preferred during the analysis of high-quality alternatives if there are some alternatives ranking close to each other following the complex of criteria.

A springboard for the formation of alternatives could be the description of the current status of the system for population and critical infrastructure protection with an analysis of the problems and alternatives.

The next step, after the formation of the ultimate range of basic (preferred) alternatives, is the analysis and synthesis of the steps of an action plan (transformation plan) for the transformation of the current state into a target state with transition through a number of intermediate states. The goal is to choose the optimal trajectory of transformation, to extract invariant steps and principles of action, which is to guarantee the success of the transition. Due to the limited time for this research and its preliminary character, the goal set is to achieve a strategy for transformation rather than a transformation plan, with a range of variation steps.

There is a whole set of internal and external conditions for implementation of the transformation. The most important internal conditions are as follows: a well-defined term of office and strong leadership, an efficient body for strategic planning and co-ordination (a system of the Planning, Programming and Budgeting type for the system for population and critical infrastructure protection) in the central government, as well as an efficient information system for management that ensures monitoring of key indicators of the transition and real-time response.

Mission of the system for population and critical infrastructure protection used in the study is:

> *Development, maintenance and efficient use of capabilities for prevention, monitoring, due and adequate response and recovery after natural disasters, accidents and emergencies and other considerable negative impacts on the population and critical infrastructure.*[2]

This system has the following *goal* [3]:

> *Minimization of negative consequences*.

Each alternative put forward in this study is assessed on the basis of a common goal. The proposed *Motto* of the system is:

> *From civil protection to higher security from and for Bulgarian citizens and society in the 21st century*.

The criteria for assessment of alternatives, determined as a result of interviews and analysis of data, follow the PEST model similarly to the initial analysis of the status of the population and critical infrastructure protection system through SWAT analysis. The criteria are of the following classes: *political*, *economic*, *social*, *technological*, described in quantifiable terms in a special table for the experts participating in the assessment process.

When the trajectories for attaining the alternatives are defined, apart from the above-mentioned criteria, a definition is also given to "risk"—short-term, mid-term, and long-term—for achievement of the end goal. Each criterion is evaluated on the basis of its importance to the achievement of the goal while each alternative is evaluated for compliance with each criterion.

The cost of transition also plays important role during the development of the transformation plan. The cost is regarded as an additional criterion for selection of an alternative or formation of a multi-layer plan which includes the gradual implementation of various alternatives.

The elaboration of the alternatives is based on:

- Changes in the operational architecture through addition or exclusion of objects, links, and changes in the characteristics of the objects;
- Changes in the system architecture through addition or exclusion of objects, links, and changes in the characteristics of the objects.

Preliminary analysis could help in excluding entire groups of alternatives. The main alternatives are based on separate states of the system for population and critical infrastructure protection within the space of alternatives on the basis of the following "axes:"

- Scope of risks, goals, and corresponding capabilities (broad-narrow);
- Structure of the system for population and critical infrastructure protection (centralized-decentralized);
- Organization of the system for population and critical infrastructure protection (departmental-interdepartmental);
- Type of public-private partnership (strong-poor).

On an expert level, it is possible to add other high-quality alternatives based on difference in another area (apart from risks, structure, organization, and partnership) – specific financial model of operation, specific partnership schemes, etc.

The method for quantitative optimization of alternatives allows the selection of values for the key system parameters. The change of quantitative parameters (e.g., number of elements, centers, capacity) results in additional quantitative alternatives for each option differing in quality. Only the best quantitative alternative is chosen to participate in the general assessment and selection of a pool of quality alternatives.

The method for selection of alternatives differing in quality (already quantitatively optimized) that meet the goal of the system for population and critical infrastructure protection, the criteria for assessment of alternatives and for development and description of the alternatives in terms of the architecture model is implemented through their assessment and ranking compliant with objective methods set in the *Expert Choice* software.

The selected optimal architecture provides the basis for drafting a plan for transformation of the system for population and critical infrastructure protection and its subsequent operation.

The structure of the transformation plan includes:

- Goal of the transformation and criteria for success (factors for measuring progress);
- Stages of transformation and main goals;

- For each stage – steps taken by the corresponding contractors, deadlines, and implementation resources.

The strategy and vision determine the steps in the seven areas of achieving these parameters which are determined as optimal for the selected alternative for development of the system for population and critical infrastructure protection – i.e. who, what, when, how, where, how much, with whom.

1. Risk environment and types of operations of the system for population and critical infrastructure protection;
2. Main capabilities necessary for the protection of population and critical infrastructure;
3. Structure of the system and distribution of responsibilities and necessary operational capabilities compliant with the elements of the structure;
4. Partnerships between the organizations within the system for population and critical infrastructure protection and international cooperation;
5. System management and forms of public-private partnership;
6. Establishment of technical systems – development and use;
7. Financial model of population and critical infrastructure system.

The development of the financial model of the system for population and critical infrastructure protection is assessed, particularly in relation to point 7, following the adopted model of the system for population and infrastructure protection. It is also used to plan the financial policy including the financing of projects for modernization and prevention.

It is possible to present the plan as a network schedule (in *MS Project*) by presenting the steps (actions) of the different groups of participants in the process: National Assembly, government, minister in charge, partner administrations, other public and private partners, including in an international perspective. The management of the implementation of the plan is a key element.

The research and technological foundation is to a great extent independent of the alternative due to the uniqueness of established systems, the need to use them, when it is a matter of national security and consolidation of positions in NATO and EU on issues of population and infrastructure protection. The serious technological slow-down in equipment of systems and even staff training, the lack of research-and-development units could be overcome with the help of the Research Consultative Council and an efficient modernization plan.

Alternatives and Transformation Plan for Bulgarian Civil Security System

In order to facilitate the decision-making process in the national organization for civil / societal security, the research team designed, analyzed and tested through expert assessment a number of alternatives.

Initial basic alternatives were designed along the following axes of a hypercube:

- Scope of the countered risks and threats, respectively tasks and capabilities of the system;
- Level of centralization / decentralization from a territorial perspective and organizational hierarchy;
- Organization from administrative perspective – centralized (in one state "agency")/ decentralized (network of agencies and other players);
- "Ownership" of the system, i.e. level of public-private financing, business and citizen's participation.[4]

Thus, there are 16 boundary variants of the system for protection of the population and the critical infrastructure and a considerably higher number of interim variants. Therefore, the basic alternatives were explored and further elaborated under the following two hypotheses:

(A) The central governmental authorities will preserve considerable power and responsibilities within the system for protection of the population and the critical infrastructure for all basic alternatives; however, the responsibilities and the capacities of local and regional authorities for civil protection will be significantly enhanced. In this case, a centralized administrative structure will maintain administratively and operatively subordinated structures (forces) in several "regional centers" (in our case they could be six in the respective planning regions of the country; it is also possible that the separate structures specialize in different capabilities from a functional point of view), while at local level, the predominant role will be vested in the forms of civil participation for population and critical infrastructure protection, e.g. through structures of a "Civil Guard."[5]

(B) For all basic alternatives, with the exception of alternatives 4 and 5—"Centralization based on the Ministry of Defense" and "Centralization based on the Ministry of the Interior"—the dominant tendency is that of joint public-private financing, i.e. sharing responsibilities for financing among the state, local budgets, NGOs, private business, including operators of critical infrastructure and services, insurance companies, citizens and legal entities.

Under these hypotheses, the research team selected six basic alternatives for detailed description and analysis.

Basic Alternative 1 – Optimization of the current organization

Alternative #1 envisages improvement of the current structure of the State Agency for Civil Protection and concentrates only on the optimization of the work of the existing agency and the coordination of its activities with other state agencies. In practice, this alternative does not lead to the establishment of a *system* for protection of the population and the critical infrastructure, or to the establishment of a civil security system. Basic Alternative #1 is mainly of an intradepartmental nature; it requires the least efforts and resources and, consequently, will lead to a slight change as compared to the current status. A "narrow" scope of risks and capabilities for this alternative means preservation of the current scope of the State Agency for Civil Protection. This alternative could be defined as *preservation of the status quo*.

From a functional perspective, Alternative #1 is targeted at bridging over the following problems in population and critical infrastructure protection: not sufficiently efficient model of commanding interactions and distribution of command information, i.e. a change in the hierarchical model used so far for exchange of information and coordination of decisions and actions; not sufficiently efficient prediction of risks, disasters, accidents and emergencies, i.e. improvement of prevention; lack of 100% coordination among rescue teams in different ministries, agencies and administrations (State Agency for Civil Protection, Ministry of Defense, Ministry of the Interior, medical teams, etc.).

A major weakness of Alternative #1 is that it will not neutralize the problems of interdepartmental coordination in time of disasters, accidents and emergencies. From an institutional perspective, Alternative #1 is based on a number of organizational and technological activities of the State Agency for Civil Protection, such as establishment of a Center for collection, processing and distribution of space information; establishment and maintenance of a central Register of critical infrastructure; establishment of a unit for psychological protection of the population in case of disasters, accidents or emergencies (possibly within the framework of the Information and Public Relations division of the State Agency for Civil Protection; optimization of the system for emergency management, particularly through developing capacities for field management.

Basic Alternative 2 – Optimization of the Operational Coordination

Alternative #2 envisages significant optimization of operational coordination among different units in charge of population and critical infrastructure protection. This alternative is part of the philosophy of the draft Law on Crisis Management. Its imple-

mentation presupposes the following steps: adoption of the Law on Crisis Management, establishment of a National Center for Crisis Management, the initial experience from the practical implementation of the Law and its "narrow interpretation" for a limited scope of risks. This alternative encompasses mainly two lines of activities: establishment of a crisis response system under the Law on Crisis Management, along with the National Center for Crisis Management to the Security Council at the Council of Ministers, Security and Crisis Management Councils with the Ministers and other central authorities of executive power, security and crisis management councils with the regional governors and mayors of municipalities, as well as crisis response forces; establishment of interdepartmental "mutual trust" among the structures of the newly-built system for response to crises, the "traditional" structures for population and infrastructure protection – the State Agency for Civil Protection, PCPPNDAC and the "traditional" power ministries (the Interior Ministry and the Defense Ministry).

In the case of this alternative, several organizations with different traditions and culture will coordinate their action plans for crisis situations. They are expected to regularly train the management and crisis situations response procedures within the framework of joint exercises. What is more, their actions in emergency situations will be controlled by a unified, integrated management system. "Narrow" scope of risks and capabilities under this alternative means preservation of the current scope of the State Agency for Civil Protection.

According to the research team, in Basic Alternative 2 the "operational coordination" between the State Agency for Civil Protection, the National Center for Crisis Management and the inevitable third parties (the Interior and the Defense ministries, as a minimum) will be accompanied by a "timid" application of the newly-adopted Law on Crisis Management and mutual testing of "partners," and in the worst case the end result will be mutual blockage of separate activities. Due to the vague normative regulations, this alternative gives to the traditional power ministries the opportunity to take over the initiative in the system for crisis management, as well as to dominate the structures for citizen and infrastructure protection. This alternative could be defined as an alternative to the fragile interdepartmental balance. It requires certain vision and efforts for the implementation of the expected final results.

Basic Alternative 3 – Interdepartmental coordination of capabilities development and operations (maximum interdepartmental coordination, a prerequisite for integrated population and critical infrastructure protection)

In addition to the operational coordination, Basic Alternative 3 envisages the coordination of plans for development of capabilities for protection of the population and the critical infrastructure between several agencies (possibly of major participants

outside the executive power, too) and the fulfillment of those plans. The implementation of the alternative presupposes a broader interpretation and application of the Law on Crisis Management, including development and adoption of a number of additional normative documents. Alternative #3 assumes a higher degree of integration of the crisis response system and the existing structures for population and infrastructure protection. Key role in this alternative is played by the State Agency for Civil Protection, the National Center for Crisis Management to the Security Council, and PCPPNDEA. For a more efficient integration, the "power vice premier" may play a significant role. A permanent interdepartmental group or an administrative structure to the Council of Ministers may be set up with the "power vice premier."

Several organizations in this alternative will coordinate not only their action plans for crisis situations, but will jointly draft plans for development of related capabilities, for use of financial means and for technological optimization (acquisition of new means and systems). What is more important, they will be supposed to coordinate the development of normative documents for use of the "forces," means (statutes, instructions and other by-law regulatory documents) and their decisions for dislocation of "forces" and means; they will jointly use training ranges, storehouse facilities, different types of technical means and equipment; they will apply unified requirements to the training and preparation and will even use in coordination education, research and scientific resources. Thus, in practice, the organizations will be functioning within the framework of an integrated system for management, including for ongoing control of decision implementation with regards to developed capabilities, provision, preparation and delivery of new equipment. An "enlarged" scope of risks and capabilities in this alternative means enlargement of the present scope of the State Agency for Civil Protection and incorporation of new risks, capabilities and activities.

The implementation of this alternative may to a high extent require strong leadership, managerial experience and ability to accomplish the targeted goals and tasks.

Alternative #3 could be discussed as "almost a ministry, while a ministry is actually not set up." Its implementation will to a large extent improve interdepartmental operational coordination, and, what is more important will help in the establishment of coordination development plans. The advantage of this alternative is that the protection of population and infrastructure and crisis response activities will be improved without the establishment of a new ministry, which otherwise will be very likely perceived as an "empty" and useless ministry in the public eyes. Alternative #3 could be seen as a proper step in the formation of a "new ministry" that will help in the accumulation of experience and expertise for the actual establishment of such a ministry. This alternative broadens the scope of work from "traditional" civil protection to civil security.

Basic Alternative 4 – Integration into the Ministry of Defense and ***Basic Alternative 5*** – Integration into the Ministry of the Interior.

These two alternatives envisage integration of the existing structures for population and infrastructure protection into the Ministry of Defense and of the Interior. Each of the two alternatives is in practice a step backwards from an organizational perspective. These alternatives are often based on practice adopted in several European countries. It is a fact, however, that the discussion on these issues goes on in a number of European countries (Sweden, Norway, Germany, etc.) and there is a tendency towards the separation of civil security as a "third pillar" of the security sector. The integration of the structures for population and infrastructure protection in some of the power administrations eliminates in practice the possible implementation of the civil security concept and the idea for initiative, contribution and self-organization of citizens for the protection of population and critical infrastructure. An "enlarged' scope of risks and capabilities in these alternatives means the enlargement of the present scope of civil protection in a direction of including new risks, capabilities, and activities within the competence of the corresponding ministry.

Basic Alternative 6 – Ministry of Civil Security

The establishment of a new Ministry of Civil Security to a large extent corresponds to the formation of an integrated security sector in Bulgaria and a separate "third pillar." As a separate ministry, the Ministry of Civil Security is intended to bridge the gap between the system of national security (at a macro-level) and the system of population and infrastructure protection (at a micro-level). A new Ministry of Civil Security will enable the coverage of a larger scope of risks and will, apart from that, permit a more active civil participation through voluntary paramilitary formations, through the structures of civil society and business. An "enlarged" scope of risks and capabilities in this alternative means enlargement of the present scope of the State Agency for Civil Protection to cover new risks, capabilities, and activities.

The Ministry of Civil Security could be partially established based on the experience of the *Department of Homeland Security* (in the US) and the Ministry of Emergency Situations (in Russia and Ukraine), on one hand, and on the Bulgarian traditions, capabilities and realities, on the other. The Ministry of Civil Security is to include organizational units based on the following current state agencies:

- The State Agency for Civil Protection;
- The State Agency for Refugees;
- The State Reserve and Wartime Stocks State Agency;

- The newly established agencies, including "Civil Security Services" Agency – a new agency which is to coordinate and control the work of paramilitary voluntary formations (Civil Security services) set up with the regional governors.

The establishment of a Ministry of Civil Security raises the issue of the institutional place of several other agencies and services directly related to the provision of civil security – namely, the National Service "Fire and Emergency Safety," which is currently a structure within the Ministry of the Interior. Since the National Service "Fire and Emergency Safety" is an important element of the citizen and infrastructure protection system, it is logical to include it in a possible Ministry of Civil Security in the future.

These six alternatives were described and analyzed within the context of the following factors and circumstances (divided in four groups), characterizing both the present and future target state of the system for protection of the population and the critical infrastructure:

- *Vision*. The establishment of the present system is compliant with the requirements of a totally different social and political system and threats and this necessitates adequate changes and optimization pursuant to new realities: market environment of social development; increasing significance of critical information infrastructure protection; implementation of the idea for initiative, contribution and self-organization of citizens for protection of the population and critical infrastructure; implementation of efficient monitoring and prevention.
- *Capacity*. It is necessary to maintain an integrated combination of capabilities, optimally distributed among different organizational structures. The main groups of system capabilities are: monitoring; early warning; preparation of the forces, population, infrastructure, system; readiness; rapid reaction; augmentation of response efforts; reconstruction; reduction of vulnerability [6] and other types of prevention.[7]
- *Financial and economic state*. The maintenance of such capabilities should be compliant in volume and type with the resource capacities of the state and the principles of good governance in democratic societies.
- *Management*. Decentralization will enhance responsibilities and motivation of the individual local structures, while the central structure should provide for efficient coordination and active development of necessary capabilities. The central coordination structure should develop and apply consistently a number of functional strategies and programs for: capability development; human resources optimization; technological modernization of the necessary equipment; efficient financial management and investment attraction, including based on joint ownership and development of public-private partnership; development

of information-management and legal and normative framework of the system for population and critical infrastructure protection.

The expert analysis determines Basic Alternatives #2, #3, and #6 as fully compliant with the mission of the population and critical infrastructure protection system, with its scope and capacities, and with the resource provision which Bulgaria is able to guarantee.

Transformation also depends on the price of transition, which is seen as an additional criterion for selection of a final alternative or the formation of a transformation plan that includes the consistent implementation of a number of specific steps.

The results from the assessment and ranking of these alternatives are presented in Table 1. These results determine the selection of Basic Alternative #3—*broad interpretation of the Law on Crisis Management*—as the most suitable of the three basic alternatives for implementation in Bulgaria.

At this stage, the results of the analysis and the assessment show that:

- The optimization of the system for civil protection is related to more serious reforms and evolutionary improvement of the existing system with a focus on joint planning, preparation, common process for acquisition of capabilities;
- The fast transition to establishment of a Ministry of Civil Security raises suspicion of bureaucracy and shifts the focus from rescue teams and work at the local level to complicated procedures in the center.

Table 1: Summarized Expert Assessment of the Basic Alternatives.

	Alternative		
	Optimization of the operational coordination	Interdepartmental coordination of capabilities development and operations (maximum interdepartmental coordination, prerequisite for integrated population and critical infrastructure protection)	Ministry of Civil Security
	Draft Law on Crisis Management (Alternative #2)	**Broad interpretation of the Law on Crisis Management (Alternative #3)**	**Ministry (Alternative #6)**
Summarized expert assessment with EXPERT CHOICE	**0.192**	**0.420**	**0.387**

- The expectations from the adoption and implementation of the Law on Crisis Management are great and the achieved results will be of key importance for choosing the next steps.
- The complexity of analysis and assessment of the three alternatives suggests that the implementation of the Law on Crisis Management will be a difficult process, which requires a further development of this research following a similar methodology.

The main conclusion is that the expert opinion is seriously in favor of an integration of the crisis response system based on a broad interpretation of the Law on Crisis Management, which is very close to the establishment of a Ministry of Civil Security.

Main Steps in the Transformation of the System for Protection of Population and Critical Infrastructure

The main steps in the transformation of the system for protection of population and critical infrastructure could be divided into two groups: (1) invariant steps (unrelated to the selected alternative); and (2) steps whose detailed definition and/or implementation depends on the choice of alternative.

The invariant steps are:

Steps for development of normative base

- *Concept* of the system for protection of population and critical infrastructure (civil security system);
- *Strategy* for building up this system;
- Normative base for the development of public-private partnership for the protection of population and critical infrastructure – at a central level, at a local level, in the establishment and maintenance of specialized capabilities and means;
- Normative base regulating the protection of critical infrastructure, as well as the protection of critical information infrastructure in particular.

Steps for the introduction of principles and practices for efficient inclusion of citizens in the provision of security through the formation of voluntary paramilitary formations – the US National Guard and the UK Territorial Army could be used as a model for the establishment of these formations of civil security (establishment of Civil Security services with the regional governors).

Steps for introduction of principles and practices for efficient management

- Development and maintenance of a unified architecture of the system for population and critical infrastructure protection;

- Development of "sector architectures:" of a system for risk prediction and assessment; for integration of fixed and field communications and information systems; for collection, processing and distribution of space (aerospace) information, etc;
- Introduction of procedures and system for program management of the resources for protection of population and critical infrastructure;
- Introduction of efficient financial management and investment attraction, including on the basis of joint ownership (public-private partnership);
- Creation, testing and introduction of mechanisms (procedures for action, interaction, authorities, registries and other information systems) for the protection of critical infrastructure, including critical information infrastructure;
- Introduction of methods, models and systems for decision support, including the adaptation of models developed by the NATO C3 Agency and EU and NATO member-states.

Steps for research support

- Development of a model structuring the necessary capabilities for population and critical infrastructure protection according to risks and tasks, on one hand, and providing organization (the latter depends on the selected alternative), on the other hand;
- Development of a model of critical infrastructure and targeted analysis;
- Assessment of infrastructure interdependencies;
- Identification of critical sites and subordinations;
- Analysis of vulnerability to accidental and premeditated acts;
- Assessment of alternative proposals for increase of infrastructure robustness, including an analysis according to the "price-benefits" criterion;
- Development of a model of critical *information* infrastructure, vulnerability assessment, correlations, and risk;
- Assessment of the capabilities and development of a concept for the use of UAVs within the system for population and critical infrastructure protection.

Steps for technological optimization

- Optimization of the National Centre for Crisis Management (specification of information systems, decision support systems, systems for communications support, etc.)
- Establishment of a Center for collection, processing, and distribution of space and aerospace information;

- Participation in the development of a national system for monitoring of the radiation, chemical, biological, and bacteriological situation;
- Introduction of packages of modules for field emergency management.

The institution in charge of the implementation of these steps is the Security Council to the Council of Ministers (PCPPNDAC) and the State Agency for Civil Protection.

Steps for staff education and training

- Development of coordinated programs for staff education, training and further development according to the types of capabilities, risks, participants in the system for population and critical infrastructure protection – depending on the organizational affiliation and the extent of maintained preparedness for action;
- Development and application of unified education and training requirements to the staff within the system for population and critical infrastructure protection;
- Development of qualification requirements taking into consideration the specifics of the types of capabilities, risks, and the role within the system for civil security;
- Development and implementation of joint training programs.

Public awareness steps

- Development of coordinated programs for raising the public awareness of the need for the undergoing transformation within the system for population and critical infrastructure protection.

Steps for development of international cooperation

- Development of legal and normative basis and procedures / mechanisms for coordination of actions with other countries in the region, the European Union, and NATO.
- Consolidation of the participation in international organizations and initiatives.

The list of steps for transformation depending on the selected basic alternative is also of considerable length. The list could be studied after definition of the preferred alternative by the Council of Ministers and the Parliament.

Conclusions

The development of the Civil Security System is one good example of the transformation effort. It is a process that requires specific methodology to be implemented and the key is the interdisciplinary character of the issue. Based on the experience of the CNSDR-BAS in many similar projects—from White Paper on Defense through transformation of the largest defense company TEREM to the White Paper on Civil

Security—an idea to form a Center of Excellence in Security Sector Transformation (CoE in SST) has been developed. The Center could consist of:

1. Communication and Information Infrastructure (CII);
2. Working Groups (WG);
3. Knowledge Infrastructure (KI);
4. Expert Network (EN).

CII includes central hub with servers and workstations connected to the Internet and distributed virtual network of workstations of the WG members. *WG* are in the following areas: WG1 – Security Policy and Strategies; WG2 – Integrated Security Sector Architecture and Change Management; WG3 – New Technologies in Security and Defense.

KI consists of theoretical models in security and security sector areas; computer (software) models; literature and selected publications; accomplished projects in CoE; produced papers. KI is managed by a set of matrices to establish cross reference between problems and methods to support their solution in order to easily form strategies (networks) of steps for decision making.

One of the key elements of the CoE is the *Expert Network* built around the participation in conferences, editorial boards, NATO SC panels, PfP Consortium, DCAF, CESS, and other international security-related organizations and programs. Of course, the EN is extension to the WG and KI. One of the key elements of the EN / KI is the capability to deliver knowledge through different courses, including in an ADL / CAX environment.

Development of such a type of support to decision making and to the implementation of security sector transformation is proved to be critical especially for problems of building architecture for network-based capabilities.

In this direction is the current NATO Science for Peace Project SFP-981149 for building new capabilities in Decision Making Support for the Bulgarian Security Sector "*Operations Research Support to Force and Operations Planning in the New Security Environment*." The project aims to provide timely and effective scientific support, drawing on existing and developing novel operations research methods and models, in order to meet current and anticipated needs of end users from defense establishments, ministries of interior and civil protection agencies both in decision making process / change management and support of computer aided exercises. In addition, project results will be incorporated in the curricula of Bulgaria's Defense and Staff College and the Academy of the Ministry of the Interior.

Through this project Bulgaria will establish a Centre of Excellence in Operations Research (OR), attracting promising young scientists, conducting cutting-edge research on force and security-sector transformation and network-enabled operations, and facilitating the integration within the NATO's OR community. The project networks the supplementary capabilities of several academic and research organizations from Bulgaria (the C4ISR Laboratory of the Institute for Parallel Processing and the Operations Research Department of the Institute of Mathematics and Informatics, both at the Bulgarian Academy of Sciences, supported by many other institutes as Institute for Parallel Processing, and the Defense and Force Management Department of the Rakovsky Defense and Staff College), from Germany (Niemeyer Operations Analyses), and The Netherlands (the Operations Research and Business Management Division at TNO Defense, Security and Safety).

Best way to achieve comprehensive understanding of the security and to plan transformation of the security institutions in an integrated security sector is through multidisciplinary joint / multinational studies. As in the theory and practice of computer networks, the architectural approach is proved as a best tool – such instrument is needed for change management in the area of security and security sector. The presented project is one practical implementation of this idea to be tested further in real environment by supporting the implementation of the just approved Crisis Management Law.

Acknowledgement

This research is sponsored by NATO's Scientific Affairs Division in the framework of the Science for Peace Program through project SfP 981149 "Operations Research Support to Force and Operations Planning in the New Security Environment" and by the Permanent Committee for Protection of the Population against Natural Disasters, Accidents and Emergencies of the Council of Ministers of the Republic of Bulgaria.

References:

1. Alan Bryden and Heiner Hanggi, eds., *Reform and Reconstruction of the Security Sector* (Münster: Lit Verlag, 2004).
2. Bengt Sundelius, "The Challenge of Security Threats and Emergencies in Modern Society," in *Societal Security and Crisis Management in the 21st Century* (Stockholm: Swedish Emergency Management Agency, April 2004): 17-19.
3. Doron Zimmermann, "Between Minimum Force and Maximum Violence: Combating Political Violence Movements with Third Force Options," *Connections: The Quarterly Journal* 4, no. 1 (Spring 2005): 43-60.

4. Eden Cole, Timothy Donais, and Philipp H. Fluri, eds., *Defence and Security Sector Governance and Reform in South East Europe* (Baden-Baden: Nomos, 2005).
5. Forum Report on Critical Infrastructure and Continuity of Services in an Increasingly Interdependent World (Geneva: Geneva Centre for Security Policy, October 2003).
6. Philipp H. Fluri and Velizar Shalamanov, eds., *Security Sector Reform – Does It Work?: Problems of Civil-Military and Interagency Cooperation in the Security Sector* (Geneva/Sofia: DCAF and GCMA, 2003), 240 p.
7. *Societal Security and Crisis Management in the 21st Century*, Proceedings of the 6th CRN Expert Workshop (Stockholm: Swedish Emergency Management Agency, April 22-24, 2004).
8. Valeri Ratchev, Velizar Shalamanov, and Todor Tagarev, "Reshaping Bulgarian Armed Forces for the 21st Century," in *Bulgaria for NATO 2002*, ed. Ognyan Minchev, Valeri Ratchev, and Marin Lessenski (Sofia: Institute for Regional and International Studies, 2002), 204-278.
10. Velizar Shalamanov, "Progress and Problems in Security Sector reform in Western Balkans: Is there a Universal Solution?" in *Security Sector Governance in the Western Balkans 2004*, ed. Istvan Gyrmati and Scott Vesel (Baden-Baden: Nomos, 2004), 51-66.
11. Velizar Shalamanov and Todor Tagarev, "Transforming the Security Sector in the Context of the Euroatlantic Integration. Developing Capabilities for Effective Contribution to NATO," in *Bulgaria's Roadmap to NATO beyond Prague*, ed. Konstantin Dimitrov (Sofia: Institute for Euroatlantic Security, 2004), 68-85.

Notes:

[1] We should add to these three pillars also foreign politics and diplomacy (particularly the protection of Bulgarian nationals and property abroad) conducted by the Ministry of Foreign Affairs.

[2] With regards to infrastructure, the function "monitoring" is implemented only in relation to the one defined as critical.

[3] This definition of goal allows the application of methods for qualitative assessment and optimization.

[4] Known as "public-private partnership."

[5] At this stage there is no such or similar organization in Bulgaria

[6] In principle, one of the results of systematized efforts for risk management (mitigation).

[7] As far as this is technically possible and expedient from a resource perspective.

VELIZAR SHALAMANOV is Senior Research Fellow and Head of the C4 section of the Institute for Parallel Processing of the Bulgarian Academy of Sciences. He is advisor to the President of the Bulgarian Academy of Sciences on security and defense issues and Chairman of "George C. Marshall"-Bulgaria. From November 1998 till July 2001 Dr. Shalamanov was Deputy Minister of Defense, responsible for defense policy and planning. He has more than 150 publications in the areas of CIS architecture and development, information warfare, decision support, national and regional security policy, defense planning and reengineering. Dr. Shalamanov is co-founder of the AFCEA-Sofia Chapter and the Business Executives for National Security – Bulgaria. He serves on the International Advisory Board of DCAF. *E-mail:* Shalamanov@GCMarshall.bg.

STEFAN HADJITODOROV is Director of the Center for National Security and Defense Research at the Bulgarian Academy of Sciences and Scientific Secretary of the Academy. He

holds M.Sc. degrees in Control Engineering (1978) and in Applied Mathematics (1979) and Ph.D. degree in Cybernetics (1983) – all from the Technical University of Sofia, Bulgaria. Prof. Hadjitodorov is Scientific Secretary of the Bulgarian Academy of Sciences since 1991 and Secretary of the Scientific Coordination Council to the Interdepartmental Committee for Protection of the Population in natural disasters, industrial accidents, and catastrophes since its establishment in 2003. *E-mail:* sthadj@argo.bas.bg.

STOYAN AVRAMOV is Research Fellow and Head of the C4ISR Laboratory of the Space Research Institute of the Bulgarian Academy of Sciences. He graduated from the Bulgarian Air Force Academy in 1984 with a M.Sc. Degree in Electronics Engineering and Received a Ph.D. degree in Radar Systems and Technologies from the Zhukovsky Air Force Engineering Academy in Moscow, Russia, in 1991. Until 1995, he served in the Bulgarian Air Force in a variety of positions related to the development of automated C2 systems. Dr. Avramov is member of the Editorial Board of *Information & Security: An International Journal*. He specializes in technology integration, system design, prototyping, and advanced technology demonstrations. *E-mail*: stav@digsys.bg.

TODOR TAGAREV is Associate Professor and Chair of the Defense and Force Management Department of "G.S. Rakovski" Defense and Staff College, Sofia, Bulgaria. He was the first Director of the Defense Planning Directorate since its establishment in early 1999. From May until late 2001, he served as Director for Armaments Policy in the Bulgarian Ministry of Defense and National Armaments Director. Among other duties, he coordinated all defense modernization and R&D programs in support of defense reform and NATO integration. He graduated from the Bulgarian Air Force Academy in 1982 and received a PhD degree in systems and control from Zhukovsky Air Force Engineering Academy, Moscow, in 1989. Dr. Tagarev is a 1994 Distinguished Graduate of the US Air Command and Staff College at Maxwell Air Force Base, Ala., and a 1994 Distinguished Young AFCEAn. Dr. Tagarev is Managing Editor of Information & Security: An International Journal. *E-mail*: infosec@procon.bg.

VALENTIN STOYANOV is Coordinator and System Manager at the Center for National Security and Defense Research – Bulgarian Academy of Sciences. He is also Research fellow at the Institute of Control and System Research – BAS. He holds M.Sc. degree in Automatic Control Systems from the Technical University in Sofia (1980) and is alumnus from the High Military School in Shoumen. Mr. Stoyanov has worked as System engineer at the Ministry of Defense of Bulgaria and in private companies. His main research interests are national security, defense and system architectures. *E-mail:* v_sto@mail.orbitel.bg

PENCHO GENESHKY is Coordinator at the Center for National Security and Defense Research – Bulgarian Academy of Sciences. He holds MA in engineering from the Technical University of Dresden. From 1978 till 1999 he worked at the Military Technical Institute of the Ministry of Defense. He held also administrative positions at the Headquarters of the Bulgarian Academy of Sciences. His main research interests are national security and defense. *E-mail:* geneshky@yahoo.de

NIKOLAY PAVLOV is Coordinator at the Center for National Security and Defense Research – Bulgarian Academy of Sciences. He holds a MA in International Relations and is presently a PhD aspirant in International Relations and International Security at the Faculty of Law in Sofia University "St. Kliment Ohridski." His main research interests are national security, security sector reform, nation-building and psychological operations (PsyOps). *E-mail:* nikolay_pavlov@abv.bg

Critical Infrastructure Protection

- Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations
- Simulation of Critical Infrastructures

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: ANALYSIS, EVALUATION AND EXPECTATIONS

Eugene NICKOLOV

Abstract: The article provides a brief description of critical information infrastructure and analyzes the extent to which organizations depend on the proper functioning of banking and financial services, electricity, fuel and water supply networks, as well as information and telecommunication networks. The consequences of attacks on specific elements of these infrastructures are examined, as well as the initiatives and problems that arise with their protection on national and international level. Special attention is paid to the state of critical infrastructure protection in Bulgaria, with analysis of the reasons for its poor level and recommendations for improvement.

Keywords: Critical Information Infrastructure Protection, Information Security, Malware Attacks, Vulnerabilities, National Cybersecurity.

Introduction

The information revolution and the spread of Internet are stimulating globalization and allowing corporations to conduct business around the world. Communication technologies improve the productivity, efficiency and competitiveness of organizations around the globe. Today, organizations are outsourcing much of their business, consolidating operations by tunneling data to one central processing location, and using the Internet to cut down operation costs and overhead. With the increasing number of transactions, enormous amounts of data with varying degrees of protection are flowing over the Internet.

On the other hand, modern society has become much more dependent on the availability, reliability, safety and security of many technological infrastructures. Both because of the significant social and economic benefits they provide as well as because of the serious consequences of their malfunctioning, information systems have become a necessity for human well-being. Infrastructures considered critical are those physical and information-based facilities, networks and assets, which if damaged

would have a serious impact on the well-being of citizens, proper functioning of governments and industries or other adverse effects. The following infrastructures need to be functioning at least at a minimal level for the public and private sectors to be able to survive:

- Electricity, fuel and water supply;
- Transportation and communication systems;
- Food supply and waste management;
- Finance and insurance;
- Information and telecommunication networks;
- Military and defense systems, civil protection;
- Emergency, health and rescue services;
- Public agencies and administration, justice system;
- Media, major research establishments, etc.

The energy supply and the communication systems can be regarded as crucial since the rest of the infrastructures depend on them in order to function properly.

Although in the past many of these systems have been physically separated since the technology boom and the change of market dynamics in the 1970s, critical infrastructures have progressively converged and become dependent of information structures such as the public telephone network, the Internet, terrestrial and satellite wireless networks for a variety of information management, communications, and control functions. Technological progress has lead to more automation in the operation and control of critical infrastructures and the creation of a special information infrastructure. Recently, this infrastructure has emerged as one of the most important critical infrastructures because it is the base for managing and integrating all other critical infrastructures as well as new forms of communication, information exchange and commerce. This symbiosis is a national security priority, since the information infrastructure is crucial for economic progress, military and civilian government operations. In particular, the government and military information infrastructures depend on commercial telecommunications providers for everything from logistics and transport to personnel and travel functions. The extent to which these systems are intertwined increases the effects of any malfunctioning since they are spread across different infrastructures, affecting a wide range of users.

Furthermore, the greater role of information and the availability of electronic means to collect, analyze and modify it, have transformed information and information systems both into an invaluable asset and a lucrative target.

Following this train of thoughts, one should place the destructive potential of cyber-war in between nuclear and conventional war although currently tools for cyber attacks are developed in 120 countries, and nuclear arms – in 20 countries.

Vulnerability of Critical Infrastructure

The increased interdependency combined with greater operational complexity, has made critical infrastructures particularly vulnerable to natural hazards, human error and technical problems as well as new forms of cyber crime, terrorism and warfare. Each of these events can result in severe service deterioration or outright infrastructure failure. The technology development and the struggle towards complete automation have reduced our ability to incorporate the necessary safety features, including detection, prevention and mitigation standards and practices. The vulnerability created by these gaps affects not only utility services, but also databases and systems that maintain a variety of sensitive and confidential information.[1]

Many of our most critical systems are extremely vulnerable to natural disasters such as earthquakes, inclement weather, etc. Even when they are not physically impacted, sudden demand surges during crises can provoke blackouts, leading to loss or denial of service. Similar scenarios can occur through deliberate or accidental human action. The Critical Information Infrastructure (CII) has become especially vulnerable to fun-seeking hackers, criminals and even state actors and terrorists. The main tools used to attack critical systems are malware (computer viruses, worms, logical bombs, trojans) that modify and destroy information or block the computer systems. Tools for eavesdropping of information exchange in computer networks as well as tools for modifying the normal function of the computer network and blocking the access to its services are also widely used for destructive purposes.

These automated tools allow intrusions from remote systems to be done within a few seconds which makes Internet attacks easy to launch and increasingly hard to trace.

The Enemy Is Really Dangerous

Underestimating the abilities, knowledge and experience of cyber terrorists could be fatal for critical infrastructures. Some Islamic fundamentalists declared that Al-Qaeda and other Islamic fundamentalist groups plan to use the Internet as a weapon against CII in the US and Western Europe. A leader of a fundamentalist organization said recently: “We will soon be the witnesses of attack to the stock exchanges in New York, London and Tokyo.”

The variety of activities undertaken by hackers is enormous: attacks on systems with insecure perimeters, use of third-party web pages for nationalist propaganda, e-mail bombs that overwhelm servers at organizations they are protesting against, zombie

computers deployed across the Internet serve as remote controls for attacks. In some countries even the government is involved by approving official documents for the preparation and execution of cyber attacks.

Most cases of CII breach are easy to perform since the vulnerabilities or configuration errors as well as detailed how-to guides are available for everyone on the Internet. However, the background knowledge required to perform the intrusion is steadily decreasing, thus increasing the overall success rate of intrusions. All one needs in order to initiate an information structure attack is a personal computer connected to the Internet and an e-mail program, while organizations trying to prevent intrusions are usually constrained by both staff and equipment shortage. End-users are often left to train themselves; new employees may not possess the same level of knowledge as incumbents about system capabilities, potential vulnerabilities or risk reduction measures.

Due to the increasing pressure to reduce production time, a new surge in the number of computer and network vulnerabilities is to be expected. Therefore, one should plan for infrastructures that have built-in instability, critical points of failure, and extensive interdependencies. Furthermore, more and more CIIs are becoming privately-held or owned by foreign nations.

CII attacks include:

- Unauthorized access to sensitive or confidential information;
- Destruction, modification or substitution of software needed by critical infrastructures;
- Limited access for the agents able to prevent or mitigate the results of the attacks.

The possible consequences from critical infrastructure attacks include:

- Blocked transportation, electricity and water supply, communications, data transmission, nuclear power plants, air-traffic control;
- Bankruptcy of commercial structures and financial systems, failure of international business transactions, destabilization of markets and financial institutions, money and information theft;
- Loss of intellectual property or reputation (due to a worm attack the company for on-line payments PayPal was facing a bankruptcy in 2002);
- Human victims or material losses, provoked by the destructive use of critical infrastructure elements (cyber sabotage in the food industry, air or railway traffic);
- Unauthorized access and/or modification of personal information;

- Possibility for imputing terrorist acts to other country/government and aggravation of the tension in international relations.

While the actual restoration of the CII is often a quick and easy task, the indirect effects of even the shortest failures can be felt for a while. CII attacks can seriously undermine public and business confidence in electronic commerce and government initiatives. The human and economic costs associated with recovery or mitigation strategies are enormous. The loss of business and productivity is now measured in billions of dollars from each world-wide virus attack, and even the largest software vendors are hard-pressed to keep up with security enhancements.

Measures for CII Protection

The CII Protection (CIIP) has three strategic objectives [2]:

- Prevent cyber attacks against critical infrastructures;
- Reduce national vulnerabilities to cyber attacks;
- Minimize damage and recovery time from cyber attacks that do occur.

In order to achieve these objectives a new strategy is needed; one that incorporates more than just the technological issues and includes the following elements:

- Taking preventive measures at all levels;
- Improving early detection and rapid reaction capabilities, both for damage control and pursuit of the culprits;
- Limiting the impact of disruptions on government and society;
- Ensuring that the affected systems continue to function at a minimum level or can be restored within the shortest possible time.

Threats and vulnerabilities consist of physical, informational and psychological components; therefore, an open, non-hierarchical dialogue on newly recognized vulnerabilities is needed and physical, informational and psychological protective measures have to be defined.

Measures on National Level

Five national priorities can be defined:

1. Establishing a national cyberspace security response system.
2. Developing a national cyberspace security threat and vulnerability reduction program.
3. Creating national cyberspace security awareness and training program.
4. Securing government systems.

5. Strengthening national security and international cooperation on cyber security.

The framework for CIIP at national level has to be considered in the wider context of the business, social, and technical environment. CIIP requires a multidisciplinary response incorporating technical, management and educational solutions. Both vendors and consumers need to prioritize better security in their products. Companies must adopt and share their best practices. The third approach is to promote better understanding of computer security and ethics through public education efforts. This program requires improved communication and coordination at three levels – within the industry, between the industry and the government, and within governmental structures and bodies.

Protection of the CII within Enterprises and among Industries

The most important factors for critical infrastructure vulnerability in the enterprises include:

- Large staff;
- Numerous physical facilities;
- Wide availability of phone numbers;
- Lack of security training;
- Lack of a system for data classification;
- Lack of procedure for reporting and reacting to incidents.

The measures that could be undertaken include:

- *Physical Protection of the Key Elements of CII.* Depending on the business, it may be necessary to install badge swipes, access codes or hire security guards. Cable locks, alarms, motion detectors, antitheft systems, biometric scanners, etc., could also come in useful. Electronic keypads on server rooms that are not shut off in the event of power loss may be necessary for some companies. These are just a few example physical security measures needed to secure a facility.
- *Technical Measures – Technical Security.* They include use of e-mail and file encryption to conceal the operations and prevent sensitive data from unauthorized disclosure, whether national security secrets or private customer account data or confidential proprietary information. Firewalls, intrusion detection systems, access control lists, strong password policy, and anti-virus software are also components that companies may need.
- *Social Measures - Staff Training and Control.* A background check on new employees is an excellent security measure. This is a good defense measure from

an information warfare standpoint. It informs employers whom they are hiring before the new employee has any physical access to a facility and sensitive documents.

User training is a huge step in the right direction. All employees have to be trained to lock their computer screens when they leave their desks, to use strong password management schemes, to know the methods of social engineering so that they do not end up revealing any confidential information. When employees feel personally involved in protecting the company or agency they work for, they tend to take more pride in what they do. The more they understand the policies set forth, the less potential problems will arise in future.

- *Security Policy*. All technical and social measures have to be implemented with a strong security policy that should:
    - Define what the user wants to protect;
    - Analyze what it is the user wants to protect it from;
    - Explain how the user intends to protect it.

  The policy must be updated regularly, signed off by management, and everyone in the IT department must be familiar with it.

  The overall security policy will address such areas as:
    - Physical security of the data and systems;
    - Access control to the data and systems;
    - Data integrity and availability;
    - Contingency and recovery plans.

  To be effective, the security policy must be both inclusive and dynamic. To be successful, it must have realistic goals and be phrased in a way that is simple and short enough to ensure it is understood and followed by all users.

Public / Private Cooperation between Industry and Government

Due to the large number of private actors that own or use CIIs, forming public-private partnerships is an important part of CIIP.[3] These partnerships should include:

- Problems and threats to national CII;
- Alerting software and hardware vendors to the security and the protection of their products;
- Fast and efficient reaction to all incidents related to the functioning of critical systems;
- Creation of systems for formal and informal sharing of information about computer related crimes and cyber terrorism.

Looking into more detail at the last item, it is clear that the private sector and law enforcement must gather and share information about threats, vulnerabilities, remedies and successful operating models of cyber security. To improve CIIP, industries have to share some information about incidents and damages with the government and the public, even when information sharing is damaging for the company itself. Only complete disclosure of information both in the private sector and the government could even the potential of the attackers and the defenders of the CII.

On the other hand, sharing CII has some negative side effects both to public and private interests. Information sharing could be regarded as price fixing, unreasonable restraint to trade, or systematic discrimination against certain customers. It also could raise privacy concerns, expose proprietary corporate secrets, and reveal weaknesses and vulnerabilities that erode public confidence and invite hackers. Retailers and credit card issuers often worry that disclosing any problems with the security of online transactions (e.g., hackers gaining access to credit card numbers or purchase history) may undermine public confidence in Internet commerce, to the detriment of their businesses. An ISP attack disclosure also could lead to a loss of customers and revenue.[4] Releasing a top ten vulnerabilities list to the public helps system administrators and computer users, but provides hackers with the information they need to successfully attack at-risk networks.

Therefore, trust with respect to how the information will be used, how it will be protected from disclosure, and whether legal tools can be used by the government and private parties against those sharing information is needed among those sharing information in order to achieve successful protection of the national CII.

Tasks on Governmental Level

The most important task is the creation of a national security policy which has to include:

- Security policy for strategic objects controlled by computer networks, based on the risk analysis of possible attacks;
- Programs for practical implementation of security policy and operational measures to ensure the rules are followed;
- Strict adherence to the assessment standards of products and systems prone to cyber attacks;
- Analysis of the current reaction abilities of network elements and systems based on their reaction to possible attack scenarios;
- Assessment of the efficiency of protection tools by:

- Reliable verification (reasonable balance between confidentiality and access to common data);
- Protection of all systems and subsystems using testing (honey pots and honey nets) and specific criteria ("Orange book," Canadian criteria for security estimation of information technologies, harmonized European criteria).

The best practices and resources on cyber security policy developed in the last years provide valuable guidance both to industrialized and developing countries. The forerunner, the British Standard 7799, has now evolved into the International Standard ISO/IEC 17799. A number of other IT security standards have been developed, including ISO/IEC 13335 which relates to the Guidelines for the Management of Information Technology Security.

One of the most important aspects of effective organization of CIIP is government funding. Often the security measures undertaken by businesses are not very effective – or effective enough to outweigh the investment. Government investments in research and development of computer security measures resolve this problem to a certain extent. The second important task to be performed on the governmental level is the elaboration of common policy in the control of computer systems especially for the vital branches of national defense and business. This policy has to be founded on a legal framework for CIIP to be considered in the larger context of the business, social, and technical environment. CIIP has to be seen as a part of society's (cyber) crime prevention. Cyber crime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and includes issues such as copyright infringement, computer fraud, child pornography, and network security violations. Cyber crime is generally fought with traditional law-enforcement strategies that include adopting appropriate legislation and fostering international cooperation.

Only governmental institutions could create a united front against cyber attacks. This front needs a central unit for infrastructure protection – a body that is already created in some countries. It must focus on the collaboration of the private sector, law enforcement, prosecution and the intelligence community and provide support in the following four areas:

- Management of the computer emergency response teams (CERT) and virus centers in the country;
- Investigations on the Internet to identify criminal misuse and to monitor dangerous situations, such as the vulnerability of widely used hardware and software products;

- Verifying whether the reported matter constitutes a criminal offence, coordinating with ongoing proceedings and referring the case to the relevant prosecution authorities at home and abroad;
- Analyzing the interconnectedness of critical sectors and their dependence on information technology, and developing measures for prevention, response, and comprehensive security management of the national critical information structure.

These tasks include systematic examination of all infrastructure areas for possible weaknesses and improvement possibilities in terms of IT dependencies and security. Further, they necessitate the appropriate solutions, recommendations for each individual sectors, as well as indications of technical or organizational support needed in order to be executed.

The US was the first country to broadly address the new vulnerability of the vital infrastructures.[5] The Presidential Commission on Critical Infrastructure Protection (PCCIP) defined in 1997 the CII, its particularities and vulnerabilities. Following the PCCIP's publication, US President Bill Clinton started initiatives to increase the protection of critical infrastructures in the US, on the premise that a joint effort by government, society, organizations, and critical industries was needed to defend these vital assets.

Recently, following the example of the US, many countries including Australia, Canada, Germany, The Netherlands, Norway, Switzerland, the U.K., and Japan have taken steps on their own to better understand the dangers to their CII, and have proposed measures for the protection of these assets.

Computer Emergency Response Team (CERT) coordination centers are also being established around the globe and provide assistance in handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing security information and training materials.

Problems in CIIP on National Level

The main difficulty is that vendor product development and testing cycles are decreasing, thus leaving exploitable vulnerabilities. There are infrastructures with fundamental security design problems that cannot be quickly addressed. Vendors produce software with vulnerabilities, even such that can be easily avoided and computer source code often is not required to find them. In addition, the sophistication of attacks and intruder tools is increasing and many are designed to support large scale attacks.

There are also several other factors that complicate efforts to improve CII security. First, there is an inequality between the low cost performing an attack and the high cost of protection mechanisms. Therefore, there are indeed well-known technical vulnerabilities inside many infrastructures, but because of the prohibitive costs not enough has been done to address them.

Sometimes, losses from security breaches can be dealt with only if large numbers of parties coordinate to make the necessary investments. The incentive that one conscientious network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure, which would undermine the impact of the conscientious owner's measures. Moreover, assigning liability for security breaches is difficult – a user cannot easily identify the source of the problem (e.g., whether it was due to the user's software, the ISP, the backbone to which the ISP is connected, or software used by others).[6]

Another complicating factor is that computer network externalities are international in scope and implementation of a strong security policy conflicts with efforts to promote open communication environment. Furthermore, current highway net infrastructures connect countries with different levels of technological development; the "weak points" are vulnerable in two different ways: by themselves and as an initial point for attacks (zombing).

International Level

CII attacks are becoming a growing transnational phenomenon, making prosecution extremely difficult. Therefore cyber security must be approached from an international perspective, taking into account:

1. National and international initiatives;
2. Legal developments;
3. Best practices and resources;
4. Guidance on developing and implementing effective security programs;
5. Technological considerations.

Achieving cyber security requires a global effort; it cannot be achieved by a few nations. It requires the input from all information and communication technologies users, including citizens, governments, businesses, and organizations. On the multinational front, the Group of Eight (G8), the Asia-Pacific Economic Conference (APEC), the European Union (EU), the Council of Europe (CoE), the Organization for Economic Cooperation & Development (OECD), the Organization of American States (OAS), and the United Nations (UN) are each working towards solving this problem. As early as December 1998 the General Assembly of the United Nations

approved Resolution 53/70 on cyber crimes, cyber terrorism and cyber war. It appeals to the member states to inform the UN Secretary General of their opinions on the following issues:

- The problems related to information security;
- Basic notions related to information security;
- Development of international principles of the global information space and telecommunications, which help combat cyber terrorism and cyber crimes.

The EU has adopted the *Proposal for a Council Framework Decision on Attacks against Information Systems* that recommends a harmonized approach to attacks against information systems through uniform prohibitions against illegal access to information systems, as well as instigating, aiding or abetting such acts. The Council of Europe developed the Convention on Cyber crime (with the United States participating as an observer), which has since been signed by 42 countries.[7]

In October 2004 the General Assembly adopted a resolution about the creation of a global culture of cyber security and the protection of CII which recommends:

- The creation of emergency warning networks and crisis communication networks regarding cyber-vulnerabilities, threats and incidents;
- Public and private partnerships to share and analyze critical infrastructure information;
- The adoption of adequate substantive and procedural laws to enable states to investigate and prosecute attacks on CII and coordinate such investigations with other states when necessary.

In addition, many bilateral and multilateral documents have been signed for legal help, extradition, and law unification, guaranteeing transnational and international prosecution of cyber criminals. For example, the U.S. has held bilateral meetings on critical infrastructure protection (CIP) with Germany, Japan, Australia, Canada, China, and India. The European Commission recently held a conference at which EU-Russia cooperation regarding cyber security was highlighted. The case of *U.S. v. Gorshkov*,[8] in which an FBI agent conducted a cross-border search of a Russian computer to obtain evidence to indict a Russian citizen on extortion charges, is an example of how international cooperation helps cross-border searches in the current environment and how it might become the norm in the absence of formal international coordination.

Problems of CIIP in Bulgaria

The most important problems of CIIP in Bulgaria could be summarized as follows:

- Lack of legal acts for cyber criminal proceedings;

- Lack of trained staff;
- Lack of the necessary technical tools for response to cyber attacks;
- Lack of reliable system for interaction with special organizations from other countries;
- Lack of national organization on governmental level coordinating the CIIP;
- Lack of national strategy aimed at funneling the modest financial resources of the country to the development of such an organization;
- Lack of national action plan binding the national funds with international projects on regional level for the development of such organization.

Bulgaria needs a legal framework that would authorize governmental agencies to read e-mails, intercept wireless communications, monitor computer use, etc. A special law could make it illegal to intentionally crack a computer, or to deliberately cause damage launching a malicious program that harms a system. Hacking could be included in the definition of terrorism and may even face life imprisonment, as under the provisions of USA Patriot Act of 2001.

Recommendations and Suggestions

The following recommendations and suggestions could be given:

1. Organization of effective collaboration between the judicial bodies and special services of Balkan and European countries and international organizations.
2. Creation of a national strategy for prevention and combat against cyber crimes.
3. Creation of a national service against cyber criminality and international contact point for reaction and help during transnational computer incidents.
4. Extension of international collaboration in the field of judicial aid in the struggle against cyber criminality.
5. Creation of special laws in the area of telecommunications and computer networks in accordance with the current international standards and the Convention of EC for cyber criminality.

The best governmental approach would be to facilitate the establishment of a single technical point of contact that would enable the administrators at the backbone ISPs to share, in real time, information to combat a cross-industry attack (such as Bagle, Mydoom, Netsky, Sasser, Korgo, Sober). Coordination among the technical experts during a distributed denial-of-service (DDOS) attack, for example, would help them identify the source of the attack, as well as potential solutions to block the attack, and

restore the network to operational capacity faster. Informal communication and coordination do take place, but with the evolution of the Internet itself there is a need to increase the scope and scale of such activities.

Conclusion: Towards Practical CII Protection

One of the key features of our networked environment is that individuals, corporations and governments all share a responsibility in securing this environment. Therefore, the private sector, law enforcement, intelligence agencies and competence centers in certain fields, such as the CERTs in the domain of information infrastructures, must be brought together to ensure an integral and therefore successful protection of the national critical infrastructure.

Since usually the majority of a nation's critical infrastructure is operated and owned by the private sector, public-private partnerships are the key. In order to accomplish this, however, the government, which is usually in charge of the protection of the national critical infrastructure, should offer a well organized, efficient and reliable network to the private sector, covering all relevant fields from battling misdemeanors and early warning, to technical expertise and support.

Notes:

[1] John Moteff, Claudia Copeland, and John Fischer, "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress RL31556 (Congressional Research Service, Library of Congress, 21 Jan 2003).

[2] Andreas Wenger, Jan Metzger, and Myriam Dunn, eds., *International CIIP Handbook* (Zurich: Center for Security Studies at the Swiss Federal Institute of Technology, 2004), <www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf>.

[3] *U.S. The National Strategy to Secure Cyberspace* (US Government, February 2003), <http://www.whitehouse.gov/pcipb> (18 July 2005).

[4] Paolo Donzelli, "A Goal-Driven and Agent-Based Requirements Engineering Framework," *Requirements Engineering* 9, no. 1, Springer-Verlag London (February 2004): 16-39.

[5] Patrick L. Anderson and Ilhan K. Geckil, "Northeast Blackout Likely to Reduce US Earnings by $6.4 Billions," AEG Working Paper 2003-2 (Anderson Economic Group, 19 August 2003).

[6] Paolo Donzelli and Roberto Setola, "Putting the Customer at the Center of the IT System – A Case Study" (paper presented at the *Euro-Web 2001 Conference – The Web in the Public Administration*, Pisa, Italy, 18-20 December 2001).

[7] <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> (18 July 2005).

[8] *U.S. v. Gorshkov*, 2001 WL 1024026 (Western District of Washington).

EUGENE NICKOLOV, Prof. DSc. PhD Eng. Mag., has been Director of the National Laboratory of Computer Virology in the Bulgarian Academy of Sciences since 1991. He is Professor of Informatics, Doctor of Mathematics, Doctor of Computer Sciences, Engineer of Radioelectronics and Master of Sciences in Microelectronics. His main scientific interests are in informatics: algorithms, effectiveness, protections of operating systems; abstract models of computer systems, theory of programs; simulation and modelling of computer and communication technologies; theory of information and cryptographics; data security, computer security, communication security; analysis, synthesis, protection of stegano objects. *Address for correspondence*: Acad. G. Bontchev Str., Building 8, Office 104, 1113 Sofia, Bulgaria; *Phone*: +359-2-9733398; *E-mail*: eugene@nlcv.bas.bg.

SIMULATION OF CRITICAL INFRASTRUCTURES

Klaus NIEMEYER

Abstract: The paper presents a set of model prototypes developed to simulate the most critical areas of a highly-developed region in social, economic, technical and informational terms. The models were developed inspired by the fact that the highly integrated information infrastructure creates risks of failure and intrusions with a possible consequence of total loss of vital resources, such as energy or traffic. The models are seen on three levels of abstraction and are programmed and executed with tools from System Dynamics. On the highest level of abstraction, the modelled region is described and calculated using system attributes and variables like productivity, social pressure, satisfaction, etc. Different layers of social, informational and physical realities are defined. On the medium level of abstraction, critical areas of an advanced society are identified and calculated using variables that represent an entity in the reality and that, in general, have an empirical context. Identified critical areas for the first experiments with the model were the sectors of energy, communications, traffic, security, government, and defence. Applying a methodology to identify value drivers and to visualise the interrelations of components in complex systems helped in developing the model inputs and descriptive factors. This approach was used together with a group of experts in each area. On a low level of abstraction, a model prototype was developed using variables that in general can be measured and quantified based on real-life empirical sources. The latter approach is very complex and resource-intensive and requires detailed insight and knowledge. The first application of the models was related to an exercise that demonstrates the risks of software attacks in information networks and the possible consequences for other sensitive areas. Sensitivity analyses with the models showed that the threat of intrusion into the information networks with the consequence of loss of vital resources is likely to be overestimated in comparison to the threat of a direct attack on the relevant vital sectors.

Keywords: Modelling and Simulation, Critical Infrastructure, Gamma Methodology, System Dynamics, Powersim.

Background

Information Networks

The initially defined task has been inspired by fears that cleverly developed, although destructive, software (viruses, worms, etc.) possibly spreads on the Internet, as well

as on various operating systems and computer applications with the possible consequence that, at least for a certain time, the operation of software-dependent systems is interrupted.

In 1999, together with the fear that the change of the millennium would bring considerable problems in the information sector, another concern had originated – the growing network of many important industries of the social economy generates a dependence that is intense and increasingly vulnerable.

All these facts brought up the idea that the development and application of a simulation exercise that supports this hypothesis could show the vulnerabilities to the decision makers and could offer the possibility to look into potential improvements.

Essentially, the initial problem area and system of interest consist of information-networks that provide high variety of communication, control, data and other traffic between the numerous points of a highly developed socio-economic society. In the physical domain, these information networks are classic cable-based or radio networks. In addition, the information networks are characterized by the logical virtual networks installed in several layers on the physical networks with the help of the digital information technology. Meanwhile, the information networks penetrate all public areas and industries more or less intensively.

The high accessibility of the information networks, in particular the Internet, creates opportunities for the destructive software to intrude sensitive functional areas and to potentially cause considerable damage. We are afraid that the vulnerability increases with the intense network interconnectedness with the consequence of high economic losses.[1]

Although information networks were the essential element of the analyses, effects are measured only on the basis of productivity and performance of production and service industries. However, both the information networks and the production and service industries share a common user. The user is the individual human being and collectively – the social system of the society.

Socio-Economic Systems

The problem of vulnerability of modern socio-economic systems is considered extremely important. The critical conditions of modern, technologically-based economies are not enough explored and researched from the holistic point of view of the whole system. Although natural, man-made or system-inherent crises and catastrophes appear regularly, systematic examinations with the goal to forecast, to possibly prevent or to control the consequences are comparatively low or are not taken seriously. Most recent events provide evidence for this fundamental problem. If some-

thing happens, activities and planning are organized to a great extent only around the most recent catastrophic event.[2]

Crisis Team

In a crisis or catastrophe, the crisis team is the crucial group of people that can prevent possible chaotic development and disorganisation and can act to avoid disastrous consequences. These are people that come from various organisations, administrations and industries and have to get organised for the required purpose. Due to the fact that different organizations often work in normal circumstances in conditions of competition, it cannot be assumed that the designated people in the crisis team immediately find a harmonic basis for cooperative work. It is, therefore, necessary to establish methods and mechanisms for the formation of a crisis team to compensate these negative effects.

In addition, it has to be assumed that the members of the crisis team originate from very diverse knowledge areas. Although this is an essential element of crisis management, this substantial problem has to be taken into consideration in the internal communication since the different knowledge areas have developed their own, very specific languages that hinder the communication within the crisis team.

An essential attribute of crises and catastrophes is their sudden, partially very surprising emergence. Since crises are characterized by a series of unexpected and quick events, a requirement exists for the crisis team to react under very high time pressure. Since only a few people are able to act in these circumstances and since there are psychological group-dynamic effects in addition, a relevant and rational work is possible only within a very rigid configuration. For the successful work of the group, a crucial prerequisite is the structure of the team and accordingly trained personnel to fill the positions.

For the purposes of the consequent analysis, the decisions and actions of the crisis group necessitate a maximum transparency. The analysis of a crisis is required in all related areas in order to systematically gain experience. In addition, the actions of the members of the crisis team often have legal, ethical or moral consequences that are justified only with a complete set of well-documented underlying principles, causes, and effects.

Usually, the crisis team has high authority and responsibilities in order to be able to act if risk exists. Compulsory orders from higher levels in the hierarchy lead to considerable loss of time and generate worse results. The higher decision-making level or echelons do not necessarily possess better knowledge or a higher competence. Here, the constructive and very efficient principle of the task-oriented tactic used in the military has shown many positive results. This delegation of authorities has a high

value; the staff must be able to exercise these authorities and it has to recognise the related responsibilities. This also requires an excellent preparation and training of the crisis team.

Wrong decisions of the crisis team could lead to serious consequences. Decisions may even intensify a crisis; they could cause the exactly opposite of that intended or consequences with similarly negative effects as the crisis itself may occur. Since many actions are already clear and fixed during the preparation phase, a failure of a crisis team in a real crisis situation can only be sought in the intellectual and organizational preparation of the crisis team.

Therefore, *exercising of the crisis team is mandatory in all organisations.*

Exercises

The methods of model-assisted exercises and simulation are very suitable to clarify, recognize and practise system contexts. And, once more, it has been confirmed in such applications, especially in the military domain, that crisis teams act successfully in real crises if they have previously practised and exercised intensively. Without exercising, a crisis team is condemned to failure. Only real practice with tools that enable simulation of crisis situations and that show the consequences of making wrong decisions, can make possible the formation of capable and successful crisis teams.

It is assumed that a crisis in the functionality of an information network occurs starting from equilibrium or a stable situation of the socio-economic system. If a disruption, damage or any attack on the net occurs, it needs first to be recognised, second, a crisis team has to be established, which in turn has to find suitable counter-measures. Within the crisis team, the task is to get organised, e.g. to find a common language, to look for realistic solutions and to put them into operation.

The setup of an exercise consists of the crisis team and the exercise control. The crisis team involves representatives from industries and involved groups, organisations, governmental administration, etc. Peripheral groups are represented through the control team. The control team operates the script and/or the simulation model in order to provide a common picture of the development of the scenario. The simulation model has to represent the scenario in real measurement categories and elements of the reality, which are assigned to virtual entities of the model world.

The course of events within an exercise is a change between phases with lectures and/or discussions of the problem and phases of simulation in a logical sequence of events. The simulation is accompanied and assisted through quantitative evaluation of the model with a partially automated generation of events (see Figure 1). This setup can be called a Model-Assisted Exercise (MAX).

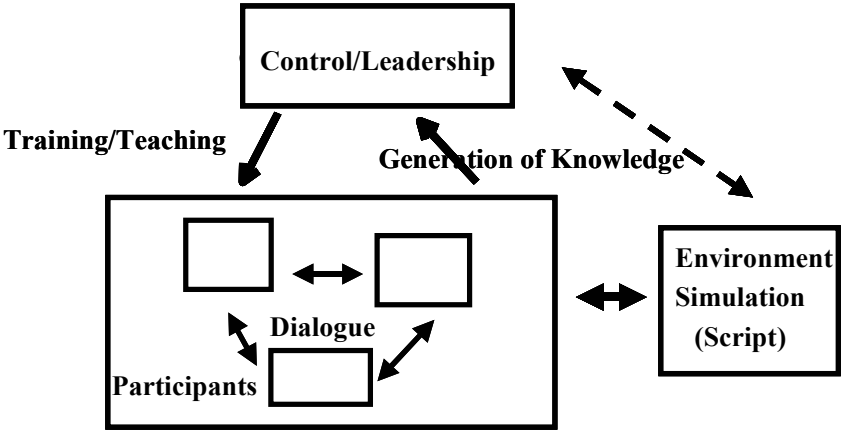


Figure 1: Model-Assisted Exercise (MAX).

The purpose of a model-assisted exercise could be: a dialogue between the participants in order to improve the communication among the experts on a peer-to-peer basis, negotiation related to the problem or simply working together towards a common objective. The control team, or the leadership, could perceive the exercise as a teaching or training device for the participants and at the same time can collect knowledge on the crisis team in terms of system analysis, testing of hypotheses, getting behavioural data, etc.

The attacker or the opponent in the exercise is usually represented as a subgroup of the control team. It represents the functions of motivation of the attacker, reconnaissance of weak elements of the system, planning and preparation of the attack, execution of the attack, eventual negotiations, and trying to ensure success.

The crisis team has to take precautionary measures, recognise the intention and perform reconnaissance of the attack, prepare for counteractions and safeguarding; once recognizing the attack, it should prevent collateral effects, counter the attack and defend, negotiate, recover and reconstitute to normal conditions.

In trying to create a reasonable model as a support tool for an exercise, many questions need to be answered during the initial phases of the project work. In particular, the dimensions of the scenario, the system under investigation, the required effort for model development, the level of abstraction of the model, the degree of detail of the model, and many other issues need to be determined.

Methodology

In a set of brainstorming sessions, a small group of analysts created and agreed on assumptions that lead to the approach summarised below.[3]

Essentially, a top-down approach of system analysis and related modelling is pursued in the presented work. Starting from a holistic point of view, the socio-economic system of a highly-developed region is identifiable by very general element areas or object classes. On this high level of abstraction, variables and objects are postulated that can be programmed in the model. This model on high abstraction level is seen as a first and rapid procedure for testing only some of the relationships and for preparation to get improved insights into system behaviour. Since almost no experience is available, such as the interactions of the information networks with the physical and social systems in mathematical-logical form, assumptions and hypotheses are made that appear plausible, but an intensive examination and verification is required.

There is a small amount of systematic and useful research and practical results available for development of such models. Nevertheless, a model of high abstraction has been chosen as a first design and quick prototype for generation of initial guess for the system structure.

In a second step, a relatively low abstraction-level model has been developed. Here, the reference to real objects is much better; however, there are also major problems regarding data collection and modelling of system structure. In addition, a much bigger effort is required for model development. Due to this reason, only a model of the traffic sector has been developed, which required considerably more time and effort for development compared to the high abstraction level model. Nevertheless, this approach should still be pursued in order to find better solutions.

As a compromise, a model has been developed that can be represented as a model of medium abstraction level. In order to collect the required input data and to generate an acceptable model of the system structure, a series of seminars and brainstorming sessions were conducted.[4] The seminars were supported intensively by the methodology "Gamma." This effort led to the development of a model that can serve as a driving force for exercises and follow-on research.

Gamma

For initial structuring, generation of assumptions, and estimation of factors and parameters, a brainstorming approach supported by computer software called *Gamma* was used. *Gamma* provides tools for interactive visualisation and analysis of complex interrelationships of systems and from the beginning it generates a holistic view.[5]

The graphical toolset generates a net diagram as a result of the thinking process of session participants and captures parameters and values of identified links between system elements. Understanding relationships of type cause and effect becomes possible. This provides a good ground for mutual acceptance and a common view of system interrelations. The generated values are available for subsequent analysis.

Gamma is not a rigid methodology providing decision optimisation with a guarantee to find the best solution. It rather belongs to the group of the so-called heuristic approaches that improve the likelihood of locating a good solution.

In an initial step, relevant influential factors and elements of the system under consideration are drafted. This is followed by the creation of a graphical network of interrelationships. Direction, type, intensity and frequency determine the relationships between the elements. The objective is to get knowledge about the structure and dynamics of the essential processes in the system.

System Dynamics

For simulation, the method of *System Dynamics* has been chosen due to the fact that it is very well suited for quick prototyping.[6,7]

This method has been applied to a wide variety of problems in both the public and private sectors. Large corporations and governmental agencies make use of the insights gained from building *System Dynamics* models while designing policies and strategies and in tactical and operational decision making.

Within the *System Dynamics* paradigm, emphasis is placed on model conceptualisation and on the utilization of a wide spectrum of criteria for model validation that help to ensure that the resulting models correspond to real systems structurally as well as behaviourally.

In particular, there are four types of structural properties that humans find cognitively challenging in dynamic systems.

First, there is the origin of dynamic behaviour itself, the relationship between flows and levels. Levels accumulate flows and flows cause the levels of levels to change over time. Although simple in principle, humans often find it difficult to distinguish between real levels and flows and to identify the behavioural consequences of flows acting on levels.

Second, there are delays or lags in actual systems. Delays distribute the effects of changes in variables throughout a system over time and often cause information to arrive at its destination in an untimely, and hence harmful, manner. Delays and lags lead humans to discover and give priority to short-run gains and to ignore and post-

pone actions against future losses. Delayed reactions typically cause systems to over- and undershoot and thus to exhibit oscillatory behaviour.

Third, there is a feedback. Real-world systems are usually characterised by circular causality. Their structures contain feedback loops that transmit the dynamic behaviour of one attribute to the next until the circle is closed and the signal, in a modified form, is fed back to its origin. Such loops have a tendency to stabilise or to destabilise a system. When humans try to control a feedback system, their actions are typically amplified or counteracted, depending on which feedback structure is dominating the system at the time.

Finally, there are nonlinear relationships. Nonlinearity implies that system attributes influence each other in a non-proportional way and that they interact so that their partial effects, calculated over time, cannot easily be distinguished. Such interactions may cause shifts in the structural dominance of a system over time. That is, substructures that have dominated a system's behaviour for some time may, suddenly or gradually, loose their influence while other substructures gain influence. This typically causes a dramatic modification of the system's dynamic behaviour.

Powersim

The availability of easy-to-use software engineering tools such as *Powersim* enabled a fast model development process.

Powersim is a software package that facilitates the study of dynamic systems. It makes possible the formulation of simulation models in the graphical notation as defined in the *System Dynamics* methodology.[8]

Powersim is particularly convenient for use of generic models. These models can be stored in a library, from which they can be copied, modified, and incorporated as co-models or integrated (pasted) as sub-models in a larger "main" model.

The ability of *Powersim* to describe and solve problems, however, suggests that its real benefit comes from its application in the model-building process itself, rather than from its ability to simulate a particular model. As a result, the people who both know the system experiencing the problem and are charged with implementing model-based results should participate fully in the modelling process. Their participation increases the probability that they will trust the model they helped to create and will implement its results. *Powersim*'s graphical user interface greatly reduces the barriers to the participation of policy makers in the modelling process. In addition, the graphical notation and the user-friendly interface make possible the fast development and rapid prototyping of simulation models.

High Abstraction-Level Model

On a high abstraction level, the system to be simulated is determined by variables that are defined in relation to a maximum possible value. In this way, it is not necessary to introduce absolute values since the variables are defined without a physical dimension and can only take values between 0 and 1. Relative variables of this type make possible the quantitative calculations with freely chosen, normally only qualitatively describable, parameters such as, for example, "satisfaction" or "alteration pressure," especially in areas where no or only restricted empirical data is available. Quickly-developed abstract models can be generated with relative variables although with the disadvantage of being highly speculative.[9]

In the high abstraction-level model, the elements are subdivided into three areas: the physical area, the information area and the social area. The physical area contains all the components that are physically defined, and can be physically measured and described. The information area contains all the components that can be assigned to an information network: the logical and virtual elements, the procedures, programs, data, or, in other words, the software and the databases. Computers, cable, storage mediums, electronic devices, etc., or the hardware, are physical components. The social area consists of humans, groups, hierarchies, organizations, etc. The elements of the social area could be allotted to the physical and information area. However, since this area contains important feedbacks, the social area is identified explicitly (Figure 2).

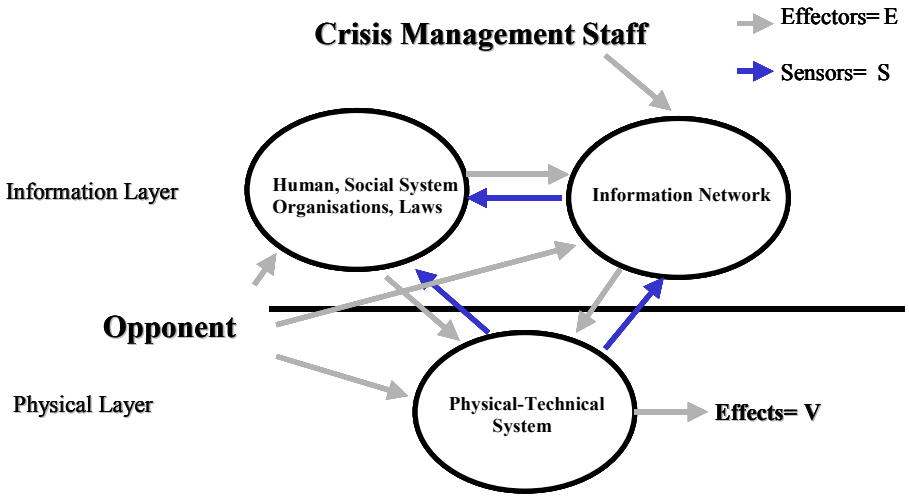


Figure 2: Layers of a Socio-Economic System.

Table 1: Objects of a Socio-Economic System.

Sectors	*Physical area*	*Information area*	*Social area*
energy	power plants, refineries, pipelines, gas stations, power lines	accounting, control of electricity	share holder, consumer
information industry	media, TV, newspapers, Radio stations, satellites, cable networks, computers	virtual nets, operating systems, software, databases, internet, applications, news	end user, consumer, opinion maker
civil service	work time, productivity	laws, regulations, orders	public opinion
security	police, armed forces, supporting forces	command, control, safety	public opinion
traffic and transport	road and rail net, links, airports, sea ports, stations	plans, nets, control	traffic participants, consumer
financial	banks, insurance companies, money	accounts	consumer

For each area, one can identify and describe sectors of industries, administration, security area, etc. The following six sectors were defined in the initial research phase: energy sector, information industry, civil service, security, traffic and transportation, and finance. Table 1 presents some of the real objects and elements that were assigned to these sectors and outlines the areas for further explanation and development.

Figure 3 illustrates the physical area. Some important interrelations are defined that already describe the structure of the simulation model in the graphical notation used by the *Powersim* simulation software. The variable physical *performance* as relative value describes the contribution of each element to the total productivity of the viewed system considering all sectors. The total productivity or the success of the system has an effect on the *satisfaction* of the social system in the social area in consequence. At the same time, the *performance* of a given sector is influenced by the performance of other sectors. Furthermore, the *performance* is diminished by random disturbances from the environment.

Each system has internal forces that keep the processes running and produce the *performance*. These forces are controlled by a feedback loop that tries to keep the

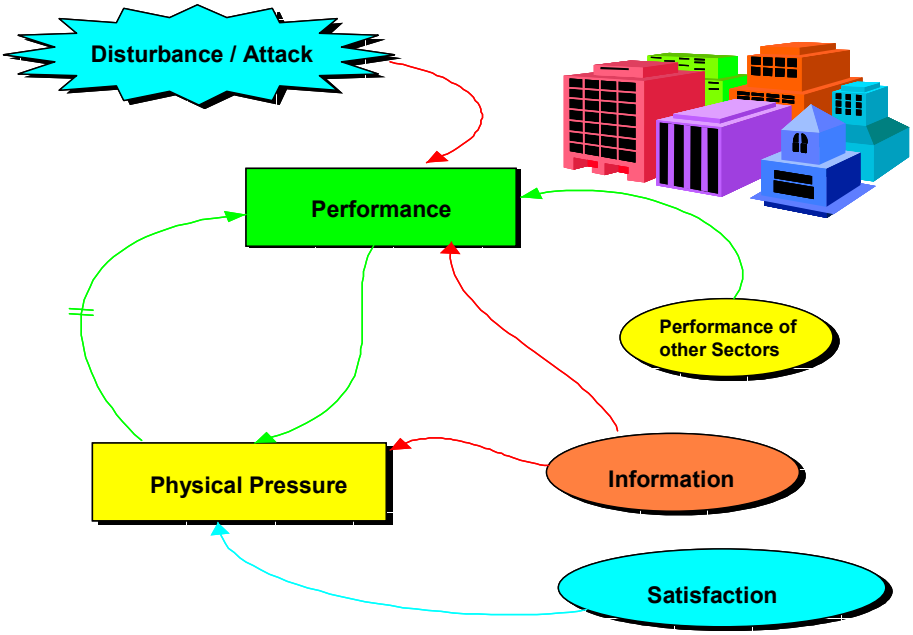


Figure 3: Physical Area.

performance level close to a desired value; in other words, the system tries to maintain equilibrium or a stable state. The role of feedback is played by the size of the variable *physical pressure*. By definition, the influence of the *physical pressure* is delayed in time and depends on *performance*. In addition, the *physical pressure* is influenced by *satisfaction* in the social area and *information* in the information area.

Figure 4 illustrates the information area. Similarly to the physical area, analogous interrelations and variables are defined. The variable *information* describes in relative terms the total result of each element of the considered system in all sectors. Again, the success of the system has in consequence an effect on *satisfaction* of the social system in the social area. The *information* of a sector is influenced by the *information* of other sectors. Furthermore, the *information* is reduced by disturbances from the environment. In addition, the *information* depends on the *performance* in the physical area.

Analogously to the physical area, a feedback loop tries to maintain the inner stability of the system, expressed via the variable *information pressure*. Again, by definition, this *information pressure* only works delayed in time and depends on the variable *information*, as well as on *satisfaction* in the social area.

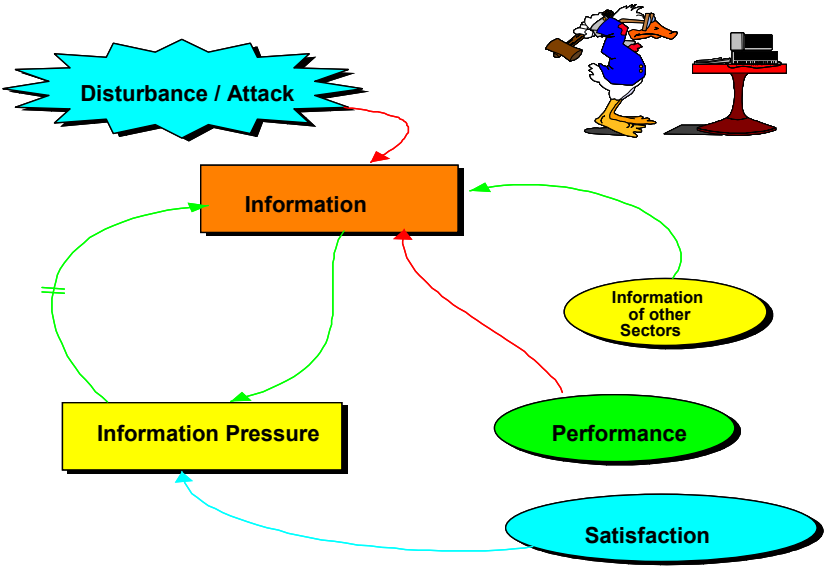


Figure 4: Information Area.

Figure 5 defines the social area. The variable *satisfaction* describes in relative terms the general status of the social part of the considered system for each element in all sectors. The *satisfaction* of a sector depends on the *performance* and the *information*

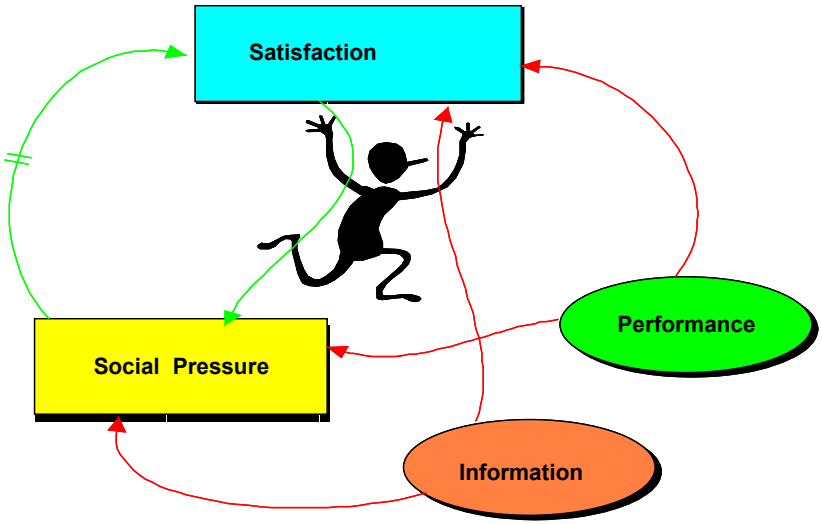


Figure 5: Social Area.

from the other areas. Again, a feedback loop is considered to cover the inner forces for maintaining a stable state. Here, the variable *social pressure* that also depends on performance and information plays the role of a feedback.

Figure 5 presents a typical diagram of the model in *System Dynamics* notation as realized in *Powersim*. Most of the variables are defined as vectors, where the index represents the sectors under consideration. The detailed description of the model is part of *Powersim*'s code. The code and the interpretation of the variables can only be seen in the context while the model is executed and calculation experiments are performed.

Low Abstraction-Level Model

Essentially, the system under consideration consists of the various types of transportation: road, rail, air and sea (water), split into transportation of goods and transportation of people. The traffic elements or the vehicles depend on the existence of a transportation network. The transportation network is simplified according to the traffic elements. For road and rail transportation, the traffic within the region and traffic in the outside world are separately modelled. For the model of the traffic within the region, the traffic is considered as a sort of container with a corresponding descriptive size; for the traffic in the outside world the region is viewed as a node of a network. For air and water transport, the region represents only one node, i.e. an airport or seaport.[10]

Although the information networks are the essential element of research in the intended application of simulation of disturbances as a training ground for exercises of crisis teams, the effects are rated only on the basis of indirect effects in the physical area. In the transportation sector, disturbances may occur due to lack of traffic control that under normal conditions optimises the flow of traffic elements and vehicles. Power outages, in particular the electric power ones, would cause major disturbances. Further direct disturbances are expected owing to physical effects, for example the cancellation of an air traffic node.

In the considered simulation of the transportation system of a region, the elements represented in Table 2 are taken into account. The abbreviation of the individual elements has the following meaning:

- Letters *F* = Long-distance traffic out of the region, *N* = Short-distance traffic within the region;
- Letters *L* = Air, *B* = Rail, *S* = Road, *W* = Water;
- Letters *P* = Passenger, *F* = Freight.

Table 2: Objects of a Traffic System.

Type	*Transport*	*Abbreviation*	*Object*	*Units of measurement*
Air (L)	Passenger (P)	FLP	Airport	Flgz, Pax
Air(L)	Freight(F)	FLF	Airport freight	Flgz, TEU
Railroad (B)	Passenger (P)	FBP	Rail station	Zug, Pax
Railroad (B)	Freight (F)	FBF	Rail station freight	Zug, TEU
Road (S)	Passenger (P)	FSP	Long-distance road net	Pkw, Pax
Road (S)	Freight (F)	FSF	Long-distance road net	Lkw, TEU
Water (W)	Freight (F)	FWF	Harbour	S, TEU
Railroad (B)	Passenger (P)	NBP	Regional railroad net	Zug, Pax
Road (S)	Passenger (P)	NSP	Short-distance road net	Pkw, Pax
Road (S)	Freight (F)	NSF	Short-distance road net	Lkw, TEU

All combinations considered realistic are given in the table. Certain combinations, for example, air traffic locally within the region, railroad freight within the region or water transport within the region, are not considered.

The objects / elements of the traffic system are empirically determined and described by means of units of measurement. The unit TEU, a standard twenty foot equivalent container unit, describes the freight. The number of *Passengers* is quantitatively described by the unit *Pax*. *Airplanes* are a quantity with measurement unit *Flgz*. For all aircraft types a common unit with an average capacity is assumed. The same is applied to trains with the unit *Zug*. For the road transport, the number of cars with an average capacity is measured with the unit *Pkw* and the number of trucks is measured with the unit *Lkw*. Similarly, the number of ships is defined with the unit *S*. For the objects in the table, the combinations of the units are important, as represented in column 5.

For the considered objects, average values can be assumed for typical sizes or can be derived from existing statistics. Some example values are given in Table 3.

The principal flow of passengers (P) and the flow of freight (F) are shown in Figure 6. It is assumed that the long-distance traffic areas are essentially connected via the local traffic areas. Furthermore, passengers and freight use the same infra-

Table 3: Some Maximum Values.

Object	*Speed*	*Average Length*	*Maximum Volume*
FLP	1000 m/h	1000 m	50 kPax
FLF	300 m/h	1000 m	500 TEU
FBP	3000 m/h	500 m	20 kPax
FBF	200 m/h	500 m	1000 TEU
FSP	120 km/h	50 km	20000 PKW
FSF	100 km/h	50 km	20000 PKW
FWF	100 m/h	25 km	10000 TEU
NBP	30 km/h	25 km	30 kPax
NSP	50 km/h	25 km	30000 PKW
NSF	50 km/h	25 km	30000 PKW

structure, such as for example railway stations, roads, and airports. In any case, the infrastructure is systematically subdivided into infrastructure of railway stations, rail network, long-distance traffic network, local traffic network, harbours, airports, vehicles, ships, airplanes, trains, trucks, cars, and freight as well as passengers. Each infrastructure object contains sources and sinks for the transportation goods that enter

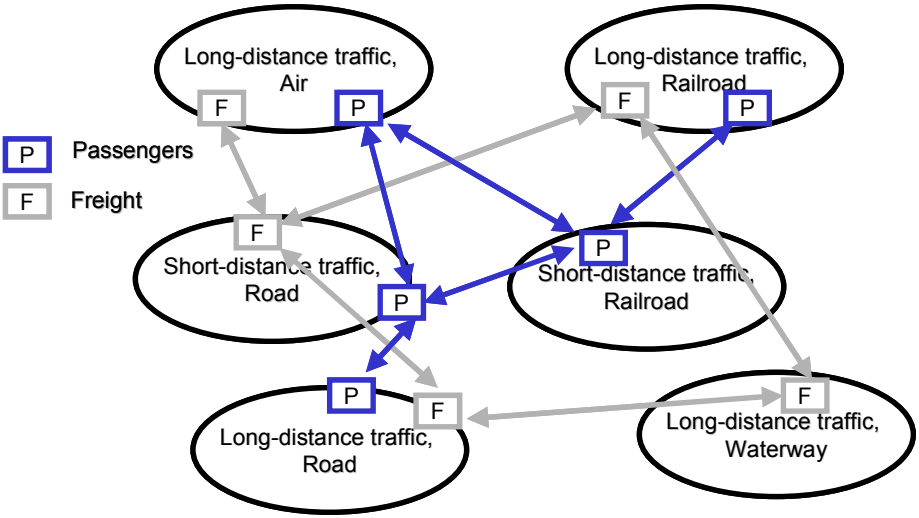


Figure 6: Flow of Passengers and Freight.

and leave the system. Within the system, the transportation goods are contained either in the infrastructure, the storages or in the transportation vehicles.

In the diagram, each node is individually modelled as a *System Dynamics* model in *Powersim*. All models are linked in a main program that controls the overall flow of processes and events. The detailed model description, definition of parameters, etc., is again part of *Powersim*'s code and can only be interpreted in context with the diagrams and the equations.

Medium Abstraction-Level Model

Experiments with the high abstraction-level model revealed the difficulty to establish a relationship between realistic absolute values and the generic variables as postulated. On the other hand, this is a prerequisite for application of models in exercises.[11]

For this reason, a series of brainstorming seminars were organised with the objective to generate real objects, entities, variables of the system and the sectors, as well as to quantitatively define their relationships.[12]

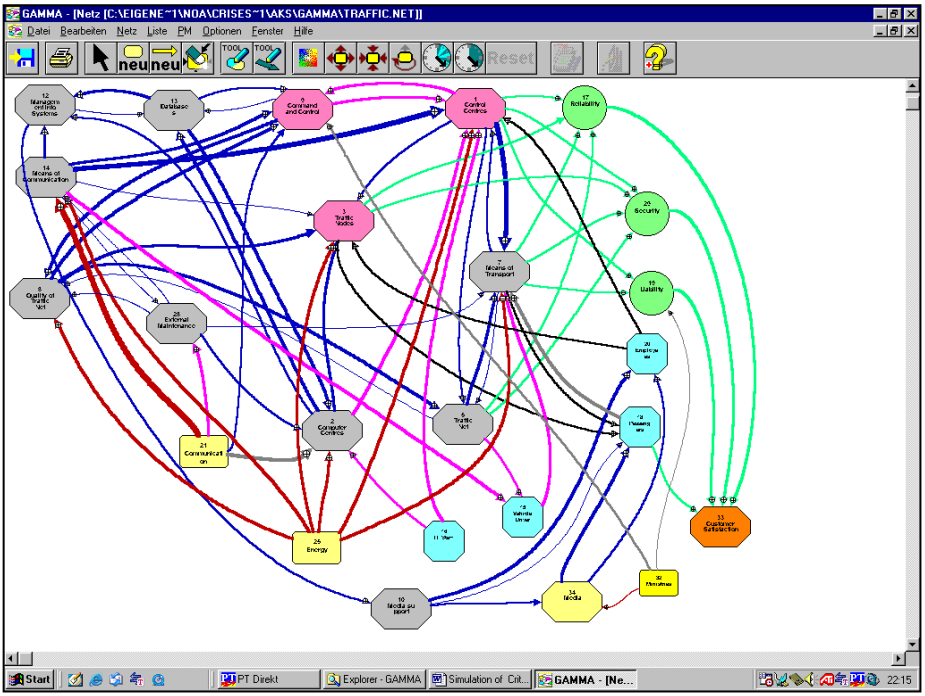


Figure 7: *Gamma* Network Diagram.

A list of elements was used as a basis for creation of cause-and-effect network in *Gamma*. With the help of *Gamma*'s graphical tools it was possible to arrange the elements as components of a network on the screen. Simultaneously, values for the influences were defined with the help of lines and arrows and their strength estimated. All the models were executed during the brainstorming sessions and corrections were made in multiple iterations, considering the different points of view of the participating experts.

A typical *Gamma* diagram for the transportation case study was created during these sessions as shown in Figure 7.

In a later phase, delay times of the influences of one element on another were defined. These delay times and the effects are direct results of the *Gamma* sessions; they are collected in tables and serve as input to the *System Dynamics* model of medium-abstraction level.

The diagram also indicates by means of lines and arrows how strong is the influence of each entity on other entities in the postulated system, which can be transformed easily into a matrix of influences. A different view at these dependencies for the en-

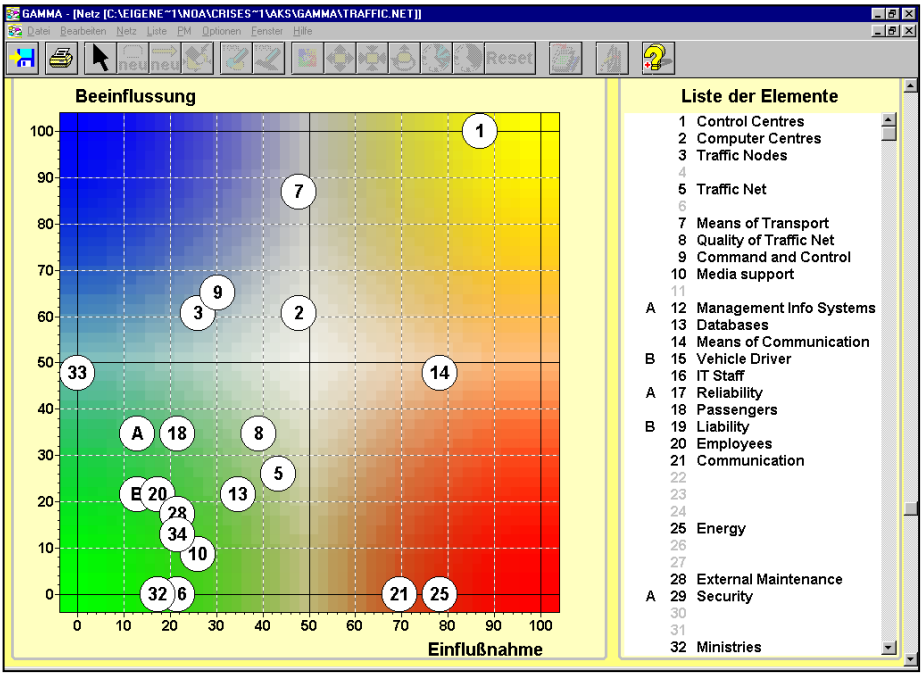


Figure 8: *Gamma* Sensitivity Diagram.

ergy sector is demonstrated in Figure 8. The horizontal axis represents on a scale between 0 and 1 the relative strength of the influence of an entity on other entities in the system, while the vertical axis represents on a scale between 0 and 1 the relative strength by which an entity is influenced by other entities in the system. Each entity has a well-defined position on the diagram. The distribution of positions demonstrates which entities are highly sensitive and require further specific attention in a straightforward manner.

Modelling and simulation of critical business and public sectors of a highly developed technical society is based on the entities, relationships and sensitive parameters as developed in brainstorming sessions by sector experts utilising the *Gamma* methodology. These relations are then transformed into a logical structure based on the *System Dynamics* methodology using *Powersim*.

On this medium level of abstraction the system to be simulated is determined and described by parameters and values, which are again defined relatively to a maximum possible absolute value. In this way, setting absolute values is not necessary since the parameters are defined without a measurement dimension and can take only values between 0 and 1. Relative parameters of this type make also possible quantitative calculations with freely-chosen, normally only qualitatively describable, parameters as defined in the expert sessions with the *Gamma* methodology.

For each industry and sector, the set of defined parameters describes the system under consideration and represents its state at any point in time if the parameter values are available quantitatively. The relative value describes the actual absolute value in relation to a maximum possible value and can formally be treated as value without a unit or measurement dimension. If the relative value is multiplied by the maximum possible value, the value emerges as value with the corresponding measurement unit.

In addition, in normal conditions the system of each sector is in a stable state or in equilibrium, i.e. the parameters do not change with time. These changes only occur if disturbances from outside act on the system. And this is the case in reality, although disturbances are continuously balanced by system internal regulations and control mechanisms. The system state becomes stable and eventually fluctuates only around the equilibrium. Only unusual disturbances are able to generate unstable behaviour, however, leading to stable state again although at different level. Theoretically, the set of relationships among the elements, as defined with the *Gamma* methodology, should cover this stabilisation effect. Unfortunately, this was not the case; all relationships were defined as positive feedbacks in the *System Dynamics* notation. In any system, for stabilising control mechanisms negative feedbacks have to be available in order to create a stable equilibrium.

Due to the fact that it is not obvious which parameters will have the stabilisation effect in the sense of a negative feedback, it has been assumed that the change of a parameter value depends on the change of all other parameter values, although delayed in time and with the effect according to the *Gamma* analyses. In principle, the state of a system is described by a state equation. However, in general this equation is not known; each parameter is a function of all other parameters. Since the values of the parameters, as determined in *Gamma*, are only positively defined, the system is unstable. All values would approach zero as soon as a disturbance occurs. Since this development does not correspond to the real behaviour of any system, it has been assumed that some inner forces of the system create an effect that stabilises each parameter after a certain time. If the disturbance remains, the system should move to a new equilibrium. If the disturbance disappears, the system should approach the original equilibrium again.

The parameters and relationships in the *System Dynamics* model follow the described assumptions. They are documented in great detail in the diagrams, equations and accompanied descriptions of the individual parameters within the *Powersim*'s code. It is recommended to perform further extensive tests with the model and adaptation of the parameters and values on this ground, respectively. Whether the model is acceptable enough for representing a scenario or a real system for use in a given exercise has to be judged by the operator.

Figure 9 presents the general picture of the areas considered in the simulation. In addition, the lines indicate the numerous many-fold interactive processes between the areas. Potential incidents resulting from terrorist acts, natural disasters or other major accidents will cause operational problems in these areas. In the simulation, the variables react on these intrusions in a manner similar to that of their real-life counterparts.

In order to develop appropriate actions and counteractions to such catastrophic events, the simulation models are used in an exercise to represent the reaction of the real world to the actions of the crisis team. Model of this form of application together with the control team of the exercise setup are the virtual environment for the participants that represent real crisis teams within the areas considered.

Presently, the following sectors have been considered: Traffic / Transportation (Air, Land, Sea), Banks and Finance, Energy, Vital Human Services, Government and Telecommunications (see Figure 9).

In the beginning of the simulation, the tabs *Causality*, *Model*, *Entities* and *Times* switch between several functional areas.

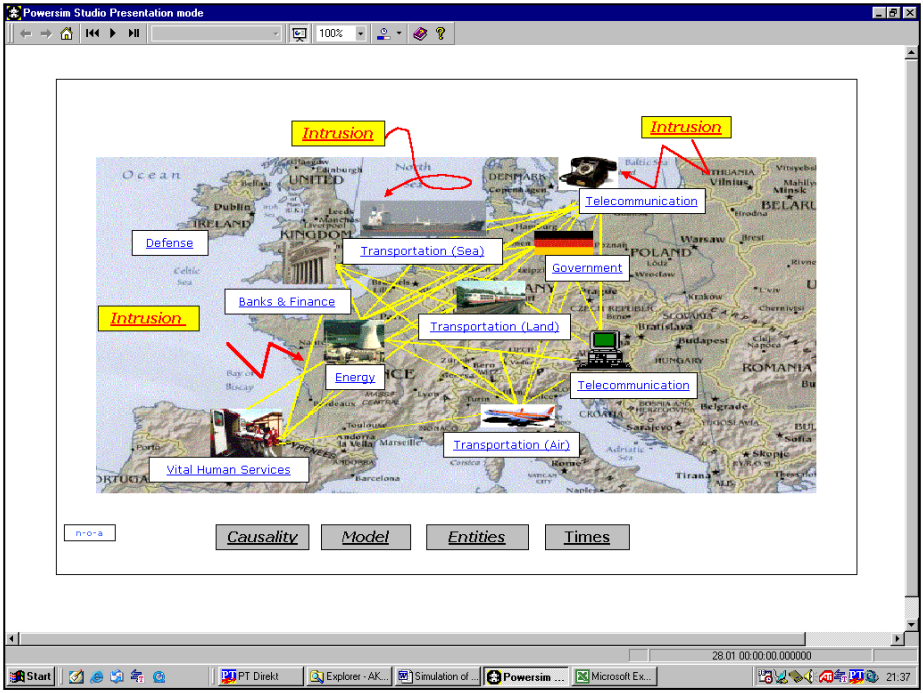


Figure 9: Sectors in the *Powersim* Model.

The tab *Times* is used to control the time periods in the gaming setup and to input intrusions and other parameters. Sliders permit simple and intuitive time setting for stop events in the course of the simulation.

The control tabs labelled *Intrusion* in this diagram provide pointers to control diagrams that enable the input of actions by the control team causing considerable changes to certain sensitive entities of several sectors, in the considered example energy, transportation and telecommunications.

The Causality Diagram in Figure 10 shows the two principal feedback loops in the model. It is assumed that these loops are valid for all sectors and entities represented in the model. Two variables are defined as levels in the *System Dynamics* notation: *Productivity* of the entities and *Internal Pressure*. Both variables / levels are defined in relative dimensions: the absolute value of any represented property of any entity is defined in relation to its maximum possible value within the system under investigation. The first feedback loop is positive. The productivity of each entity increases in the same direction as the influence or change of all other productivity levels based on the findings from the *Gamma* evaluations, considered with some time delays.

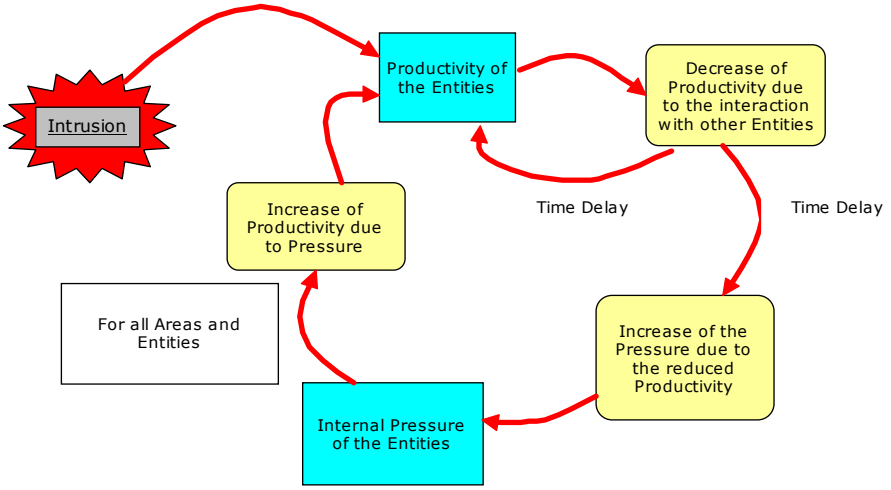


Figure 10: Causality Diagram in Powersim.

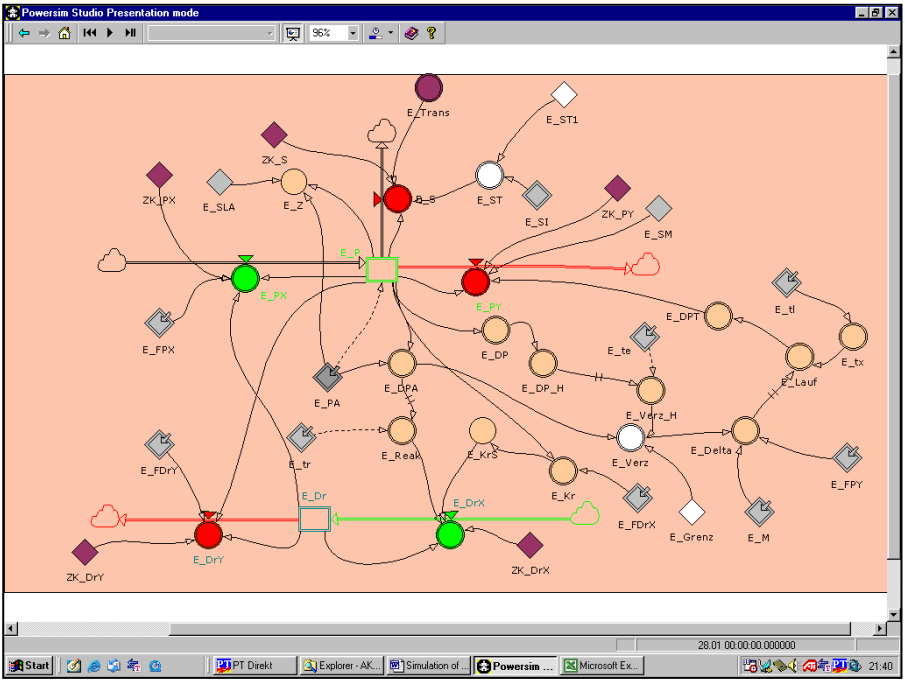


Figure 11: System Dynamics Notation in *Powersim*.

The second feedback loop is a negative one. It represents an internal build-up of counter forces of the system with the trend to stabilise the present state. This is measured by means of the assumed value of a pressure.

The model diagram in Figure 11 shows in greater detail the elements and interactions of the model for all areas, entities, levels, rates, and properties. This diagram illustrates the multiple interdependencies and it is described and integrated into the *Powersim*'s code in more detail. This diagram is the typical graphical structure used in *System Dynamics* notation and is automatically transferred to the executable computer program that simulates the dynamical system under study.

Notes:

[1] However, the anti-thesis says that increasing network connectivity creates an increased redundancy with the consequence of an increased reliability. The big success of the Internet is based on its ability to self-organise and to automatically produce new connections, if nodes or routes are cancelled or due to other reasons. Each additional computer, router or link to the Internet is an additional connection possibility, which increases the reliability. In practice, computers are constatntly switched off, completely decentralized for diverse reasons, and switched on again, without users of the network noticing this events. James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats* (Washington, DC: Center for Strategic and International Studies, December 2002), <http://www.csis.org/tech/0211_lewis.pdf> (4 July 2005).

[2] Wolf R. Dombrowsky and Christian Brauner, "Defizite der Katastrophenvorsorge in Industriegesellschaften am Beispiel Deutschlands. Untersuchungen und Empfehlungen zu methodischen und inhaltlichen Grundsatzfragen," Gutachten im Auftrag des Deutschen IDNDR-Komitees für Katastrophenvorbeugung e.V. (Kurzfassung) (Bonn: INDR, Deutsche

IDNDR Reihe Nr. 3a, 1996); Klaus Niemeyer, *Interaktive Simulationen zum Krisenmanagement* (NOA-TB-5, 2001, Krisenproblematik).

[3] Analysts from IABG and NOA. IABG (Industrieanlagen Betriebsgesellschaft mbH) is an agency providing system analysis support, <www.iabg.de> (4 July 2005); NOA is a network of freelance operation analysts, <www.n-o-a.de> (4 July 2005).

[4] These seminars were conducted in 2001 together with IABG and showed that no methodology or models seemed to exist in the sense and for use for the present purposes to simulate disturbances in a network of several industries and sectors.

[5] The tool "Gamma" is based on the ideas and the research of Frederic Vester and is developed and distributed by Unicon GmbH, Meersburg, Germany. Frederic Vester, *Das kybernetische Zeitalter* (Frankfurt/M, Germany: S. Fischer Verlag, 1982); Frederic Vester, *Leitmotiv vernetztes Denken* (München, Germany: Heyne, 1990); *GAMMA 3.0* (Unicon Management Development GmbH, 2000); <www.unicon.de> (4 July 2005).

[6] In the late 1950s, Jay W. Forrester of the Sloan School of Management at the Massachusetts Institute of Technology developed the System Dynamics method. This methodology became known from the famous study "The Limits to Growth" published in the 1970s by the "Club of Rome." Jay W. Forrester, *Industrial Dynamics* (Productivity Press, 1961); Jay W. Forrester, *Principles of Systems* (Productivity Press, 1968); Donella H. Meadows, Dennis L. Meadows, Jorgen Randers, and William W. Behrens III, *The Limits to Growth: A Report for the Club of Rome's Project on the Predicament of Mankind* (New York: Universe Books, 1972).

[7] Although the numerical integration of differential equations representing physical phenomena was used long time before the introduction of a graphical notation, the direct programming for computers and the application for large scale social-economic systems by Forrester created the methodology nowadays known as System Dynamics.

[8] <http://www.powersim.com> (18 July 2005).

[9] Klaus Niemeyer, *Modell Ausgewählter Branchen zur Simulation von kritischen Störungen* (NOA-TB-1, 2000).

[10] Klaus Niemeyer, *Modell des Verkehrssystems einer Region für die Simulation von kritischen Störungen mit einer geringen Abstraktion* (NOA-TB-6, 2002).

[11] Klaus Niemeyer, *Modell wichtiger Branchen einer Region für die Simulation von kritischen Störungen mit einer mittleren Abstraktion* (NOA-TB-7, 2002).

[12] These seminars were performed by IABG in 2001 with a group of experts for each sector utilising the supporting software Gamma.

KLAUS NIEMEYER was born in Bremen, Germany, in 1941. He left Gymnasium in 1958 and studied at the Physikalisch-Technische Lehranstalt in Lübeck and Hamburg, graduating as Diplom-Ingenieur in Technical Physics in 1963. During this period he worked also in industry, primarily with Entwicklungsring Süd, in the computing field. On graduation, Mr. Niemeyer moved to Boelkow Entwicklungen KG in Ottobrunn, near Munich, where he worked as system analyst in a team of U.S. and German scientists that initiated the German Operations Research activities for the German Ministry of Defence.

Mr. Niemeyer has had a long and distinguished career in Military Operations Research, Simulation and Computer Applications. In 1965, he joined the Industrieanlagen Betriebsgesellschaft mbH (IABG) in Ottobrunn with other German members of the above-mentioned team, and helped in establishing the Systems Analysis area at IABG. In 1966, he was assigned to US/GE advanced V/STOL-fighter assessment at the Wright Patterson Airforce Base in Ohio. As Project Leader he evaluated and analysed airborne and airbase systems.

In 1969, Mr. Niemeyer was appointed head of a group working on optimal air force structures. In this role he developed and operated the first German computer-assisted exercise in 1970. This formed the basis for establishment of the IABG Wargaming Centre, of which Mr. Niemeyer was appointed Chief in 1972. In this position, he initiated the development of several concepts, models, approaches and solutions to assessment and evaluation of force structures, and helped in initiating international programmes such as the US/German European Conflict Analysis Program (ECAP), and the Joint Simulation (JOSIM) Project. He has been responsible for many national and international studies in the areas of weapon system assessments, air and army structures, command and control, force effectiveness comparisons, arms control, conflict research, operational support, long-term defence planning, logistics planning, war gaming, exercises, and information systems support.

Mr. Niemeyer became Chief Scientist and Head of the Operations Research Division at the SHAPE Technical Centre (now NATO Consultation, Command and Control Agency) in May 1992. In this position he was the principal advisor on scientific matters and military operations analyses that affect SHAPE and Allied Command Europe. Among other projects, the Allied Deployment and Movement System (ADAMS), the methodology for the Defence Requirements Review (DRR) and the High Level Exercises have been developed in his area of responsibility. Mr. Niemeyer initiated and co-chaired the Steering Group on Modelling and Simulation and represented his organisation in several other panels and committees within NATO.

Mr. Niemeyer retired from NATO in April 1999 and now he works as a consultant.

I&S Monitor

- Bulgaria in NATO: Challenges to Civil Emergency Planning
- Homeland Security Internet Sources
- Books Related to Homeland Security

BULGARIA IN NATO: CHALLENGES TO CIVIL EMERGENCY PLANNING

Bozhidar PATINOV
First Secretary, Permanent Delegation of Bulgaria to NATO

Civil Emergency Planning, as all other NATO areas of activity, was positively affected by the accession of seven new member states to the Alliance in Spring 2004, including Bulgaria. Given their strong involvement in Civil Emergency Planning during previous years in the framework of Partnership for Peace and EAPC and as Invitees in 2003, the new Allies were able to integrate effectively into NATO's Civil Emergency Planning structures.

The year 2004 was also marked by a number of important policy initiatives in the area of Civil Emergency Planning. Allied Heads of State and Government, at the Istanbul Summit in June 2004, agreed on a broad set of measures for defense against terrorism, including a commitment to further explore and enhance Allies' and NATO's ability to respond rapidly to national requests for support to help protect against and deal with the consequences of a terrorist incident. The Istanbul Summit was also the venue for a successful exhibition on NATO's role in response to disasters and civil emergencies. Also in 2004, a Civil Emergency Planning Exercise Policy, an exercise program, and a Catalogue of Civil Capabilities for use by the NATO Military Authorities in crisis response operations were developed and agreed by the Senior Civil Emergency Planning Committee (SCEPC). With regard to disaster assistance, the North Atlantic Council (NAC) agreed in January 2004 that the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) should be ready to respond expeditiously, on the basis of SCEPC guidance, to requests for disaster assistance support by the Afghan government. The role of EADRCC for emergency response in real time and consequences management has considerably increased over the last years in EAPC area. The new expected extension of SCEPC and EADRCC activities is directed to strategic approach and practical options for an enhanced cooperation with the Mediterranean dialogue countries in the field of civil emergency planning. Furthermore, efforts continued to achieve closer cooperation among NATO bodies involved in Chemical, Biological, Radiological and Nuclear (CBRN) - related

.

matters, and, in particular, between the SCEPC and the Senior Defense Group on Proliferation (DGP). The implementation of the Civil Emergency Planning Action Plan for the Improvement of Civil Preparedness against Possible Attacks against the Civilian Population with Chemical, Biological, or Radiological Agents continued at satisfactory pace in 2004. All these policies were reflected in the new Ministerial Guidance for Civil Emergency Planning 2005-2006, which the SCEPC developed during the second half of 2004 and which was endorsed by NATO Foreign Ministers at their 9 December 2004 meeting in Brussels.

In regard to NATO's Civil Emergency Policy, Bulgaria has made essential contribution to NATO's efforts to improve its own Crisis Response System. Bulgaria has played and continues to play active role in the decision-making process with its permanent participation in the SCEPC and its Planning Boards and Committees' sessions. Bulgarian national representatives have participated in the development of the main strategic NATO's documents in the areas of civil emergency planning and the protection of civilian population and critical infrastructure. Many institutions and organizations in the country have worked hard to improve their own preparedness in the field of civil emergency planning and gave their contribution to the development of the national crisis response system. Numerous activities took place during this one year period: the adoption of the new crisis management law; conduction of emergency response exercises; implementation of research studies, projects and programs in the field of national and regional security and risk prevention; conferences, seminars, working meetings on bilateral and multilateral basis, etc. Most of them were presented in NATO and were highly appreciated by the International Staff and the Allies.

Bulgaria will continue to share and bear the common NATO responsibilities and values not only in piece keeping, but also in developing the increasing NATO role in protection of the civilian population in case of emergencies. The adequate approach to the achievement of this humane task for Bulgaria for the next couple of years is the development of modern national crisis response system in accordance with the NATO's crisis response system. The system has to be flexible, integrated, and quickly deployable and to comply with the NATO standards, allied agreements and procedures. The system has to be supported by clearly-structured institutional organization on a national level with integrated state, regional and local network of emergency management centers, bodies and rescue teams. This organizational structure should be fully equipped and oriented towards protection of the civilian population in case of disasters, accidents, and catastrophes.

One of the best practices and priorities that Bulgaria has to follow is strengthening of the regional cooperation. Good example in this direction is the initiated and organized by Bulgaria Civil Military Emergency Planning Council for South Eastern

Europe. This governing body has already gained rich regional and international experience in dealing with natural disasters and technological accidents. The scope of Council's activities covers also improvement of civilian preparedness and protection against terrorist acts.

The Bulgarian efforts to keep, protect and maintain the civilian security and stability in case of emergencies would be very much facilitated by our active and visible NATO membership. And if we wish to contribute to the Alliance efforts in developing a reliable and efficient common collective security system, including a secure civilian environment and protection, we, on a national level, have to improve the realization of the following NATO priorities:

- Development of a National Capabilities Inventory;
- Participation in the work-out of the non-binding guidelines and minimum standards against CBRN agents and Weapons of Mass Destruction (WMD);
- Protection of the civilian population through development, introduction and application of new technologies in crisis management;
- Improvement of Civil-Military Cooperation;
- Development of Border Crossing Agreement in case of emergencies;
- Critical Infrastructure Protection;
- Development of Training and Exercise Policy in Civil Emergency Planning;
- Inclusion of the scientific community and the non-governmental organizations in the civil emergency studies and research.

We have to look for opportunities to raise the public awareness and understanding of the necessity for a highly effective and transparent system, able to overcome the challenges to the natural and man-made surrounding environment. The role of the authorities and the civilian associations is very important here, in how to initiate a public debate on this important subject – the protection of the population.

HOMELAND SECURITY INTERNET SOURCES

USEFUL SITES, PORTALS AND FORUMS

Homeland Security Home Page

http://www.whitehouse.gov/homeland/

A federal agency whose primary mission is to help prevent, protect against, and respond to acts of terrorism on United States soil.

U.S. Department of Homeland Security

http://www.dhs.gov/dhspublic/index.jsp

Governmental agency working on the prevention of terrorist attacks within the United States, reducing America's vulnerability to terrorism, and minimizing the damage from potential attacks and natural disasters. Includes articles, news and grants programs.

Homeland Security Institute

http://www.homelandsecurity.org/

The primary mission of the Homeland Security Institute is to assist the Department of Homeland Security (DHS) and its Operating Elements in addressing important homeland security issues, particularly those requiring scientific, technical, and analytical expertise. The institute provides extensive coverage on the issue and information on current events, a weekly newsletter, bibliography, virtual library, and links.

Survivability/Vulnerability Information Analysis Center (SURVIAC)

http://www.bahdayton.com/surviac/

.

SURVIAC is the U.S. DoD's institution for collecting, analyzing, and disseminating scientific and technical information related to all aspects of survivability and lethality for aircraft, ground vehicles, ships and spacecraft, to conventional homeland security threats including chemical, biological, directed energy, and non-lethal weapons.

Homeland Security Advisory System

http://www.nationalterroralert.com/overview.htm

This is the website of a Homeland Security advisory system and resources. It provides Homeland security guides for preparing against terror attacks and a free 300-pages homeland security manual.

Air War College: Homeland Security, Homeland Defence, Domestic Preparedness

http://www.au.af.mil/au/awc/awcgate/awc-hmld.htm

Links to mostly government and military websites related to homeland security, created for military members by the Air War College.

Federal Commission for NBC-Protection (ComNBC): Facts on NBC threats

http://www.komabc.ch/e/aktuell/index.htm

After the terror attacks in the US: Facts on the threat of nuclear, biological and chemical weapons (NBC weapons).

Commission of the European Communities: Reinforcing the Civil Protection Capacity of the European Union, European Commission, Brussels, Belgium

http://europa.eu.int/eur-lex/en/com/cnc/2004/com2004_0200en01.pdf

A set of recommendations on Civil Protection to the European Parliament and the European Council, released on 25 March 2004 in light of a series of natural disasters in 2002 and 2003 and the recent terrorist bombings in Madrid.

ON-LINE JOURNALS

Journal of Homeland Security

http://www.homelandsecurity.org/journal/

The interdisciplinary, refereed Journal of Homeland Security is devoted to the discussion and analysis of issues related to the subject of Homeland Security. The Journal publishes feature articles, book reviews, commentaries and articles focusing on science and technology relevant to the field of homeland security.

Journal of Homeland Security and Emergency Management

http://www.bepress.com/jhsem/

This journal aims to provide new information and understanding of emergency management in the homeland security environment and hopes to foster a community of persons who share these interests. Its intent is to provide quality content in the new realm of homeland security and to discuss the relationships between emergency management (for natural, technological and industrial, and terrorism events) as currently understood and conducted and the new field of homeland security.

Journal's intent is to provide information and insights on homeland security and emergency management from a broad array of professions, including engineering; political science/public administration/ policy analysis; decision science; and health and medical.

Homeland Security

http://www.govexec.com/homeland/

This is a monthly publication for senior U.S. Government officials. It includes regularly updated features on management, homeland security, defense, outsourcing, procurement, and e-government.

Homeland Security Weekly

http://www.homelandsecurity.org/bulletin/current_bulletin.htm

This is a homeland security resource newsletter. It offers free online courses and books, utilities and links to federal and state agencies dealing with homeland security issues.

Connections: The Quarterly Journal, Fall 2005

http://www.pfpconsortium.org <Publications>

Special issue on homeland security, covering roles of the armed forces of seven countries both NATO members and neutral states.

McGraw-Hill's Homeland Security Magazine

http://www.mcgraw-hillhomelandsecurity.com/

Journal's mission is to provide industry and government agencies with the information necessary to help protect the Homeland and develop commerce to enable them to achieve that goal. McGraw-Hill Homeland Security products and services include: The Homeland Security Supplement, The Homeland Security Summit and Exposition, The Homeland Security Channel on the Aviation Week Intelligence Network.

Homeland Defense Journal

http://www.homelanddefensejournal.com/

The journal is a monthly publication, featuring in-depth looks and analyses of homeland-related topics, the people leading this community and those that support them. Homeland Defense Journal and Homeland Defense Journal Online together seek to facilitate communication among all levels of government concerned with homeland security, covering the issues and the technology, solutions, policies, people, case studies and events affecting that community.

CONFERENCES

Homeland Security Conference 2006

http://www.afcea.org/events/homeland

The conference will be held on 22-23 February 2006 at Ronald Reagan International Trade Center, Washington, D.C.

Fourth Annual Homeland Security Conference

http://www.nmhsconference.org/

The 2005 Fourth Annual Homeland Security Conference will take place in Albuquerque, New Mexico, November 16-18, 2005. Activities will include presentations, workshops, and demonstrations by homeland security and counter-terrorism experts and displays by nationally recognized vendors.

Technologies for Critical Incident Preparedness Conference & Exposition 2005

http://www.regonline.com/eventinfo.asp?EventId=21494

This conference offers an opportunity for first responders, business and industry, academia, and elected federal, state, local, and tribal stakeholders to network, exchange ideas, and address common critical incident technology and preparedness needs and solutions. It will be held from October 31, 2005 until November 02, 2005 in San Diego, CA.

2005 Corporate Security, Business Continuity and Crisis Management Conference: Emerging Threats to the Corporation--Strategies to Detect, Deter and Defuse Crises

http://www.conference-board.org/conferences/conference.cfm?id=980

At the conference, the private sector can find ways to protect companies against terrorism. This event will benefit senior executives, government officials, policy experts, and other thought leaders who want to examine strategies to limit risk, control damage, maintain critical operations, and effect recovery. It will be held at Westin New York at Times Square, New York, NY; November 17-18, 2005.

5th Annual Critical Infrastructure Resilience & Infrastructure Security for the Built Environment Congress & Expo

http://www.protectinfrastructure.com/

This event will bring together government and industry officials from around the world to discuss and formulate solutions to protect the homeland. Issues such as physical security, cyber-security, standards, interoperability, biometrics, threat and vulnerability assessments, research and development efforts, and first responder requirements will be discussed.

BOOKS RELATED TO HOMELAND SECURITY

INTRODUCTION TO HOMELAND SECURITY

Authors: Jane A. Bullock, George D. Haddow, Damon Coppola, Erdem Ergin, Lissa Westerman, and Sarp Yeletaysi

Publication Date: June 2004

Publisher: Butterworth-Heinemann

ISBN: 0-7506-7787-2

This book presents a comprehensive account of past and current homeland security reorganization and practices, policies and programs in relation to the government restructuring. It provides definitions of the terms used in homeland security; a comprehensive contact list of Federal and State government homeland security offices and officials; case studies of past domestic terrorism events such as the World Trade Center, the Pentagon attack, the Oklahoma City bombing, the anthrax crisis and the Washington, DC sniper attacks; and an Instructor Guide complete with chapter summaries, exam questions, and discussion topics.

DEFENDING THE HOMELAND: DOMESTIC INTELLIGENCE, LAW ENFORCEMENT, AND SECURITY (CONTEMPORARY ISSUES IN CRIME AND JUSTICE SERIES)

Author: Jonathan R. White

Publication Date: April 2003

Publisher: Wadsworth Publishing

ISBN: 0-5346-2169-4

Keywords: United States – Terrorism, Prevention, National Security, Civil Defense, Law Enforcement

The U.S. government reorganizes in order to increase domestic security. How will these changes influence the American criminal justice system? This book provides up-to-date information on how the U.S. criminal justice system has changed since

.

9/11. The author provides an insider's look at issues related to restructuring of federal law enforcement and recent policy challenges. The book discusses the problem of bureaucracy, interaction between the law enforcement and intelligence communities, civil liberties, and theories of war and police work. From a practical perspective, the book examines offensive and defensive strategies. The book gives an introduction to violent international religious terrorism and an overview of domestic terrorist problems still facing law enforcement.

THE MYTH OF HOMELAND SECURITY

Author: Marcus J. Ranum

Publication Date: October 3, 2003

Publisher: John Wiley & Sons

ISBN: 0-4714-5879-1

Keywords: Civil Defense, War on Terrorism, Defenses

In this study of the state of modern American security issues, the author denigrates the prospect of "cyberwar," and discusses in some detail the disruption that hackers have caused. Existing firewalls and virus protection are valuable, but only if universally and rigorously used. Ranum notes that more cooperation with foreign intelligence agencies is needed, and is possibly occurring.

HOMELAND SECURITY ASSESSMENT MANUAL: AN ORGANIZATIONAL ASSESSMENT BASED ON BALDRIDGE CRITERIA

Author: Donald C. Fisher

Publication Date: September 2004

Publisher: ASQ Quality Press

ISBN: 0-8738-9640-8

Keywords: Emergency Management, Civil Defense, National Security, Terrorism-Prevention-Government Policy-United States

Since the terrorist attacks of September 11, 2001, America has made great efforts to improve homeland security. Yet, America's critical infrastructure, facilities and organizations are at risk – and vulnerable. How do organizations gauge their strengths and opportunities for improvement in integrating security into their business model? Fisher's comprehensive and hands-on manual, based on the Malcolm Baldrige National Quality Award Criteria, helps organizations measure their overall alignment and integration of key processes with homeland security issues. These are issues that both public and private organizations must address in order to ensure a safe work

environment for their employees, suppliers, partners, and customers. The CD-ROM that comes with the book includes self-assessment scoring documents and questions to ask that provide valuable insights when analyzing a given organization. Homeland Security Plan and Budget forms are included which allow assessment results to be transformed into a strategic plan with costs identified for each objective, strategy, and action item.

MAPPING THE RISKS: ASSESSING THE HOMELAND SECURITY IMPLICATIONS OF PUBLICLY AVAILABLE GEOSPATIAL INFORMATION

Authors: Beth E. Lachman, David R. Frelinger, Kevin M. O'Connell, Alexander C. Hou, Michael S. Tseng, David Orletsky, Charles Yost, and John C. Baker (Editor)

Publication Date: October 2004

Publisher: RAND Corporation

ISBN: 0-8330-3547-9

Keywords: Civil Defense, Geographic Information Systems-Defense measures-United States.

Following the attacks of September 11, 2001, many agencies within the U.S. federal government began restricting some of their publicly available geospatial data and information from such sources as the World Wide Web. As time passes, however, decision makers have begun to ask whether and how such information specifically helps potential attackers, including terrorists, to select U.S. homeland sites and prepare for better attacks. This book aims to assist decision makers tasked with the responsibility of choosing which geospatial information to make available and which to restrict.

A WAR OF A DIFFERENT KIND: MILITARY FORCE AND AMERICA'S SEARCH FOR HOMELAND SECURITY

Author: Stephen M. Duncan

Publication Date: April 2004

Publisher: Naval Institute Press

ISBN: 1-5911-4220-2

Keywords: Civil Defense, War on Terrorism, 2001- ,Terrorism-United States-Prevention, Military Policy, United States-Armed Forces

The radically new homeland security, military, and legal strategies developed by the United States in the months following the terrorist attacks on the World Trade Center

and Pentagon are given comprehensive treatment in this book by a former senior Pentagon official, combat veteran, and criminal prosecutor. Stephen M. Duncan draws on a lifetime of military and legal experience to examine the many questions relating to the role of the armed forces in homeland security, including elements of constitutional and criminal law, foreign policy, tradition and custom, federal-state and inter-agency relations, and politics, as well as military strategy and operations.

Among the diverse subjects the author discusses are military tribunals and the International Criminal Court, the statute governing the use of military personnel in law enforcement, defense transformation, the constitutional power of the president, and the reorganization of the government to meet the terrorist threats. Duncan also discusses the strategy and tactics used in Afghanistan and Iraq and critically evaluates the U.S political leadership before and after the 9/11 attacks.

TERRORISM AND HOMELAND SECURITY (TERRORISM IN 21ST CENTURY)

Authors: Yonah Alexander (Editor) and Donald J. Musch (Editor)

Publication Date: July 2005

Publisher: Wadsworth Publishing

ISBN: 0-5346-4381-7

Keywords: Terrorism, Prevention, Homeland Security

All civilized nations, both unilaterally and in concert, are developing comprehensive strategies and capabilities to minimize future domestic, regional, and global threats. The aim of this book is to provide a comprehensive collection of important documents that focus on the critical mission of protecting the homeland from future terrorist attacks and representing the views, policies, and actions of the executive and legislative branches. Editors Yonah Alexander and Donald J. Musch have carefully selected key policy speeches, executive orders, presidential directives, reports, testimony, and legislation that reveal the inner workings of America's response to the attacks of 9/11 and efforts to prevent possible future attacks.

ARMY FORCES FOR HOMELAND SECURITY

Authors: Lynn Davis, David E. Mosher, Richard R. Brennan, Michael Greenberg, Scott McMahon, and Charles Yost

Publication Date: January 2004

Publisher: RAND Corporation

ISBN: 1598750577

Keywords: Civil defense, US Army, Civil-military relations

Although responding to terrorist attacks and other domestic emergencies is primarily a civilian responsibility, the U.S. Army has a role in filling gaps in civilian capability. Should the Army adopt a hedging strategy to meet the risks of future terrorist attacks and other emergencies? The authors of this report lay out five possible shortfalls in Army capability and suggest five responses the Army can begin today.

HOMELAND SECURITY: A COMPLETE GUIDE TO UNDERSTANDING, PREVENTING AND SURVIVING TERRORISM

Authors: Mark Sauter and James Carafano

Publication Date: April 2005

Publisher: McGraw-Hill

ISBN: 007144064X

Keywords: Cyber-terrorism, Business Preparedness, Critical Infrastructure Protection, Weapons of Mass Destruction, Policy Issues

Directed to readers who need to understand both the “big picture” and their own roles in the war against terror, the book provides a clear and comprehensive overview of an increasingly complex and misunderstood topic. This reference, filled with interesting real-life examples and tips, covers the basics of homeland security such as: national strategies and principles; federal, state and local roles; terrorist history and tactics; cyber-terrorism; business preparedness; critical infrastructure protection; weapons of mass destruction; and key policy issues.