



RESEARCH PAPER

Homeland Security and NATO Policy

Prepared for NATO Allied Command Transformation

For further information on this report:
Dr Michael Williams, Head of Programme
Transatlantic Security Issues
+44 20 7747 2633
michaelw@rusi.org

The research described in this report was sponsored by NATO Allied Command Transformation under Purchase Order 701598, 13 Nov 07.

RUSI was founded in 1831, the oldest such institute in the world, at the initiative of the Duke of Wellington. Its original mission was to study naval and military science, what Clausewitz called the 'art of war'.

It still does so: developments in military doctrine, defence management and defence procurement remain central themes in the Institute's work. But RUSI has also broadened its remit to include all issues of defence and security encompassing policy-planning related security studies and homeland security and resilience issues.

RUSI is a British institution, but operates with an international perspective. RUSI's head quarters are located in Whitehall and the Institute also has officers in Washington D.C. and Doha, Qatar.

RUSI is a non-profit Institution, independent of government and non-partisan in nature that contributes to policy and decision making through rigorous research and analysis.

© RUSI 2008

No part of this work may reproduced in any forms by any means electronic or mechanical (including photo-copying, recording, or information storage and retrieval) without permission in writing from RUSI.

Reproduction rights are granted to NATO ACT.

Published 2008 by RUSI
Royal United Services Institute for Defence and Security Studies
61 Whitehall
London SW1A 2ET
United Kingdom
www.rusi.org

I. INTRODUCTION

Contemporary security risks are transnational, originating both within and beyond states to exploit nodes of vulnerability in the complex interdependent systems on which free societies depend. The existential character of the threat puts added pressure on public and private instruments of power to address the blurred distinction between international security and internal or homeland security. Increasingly, this will warrant elevating standardized operating procedures as a means of guaranteeing agency interoperability.

If targeted states are to protect their societies effectively, they must go beyond piecemeal extensions of current policies to design international network architecture along the continuum of crisis prevention, crisis management, and post-crisis stabilization. A comprehensive transformational homeland security agenda will embrace an international community of willing partners to improve interoperability and co-operability in concept, doctrine, process and structure.

Of course ultimate responsibility for “transformed” homeland security will always rest with individual nations operating different security structures. NATO lacks the resources to conduct truly effective counter-terror operations and furthermore risks isolating member states wary of seeing foreign forces or capabilities deployed within their borders. Thus, international initiatives must develop capacity used only to *complement* allied competencies in times of crisis when these are overwhelmed or require specialized assistance.

NATO can and should develop an added-value role building on existing infrastructure for intelligence cooperation and shared best practices. By using the ‘variable geometry’ subsets of NATO member states as test beds for

coordination of homeland security policies, the alliance can move beyond the patchwork of point solutions that today gives strategies of international cooperation an inchoate character.

As NATO develops its capabilities for expeditionary operations, it needs to revitalize plans and capabilities essential to realize its core mission: protecting Alliance territory as outlined in Article 5 of the North Atlantic Treaty. If the transatlantic allies cannot find common ground in civil defence strategy, fear of reprisal at home is likely to hamper more ambitious NATO missions in hostile environments abroad.

II. CURRENT STRATEGIC ENVIRONMENT

Today's international homeland security environment is characterized by divergent risk perceptions that emanate from an intercontinental definitional debate.

In the United States, post-9/11 homeland security has been advanced as a systematic attempt to reduce society's vulnerabilities to terrorist disruption. A wholesale reorganization of domestic security and border protection capabilities has been prioritized using the rhetoric of war. Although U.S. emergency planners have experience with "all-hazard" approaches to security risk, homeland defence is predominantly limited in focus to reducing vulnerability to terrorism.¹

¹ The mission statement of the United States Department of Homeland Security does not mention natural or accidental disasters. The Bush administration made the exclusion clear in Homeland Security Presidential Directive 8 most as well as the most recent budget proposal (for fiscal year 2007): "Response to natural disasters, including catastrophic natural events such as Hurricane Katrina, does not fall within the definition of a homeland security activity."

Canada and the Allied countries of Europe have adopted a different approach, largely preferring to build on existing institutional architecture to further develop competencies in “resilience” and “societal security”. This approach prioritizes investment in civilian emergency response and a cooperative interagency approach to domestic law enforcement

A. PRIORITIZING HSR MISSION AREAS

Divergent perspectives on an issue as fundamental to Alliance strategy as domestic security, complicates transatlantic cooperation; American critics continue to charge Europeans with complacency, and Europeans continue to respond with characterizations of the American response as inappropriately alarmist.² Over the past few years each side has become more attuned to the concerns of the other, though failure to appreciate what is required to manage the full range of contingencies continues to improperly distort patterns of resource allocation.

In September 2005, Hurricane Katrina demonstrated forcefully that not all homeland security challenges stem from terrorism. To the contrary, many experts in the area of emergency action preparedness and response continue to argue that terrorism is a low probability, and guarding against it should take a backseat to protecting against the more certain effects of storms, earthquakes, industrial accidents and the like. Though such arguments are made in good faith, the likelihood and likely cost of catastrophic terrorist attack puts a premium on measures designed to secure borders and protect critical infrastructure.

² Of course, there are differences within Europe as well, which make generalizations difficult. Recent British anti-terror laws, for instance, go even further than some U.S. efforts.

Given the structure of our densely populated, unvaccinated, and deeply connected societies, it is now possible to inflict widespread damage in ways never before thought possible. Though a number of these attack profiles are difficult enough to mount that they remain unlikely (large scale biological, nuclear and radiological attack for example), the high risk associated with even the low-probability events demands that we take them very seriously. Also note the unique threat presented by small scale bio, chemical, cyber, and enhanced conventional attack scenarios³. These are perhaps more likely to occur, producing physically localized effects and a psychological impact that can roil an entire nation.

While it's true that in preparing for terrorism-related threats many of the activities within the mission area also support preparedness for catastrophic natural disasters, an effective all-hazards approach will redefine the mission itself to include the preparation for, and response to, the full spectrum of terrorist attacks, as well as natural and accidental disasters. Leveraging resources to support such an ambitious endeavour will require an innovative approach to redefining and providing for appropriate priorities, structures, and processes.

Increased civil-military cooperation must be accompanied by a pledge among allied states to jointly adjust their planning, processes, command arrangements and training. At the operational level, mechanisms of coordination and a common situational picture are important to ensure an effective multi-lateral response to major incidents. A culture of increased cross-governmental cooperation should be actively promoted, with consideration

³ Violence produced by conventional means, but designed by scale or target to produce extraordinary effects.

paid to distinct organizational cultures that might otherwise undermine the effectiveness of joint structures.

B. ACCOMMODATING CULTURALIST THEORIES OF ORGANIZATIONAL CHANGE

The friction between differing organizational cultures and their values, beliefs and assumptions may derail even the best thought out policies and plans. Attempts to reconcile divergent perspectives on appropriate homeland security missions are likely to trigger defensive reactions as they begin to encroach on organizational turf. These shrill exchanges, in turn, are likely to complicate transatlantic cooperation by sucking the political oxygen out of any possible high-profile initiatives to protect European and North American societies.

Despite practical, conceptual and political obstacles to deeper cooperation in the area of homeland security, a growing array of cooperative ventures provides ample evidence for a rethinking of collective defence that spans the transatlantic space. These efforts underscore the resilience of transatlantic partnerships even in the face of serious disagreements.

Enhanced NATO capabilities reflect the measurable success of these efforts in facilitating international coordination and harmonization. In the years since September 11, the organization has taken steps to improve its military and civilian capabilities and structures to respond to crises spanning both homeland defence and societal resilience. These measures include cross-border cooperation on consequence management for both natural *and* man-made disasters. Allied member states have agreed to improve container security, expand customs cooperation, improve public-private partnerships to ensure

transportation security, and transfer passenger name record (PNR) data. They have agreed to incorporate interoperable biometric identifiers into travel documentation, enhance their policy dialogue on border and transport security, and start a dialogue on improving capabilities to respond to terrorist attacks involving chemical, biological, radiological or nuclear weapons. NATO airborne warning and control system (AWACS) aircraft have been used to provide air surveillance at the Athens and Turin Olympic Games and the Allied ships and aircraft of Operation *Active Endeavour* regularly help detect, deter, and protect against terrorist activity in the Mediterranean. By building capacity in the area of homeland security, NATO can play an important role in releasing member states from crippling dependencies on unwieldy bureaucracies.

III. A ROLE FOR NATO IN HOMELAND SECURITY

In the absence of a unifying strategy, national approaches to homeland security within the Alliance remain ad hoc and reactive in nature. Moreover, key decisions are transposed into national law at different rates and member states themselves have enacted policies that provide different degrees of protection, resulting in varying levels of security across the Alliance.

In the coming years, limiting concepts of national sovereignty in the defence of borders are likely to give way to an increasingly networked alternative. International coordination and standardization will add further robustness to national systems whose capabilities are overwhelmed by catastrophic incidents. But adaptation and integration of Alliance activities and capabilities will require articulation of a strategic direction. With value added

activities that include the development and intensification of existing cooperation projects, NATO is well positioned to take the lead in directing planning processes. However, as a supranational organization, NATO's role is also uniquely limited.

A. A TWENTY-FIRST CENTURY APPROACH TO ARTICLE FIVE

Article 5 was invoked for the first time in NATO history in a counterterrorism context on September 12, 2001, following the terrorist attacks on the United States. The need to consider terrorist threats has been a regular theme of NATO summits since then. Nonetheless, counterterrorism within the NATO region has remained mostly the responsibility of national ministries, making it impossible for the Alliance to function as a "first responder" in the traditional sense. Rather, it must focus on complementing the capabilities and institutions that exist among individual member states in a manner consistent with the principle of subsidiarity.⁴

This is particularly true given the value-added role already sought by the European Union in integrating national capabilities for civilian and civil-military crisis management. Since 21 of the 27 EU member states are members of NATO, and 4 of the remaining 6 are Partnership for Peace (PFP) members, they are unlikely to be inclined to duplicate activities in NATO and/or the Euro-Atlantic Partnership Council (EAPC) to which they already are committed in an EU context. To avoid unnecessary replication of planned and existing structures, the Alliance can function as a helpful adjunct to homeland security missions within

⁴ NATO's role must be limited to achieving objectives that cannot be better tasked by the states themselves at a national level.

the NATO region, not a lead agency. At the same time, the role of the Alliance in strengthening transatlantic integration is likely to require the development of core competencies in a number of select mission areas.

B. GLOBAL COMMONS

Internationally, the logic of neo-liberal globalization and the growing interdependence of infrastructure systems through increasing volume and variety of cross-border transactions in goods and services, free international capital flows, and more rapid and widespread diffusion of technology has exposed critical nodes of vulnerability surrounding a variety of activities in the global commons. These include threats to international maritime trade, possible attacks on offshore oil and gas installations, and interference with cyber-defence programmes. To secure these operational domains requires an active universally networked defence. NATO is well positioned to develop this capacity by leveraging strengths in network-centric command strategy into an operational advantage.⁵

1. *Commercial Shipping*

A growing substructure of cooperative efforts to combat criminal and financial threats to global connectivity has been nurtured among the U.S. and the EU, the G-7, and other OECD countries through the 1990's. Threats derived from commercial shipping in particular have been the focus of a tremendous amount of planning and cooperative effort internationally. In this vein, the

⁵ Appreciating that relative advantage is a measure of resources committed and control of available knowledge.

International Ship and Port Facilities Security Code ('ISPS Code'), and the United States' Container Security Initiative (CSI), represent significant multi-lateral progress in a relatively short space of time.

In response to the 1985 hijacking of the Italian liner *Achille Lauro* and in the context of protecting shipping from future terrorist attacks, the International Maritime Organization ('IMO') negotiated the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation ('SUA Convention') adopted in 1988. It deals with certain acts against shipping, including: seizing a ship; acts of violence against individuals on a ship; damage to a ship or its cargo so as to endanger its safe navigation; and endangerment of the safety of a ship by interfering with maritime navigational facilities or sending a false signal. The SUA Convention applies to ships that have journeyed outside, or are scheduled to pass outside, the territorial sea of a single state

In 2005, the SUA Convention was amended by a new protocol pertaining to maritime terrorism against shipping — SUA Protocol 2005. The focus of the SUA Protocol 2005 is WMD and their non-proliferation. New offences were created, including the use of shipping for terrorist activities,

An additional basis for inspection of vessels on the high seas is derived from the Proliferation Security Initiative (PSI). Although the PSI is expressed in terms of action based on flag state cooperation, the US has concluded a number of ship-boarding agreements with non-PSI state parties including Liberia, Panama, Belize, Cyprus, Croatia and the Marshall Islands.

These initiatives provide a solid platform on which NATO counter-terrorism activities could be based. The Alliance can act to mirror the shared surveillance

and monitoring arrangements of the PSI by extending interstate ship-boarding agreements within a geographically extended *Active Endeavour Operation*. Specialized radioactive material detection units may then be used to complement a pooled special operations (SOF) capability

Successfully “pushing borders out” will require unprecedented member-state cooperation. Improved capabilities in air and coastal surveillance, port security and CBRN detection carry serious resource implications. Allied approaches to capability building must be developed in tandem with new metrics to assess whether resource endowment is commensurate with the effects that need to be achieved. The international legal ramifications of extraterritorial initiatives will require careful mediation diplomacy.⁶

Establishment of a NATO Training Center focusing on maritime interdiction exercises in the Mediterranean Dialogue region could serve a dual purpose in deepening mutual trust in the region while further developing a core competence.

2. *Cyber-Terrorism*

Another area in which international cooperation is likely to prove necessary is in the implementation of comprehensive cyber-defence strategy. Plans gained a new urgency following the three-week Distributed Denial of Service (DDoS) attacks that targeted Estonia in May 2007. NATO’s use of

⁶There are differing opinions on enhancing international legal authority for interdictions on the high seas and in international airspace. Currently, vessels on the high seas have the rights of freedom of the seas and innocent passage under the Law of the Sea Convention and customary international law. Some states prefer to continue operations within existing international law, whereas others (including the United States) would like to enhance or change international law to expand the capability to interdict potential WMD-related transfers.

sophisticated network-centric operations to enable coalition integration, positions the Alliance to share a lead role in responding to 21st century operational security challenges.

NATO provides a natural framework in which to develop a joint protection system that can be used to standardize signature- and behaviour-based defences.⁷ Housing the program within the NATO Information Security Technical Centre (NITC) will cut into the resources required for the enterprise by building on existing capacity.

In addition to devising best practice cyber-security strategies, the directorate will be tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing priority alerts and early warnings for cyber threats, improving information sharing between member states, and responding to major cyber-security incidents with in-house expertise and national-level recovery efforts.

Though it's doubtful that terrorists have the combined IT and control system skills required to penetrate a utility network, the attacks of May 2007 effectively demonstrated that those who would threaten our cyber-infrastructure are capable and increasingly adaptable. The Alliance must take steps to ensure that the same can be said for NATO member states.

C. CIVIL EMERGENCIES AND CONSEQUENCE MANAGEMENT

For decades, NATO and other security alliances have rigorously planned strategic and operational responses to military crises. The same transatlantic

⁷ NATO's current focus remains on content verification technology that can be used to prevent a repeat of Estonia's DDoS espionage attacks.

cooperation can today be effectively leveraged to augment national capabilities in civil contingency planning and response. Improving NATO's capabilities for consequence management builds on the concept of societal "resilience". To detect, prevent and manage disruptive challenges ranging from terrorist attacks to pandemics to large-scale natural disasters in the NATO region, the Alliance can provide unique planning, logistical, and operational support.

Natural and technological disasters are managed under NATO's Civil Emergency Planning Directorate. The embedded Euro-Atlantic Disaster Response Coordination Centre exists to organize relief efforts but draws resources at levels commensurate with an otherwise peripheral agency. This trend should be reversed with resource distribution reflecting the elevation of an all hazards approach to a core competence.

D. BIOLOGICAL THREAT

The world is on the cusp of a revolutionary challenge posed by pathogens and their accessibility to state and non-state actors. Given the early international ramifications of a biological attack, it is in the explicit interest of any nation to ensure that there are as few 'weak links' as possible in the international community's ability to mount an effective public health response to biological threats of international consequence.

Lacking sufficient vaccine stockpiles for their populations and limited in their production capacity, many NATO members are likely to be unprepared for the eventuality of catastrophic pandemic. International health organizations are

unlikely to be able to fill the void given their woefully under funded and under staffed crisis management programmes.⁸

In the absence of effective guidance and reliable access to pooled resources, any attack is likely to entail large-scale quarantine with severe economic, social and political repercussions for affected nations. In spite of the likely cost of inaction, states of the European Union have opted against a shared stockpile of smallpox vaccine owing to political difficulties associated with selective allocation to member states in an emergency. If the closely aligned EU is unable to agree on how to share a security asset as critical as the smallpox vaccine, the prospects for broader international sharing mechanisms appear bleak.

These challenges require actions beyond piecemeal extensions of current policies. The long-term answer is likely to require a shift in focus from disease-specific vaccine stockpiling to drug design and manufacture. A focus on drug design will permit short notice production of vaccine for distribution by rapid reaction teams. This requires unprecedented integration of the public health and national security communities. NATO's strategic added-value consists of its experience with interoperability and corresponding competencies in centralizing information and prioritizing action for government response. The organization is well-positioned to contribute management experience with international 'rapid reaction' teams. Though operationally defunct as of 2008 (the result of a failure among member-countries to honour troop pledges of up to 25,000), a modified (and less ambitious) NATO Response Force (NRF) should augment operational

⁸ The entire 2004/2005 WHO budget for bioterrorism preparedness amounted to approximately US\$6.3 million. In total resources the organization approximates a middle-sized hospital in England.

training in emergency management and evacuation control with pandemic response and recovery training. A comprehensive effort to render nations immune to the effects of bioterrorism or a CDC category 5 pandemic requires a lead agency to coordinate and deploy the contributions of the public health and national security communities. Building on existing capacity, the Alliance can bring this mission-area into its strategic fold with relative ease.

E. BEST PRACTICE INFORMATION SHARING

The most clear gap in the coordination of international homeland security is precisely the added value of Allied Command Transformation. The military command tasked with coordinating doctrine within NATO is uniquely positioned to promote an integrated assessment of global threats, risks, and existing/potential security measures. With information and intelligence centralized in a best-practice Alliance “clearing house”, threats can be prioritized and various governments coordinated to establish appropriate monitoring mechanisms. Institutional mechanisms to facilitate this level of cooperation already exist in NATO’s Terrorist Threat Intelligence Unit, the Euro-Atlantic Disaster Response Coordination Centre, and the EAPC’s Partnership Action Plan Against Terrorism.

Synchronizing these tools and adding a clearing house function to the aggregation of intelligence will provide for the coordination of specializations among NATO allies. Countries that lack the capability to manage a particular

crisis can thus be directed toward those that may be able to help.⁹ Information on the deployment of assets can be shared with appropriate national and EU law enforcement and civilian authorities to decrease NATO community vulnerability interdependence. This process can be immediately expedited by setting up a joint NATO-EU Capabilities Group to parallel databases for civilian and military capabilities relevant for homeland security missions. While facilitating community awareness of respective capabilities, the corresponding deepening of intelligence ties would also increase the chance of interdicting attacks.

However, the exchange of information among the member countries' intelligence services is effective only within the obvious limits imposed by the nature of the intelligence community. A new joint defence dimension will require access to information available only at the highest levels of government. Building on the model of the North Atlantic Council at Defence Ministers Level (NAC-D), home affairs minister meetings can provide an initial multilateral forum to review NATO's capacity to respond to consequence management challenges. Over time, a dialogue forum could expand to accommodate expert groups addressing practical cooperation projects relevant for transatlantic homeland security transformation.

⁹ Military capabilities relevant for stabilization, intervention, and homeland security include, among others, intelligence, surveillance, and reconnaissance, command and control, mobility, CBRNE detection and protection, and medical services.

IV. CAPABILITIES REQUIRED

During the Cold War, NATO's purpose was clear: the Alliance was a transatlantic politico-military partnership directed at deterring and defending against Soviet aggression. But containing the Soviet Union was not the organization's founding principle. Rather, NATO was structured to "safeguard the freedom, common heritage and civilization of [the member states'] peoples, founded on the principles of democracy, individual liberty and the rule of law." In a post-Cold War era that presents challenges outside of NATO's original purview, the time is right to open the prospect of community expansion to countries that share these commitments.

A. PROJECTING RESILIENCE

Transferring principles of homeland security transformation to neighbouring countries offers tremendous potential for expanded cooperation within a rejuvenated Partnership for Peace and its political umbrella, the Euro-Atlantic Partnership Council. Non-aligned countries worldwide have decades of experience with approaches to societal defence and often represent areas in which forward defence and security sector reform are critical in reducing risks to the transatlantic community.

For example, the strategic dependence of Europe and the United States on oil and gas resources in North Africa, the Arabian Peninsula and Central Asia puts a premium on energy infrastructure security in countries of origin and transit. "Projecting resilience" to these areas on the outskirts of the Euro-Atlantic

community will thus protect member-state societies directly while simultaneously strengthening the weakest links in global security networks.

Joint organizational and materiel reform can be used to develop warning information networks for critical infrastructure as well as to provide technical access to international security and health care databases for third country partners (the Rapid Alert System for Biological and Chemical Agent Attacks for example).

In time, the Alliance might consider amending Article 10 of the 1949 North Atlantic Treaty which confines NATO membership to European countries (in addition to Canada and the United States). A bioterrorist attack of contagious disease will not distinguish between “allies” and “partners”.¹⁰ For purposes of interoperability, aligning strategic and operational doctrine with countries like Australia, Brazil, Japan, New Zealand, and South Africa makes good sense.

At the same time, changes to institutional composition would further stretch limited resources and slow Alliance reaction time. Existing interoperability gaps already raise questions as to the future viability of multilateral operations within the Alliance. Compounding the problem by bringing new countries into the strategic fold may well undermine force cohesion and threaten the institutional logic behind the existence of the Alliance.

Whether or not sought after levels of interoperability require full institutional integration, an intensification of security cooperation with allies around the world remains desirable.

¹⁰ The crucial doctrinal difference between “allies” and “partners” that structures relationships within the Alliance today turns on the concept of cohesion. Partners may contribute to the anti-terrorism campaign, help with physical protection and tactical measures, and cooperate to defend airspace and sea lanes but they do not share sufficiently common values to be part of the “circle of cohesion.”

B. CONCEPT DEVELOPMENT AND EXPERIMENTATION (CDE)

Concept development and experimentation (CDE) can be used to develop models that improve information integration and strengthen multinational information sharing on threat assessments, incident reporting, and early warning.

More than other policy areas, homeland security must deal with critical interconnections. Especially in the field of infrastructure protection, secondary or third order effects of power shortages and the safety and security of critical nodes require comprehensive assessments of interdependencies as a basis for implementing adequate counter measures. Chokepoint analysis should be complemented by joint training in real-world exercises to effectively synchronize doctrine, training, and education in government agencies that span the transatlantic divide.¹¹

The modelling and simulation of multiple, interdependent infrastructures is immature and will require the effective mobilization of the Joint Experimentation, Exercises and Assessment (JEEA) subdivision within NATO Allied Command Transformation as well as directorates within the European civil-military planning cell in the EU Military Staff, the European Commission, emergency responders from NATO and EU countries, academic research institutes, and, importantly, the private sector.

¹¹ The recommendations of ministerial-level exercises can produce tangible results and flood governmental circles with productive insight. Appropriate examples include *Atlantic Storm*, a ministerial-level exercise convened on January 14, 2005 that simulated a series of bioterrorist attacks on the transatlantic community. The exercise was designed, organized and convened by a team from the Center for Biosecurity of the University of Pittsburgh Medical Center (PA, USA), the Center for Transatlantic Relations at the Paul H. Nitze School of Advanced International Studies of Johns Hopkins University (Washington, DC, USA), and the Transatlantic Biosecurity Network, a group of medical, public health and security experts from Europe and North America.

C. ROLE OF THE PRIVATE SECTOR

Private business, government, and Alliance security increasingly relies on interdependent networks of critical infrastructure that include the telecommunications, energy, financial services, and transportation sectors. These systems have traditionally embraced a culture of physical and logical independence. It has only been in the past decade that the revolutionizing impact of corporate consolidation and industry rationalization have produced vulnerabilities associated with interconnectedness.

In an intensively populated “just in time” economy with tight dependencies lacking in any surplus capacity, incidents like the September 2000 UK trucking industry strike¹² and the January 2003 Slammer SQL Internet Worm¹³, can bring a country to its knees. The natural inclination of private operators to shield valuable market intelligence from competitors has compounded the problem by restricting government access to proprietary vulnerability data required for effective risk modelling.

There is a need to forge new patterns of interaction in the public-private interface to better link the public Common Relevant Operational Picture (CROP) for homeland security with equivalent corporate instruments that are already in use or have yet to be established.

¹² The strike protesting fuel duty took the form of coordinated picketing outside almost all fuel depots. The just-in-time delivery principles of the oil distribution network quickly dried up retail petrol supplies. Within 24 hours, hospitals, deprived of their staff, were near closure. Within 48 hours, supermarket shelves were bare of staple foods. The financial impact of the week-long fuel drought was estimated at close to £1 billion.

¹³ The virus not only slowed web traffic but also incapacitated the 911 emergency call dispatch center in Seattle, shutdown thousands of Bank of America ATMs, and delayed a handful of Continental Airlines’ flights.

Though integration may be resisted by some obstinate corporate security and supply chain managers, many more today realize that safety makes sense for the bottom line. The 24-hour manifest rule in the cargo industry, for instance, has actually increased productivity.

Building on the uniquely American innovation of voluntary participation in Information Sharing and Analysis Centers (ISACs), NATO can expand participation in homeland security transformation to include private sector mechanisms for transatlantic information exchange. These Centers typically serve as the tactical and operational arms for sector specific information-sharing efforts designed to facilitate the free exchange of intelligence on vulnerability data and protection strategies. For example, the Financial Services Information Sharing and Analysis Center (FS/ISAC) gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector. Sources of information include commercial companies that gather this type of information, government agencies, academics, and other trusted sources. After analysis by industry experts, NATO can coordinate pass-downs to participants (public and private) containing a description of the threat or vulnerability, its severity, and recommendations for solutions.

The Alliance can also take the lead in introducing private sector, civil society building capacity to out-of-area hotspots. In this vein, NATO's operational commander has escorted a number of Chief Executive Officers from the private sector on frequent visits to Afghanistan. They have represented companies in fields as diverse as housing, health, education, construction, banking, electricity, information technology, radio and television. Sustainable economic growth in

countries of interest to the Alliance is a goal that can be reached under the guidance of NATO by mobilizing funding and expanding development-related investment. Under the NATO umbrella, Microsoft's citizenship programme in Afghanistan represents positive organizational gains in this arena, where a focus on IT training and capacity building continues to stimulate economic growth and technology transfer.

By further engaging the private sector, the Alliance can take steps to ensure both that "connectivity vulnerabilities" are not built into future systems and that gains in upcoming stability operations can be consolidated quickly with the active participation of the captains of industry.

IV. PROJECTED IMPACT ON NATO FORCE POSTURE

Important command and force posture issues follow from the reformulation and strengthening of NATO's role in homeland security and resilience. Do existing NATO military capabilities exceed potential requirements for Alliance-wide deterrence and thus allow for conversion of remaining forces to homeland defence missions?¹⁴ Should NATO develop a homeland defence platform in a command equivalent to the U.S. Northern Command (USNORTHCOM)? The answers turn on the adaptive capacity of already existing institutions.

Where inspection shows that these may be deficient in specific areas (force planning, equipment, readiness), the trade-off and interplay between two options will have to be analyzed carefully: 1) Rely upon existing structures, but

¹⁴ The US military has, for example, dedicated a command and control element together with a number of National Guard WMD-detection teams for domestic use only.

approve an organizational design that provides for additional capabilities as warranted by homeland defence requirements; or 2) Create a new command and assign forces that are sized, equipped, and trained exclusively for the homeland defence mission.

Each approach is likely to incur financial, political and strategic costs though the latter, in particular, is unreasonably likely to impact on Allied flexibility and deployment of forces for more traditional purposes.

A shift from force-oriented, terrain-based defence planning to capability-oriented approaches obviates the prohibitive expense of creating standing capabilities by favouring complementary training in passive homeland defence tasks. Active units contributed to NATO operation can be placed on heightened alert for homeland security and resilience (HSR) emergencies on a rotating basis with two NATO standard brigades consisting of approximately 4,000 to 5,000 troops trained to respond to potential actions involving military assistance to civil disturbances. These troops may be placed within a reformulated (and likely modestly sized) NATO Response Force.¹⁵

However to preserve core competencies in conventional military response, specialized training for HSR tasks should not restrict availability for deployment to an overseas contingency. Training would be designed to augment national efforts in the period immediately following a catastrophic attack/disaster by coordinating extant capabilities in homeland defence and

¹⁵ In a recurring problem that is likely to impede efforts to develop specializations in HSR response, the 26 NATO members have had trouble finding the troops, transport planes and helicopters needed to keep such a large force at full readiness. In addition, many countries are already fully stretched in other NATO missions in Afghanistan, the Balkans, Middle East and Africa. Germany, for example, has thousands of troops in Afghanistan and NATO has upped its commitment there from 7,000 to 40,000 soldiers since the NRF was declared ready last November. America, for its part, has 169,000 troops stationed in Iraq and has been unable to honour its NRF pledge.

consequence management among NATO member forces (decontamination teams to respond to CBRN attack, local airlift assets, communications and intelligence assets, and Civil-Military Coordination Group capabilities). In fact, these forces are already employed when the level of threat exceeds the capacity of State security and police forces. For example, NATO's Airborne Warning and Control System (AWACS) monitors air space during summit meetings (Operation Peaceful Summit 2006) and antiaircraft batteries are simultaneously deployed for the defence of specific locations in surrounding areas.

As the frequency of force deployment for HSR contingencies increases, NATO headquarters would no doubt need additional assets focused on homeland defence missions. Allied Command Operations (ACO) is the logical platform to host NATO military forces for these missions. A designated principal subordinate operational headquarters can function as the command structure responsible for deployment. By converting an existing principal subordinate command to coordinate organizational efforts within this mission area, time and resources otherwise devoted to creating new structures can be diverted to support the Senior Civil Emergency Planning Committee¹⁶ and its Euro-Atlantic Disaster Response Coordination Center.¹⁷

¹⁶ NATO's Senior Civil Emergency Planning Committee has already developed a Civil Emergency Planning Action Plan, which calls for the development of nonbinding guidelines and minimum standards for the protection of the civil population against CBRN risks. With sufficient resources at its disposal, the committee can set about rationalizing inventories of national civil and military capabilities that could be made available in the event of CBRN attacks.

¹⁷ NATO's Euro-Atlantic Disaster Response Coordination Center is the focal point for coordinating disaster relief efforts of the 46 EAPC nations in case of natural or technological disasters. Resources contribute to developing capacity to manage contingencies including the Pakistan earthquake, where NATO sent engineers, medical units, helicopters and crews, and a field hospital from its Response Force.

Because NATO's military commands were organized primarily to manage territorial defence of Europe, a home security combatant command modeled after the United States Northern Command (NORTHCOM) does not appear necessary. However, some improvements to NATO's strategic structure may make sense. Supplemental to changes in function within Allied Command Operations, an Assistant Secretary General for Homeland Defence is advisable as a means to charting NATO's future in the homeland defence arena. This planning body can also strengthen ties to regional organizations such as the Black Sea Economic Cooperation (BSEC) and the Southeast European Cooperative Initiative (SECI).

V. CONCLUSIONS

The Fulda Gap has long been deserted and Soviet submarines no longer threaten Cold War sea lanes. The existential threat of our time has since assumed a transnational character with an unprecedented capacity to exploit nodes of vulnerability in the complex interdependent systems on which free societies depend. NATO's operational mission has evolved with this threat and today the organization is uniquely positioned to act as lead agency in the coordination of relevant member-state capabilities.

If Alliance governments fail to defend their societies from attack while providing appropriate tools for recovery, the Alliance will have failed in its most fundamental task. The organizational logic sustaining NATO will have been marginalized and the security of Europe and North America will be further compromised.

Appropriate transformational approaches to transatlantic homeland security will require common planning capabilities, security sector reform and intelligence-sharing. As a military alliance, there is still scope for NATO to help with infrastructure protection, natural disaster relief, and antiterrorism efforts. Beyond piecemeal extensions of current policies, we must act today to design the institutional network architecture of tomorrow along the continuum of crisis prevention, crisis management, and post-crisis stabilization.

CRISIS PREVENTION

- Establish a Common Relevant Operational Picture (CROP) among allies to ensure an effective multi-lateral response to major incidents.
- Account for distinct organizational cultures and seek only to complement the capabilities and institutions that exist among individual member states in a manner consistent with the principle of subsidiarity.
- Mirror the shared surveillance and monitoring arrangements of the Proliferation Security Initiative (PSI) by extending interstate ship-boarding agreements within a geographically extended *Active Endeavour Operation*.
- Adjust the resource profile of NATO's Civil Emergency Planning Directorate and the embedded Euro-Atlantic Disaster Response Coordination Centre to reflect the elevation of an all hazards approach to a core competence.
- Provide technical access to international security and health care databases to third country partners.
- Building on the model of the North Atlantic Council at Defence Ministers Level (NAC-D), implement regular home affairs minister meetings to review transatlantic homeland security transformation challenges.
- Mobilize the Joint Experimentation, Exercises and Assessment (JEEA) subdivision within NATO Allied Command Transformation to conduct regular joint exercises with directorates within the European civil-military planning cell in the EU Military Staff, the European Commission, emergency responders from NATO and EU countries, academic research institutes, and the private sector.

- Forge new patterns of interaction in the public-private interface to better link the public Common Relevant Operational Picture (CROP) for homeland security with equivalent corporate instruments that are already in use or have yet to be established.
- Expand participation in homeland security transformation to include private sector mechanisms for transatlantic information exchange (voluntary participation in Information Sharing and Analysis Centers for example).
- Designate a principal subordinate operational headquarters to coordinate HSR organizational efforts under the auspices of Allied Command Operations (ACO).

CRISIS MANAGEMENT

- Standardize signature- and behaviour-based cyber-defences within the NATO Information Security Technical Centre (NITC). Issue priority alerts and early warnings for cyber threats, responding to major cyber-security incidents with in-house expertise and national-level recovery efforts.
- Coordinate consequence management specializations among NATO allies within a joint NATO-EU Capabilities Group.
- Place active units on heightened alert for HSR emergencies on a rotating basis with two NATO brigades trained in management of catastrophic civil disturbance as a secondary competency.

POST-CRISIS STABILIZATION

- Coordinate and deploy the contributions of the public health and national security communities to manage the effects of bioterrorism or a CDC category 5 pandemic.
- Take the lead in introducing the private sector's civil society building capacity to out-of-area hotspots.