THE EUROPEAN UNION PILOT PROJECT ON TRANSATLANTIC METHODS FOR HANDLING GLOBAL CHALLENGES IN THE EUROPEAN UNION AND UNITED STATES

EU-U.S. Security Strategies

COMPARATIVE SCENARIOS AND RECOMMENDATIONS

Full Report

This project is funded by the European Union

A project implemented by

Istituto Affari Internazionali (IAI)
Swedish Institute of International Affairs (UI)
Fondation pour la Recherche Stratégique (FRS)
Center for Strategic and International Studies (CSIS)

THE EUROPEAN UNION PILOT PROJECT ON TRANSATLANTIC METHODS FOR HANDLING GLOBAL CHALLENGES IN THE EUROPEAN UNION AND UNITED STATES

EU-U.S. Security Strategies

COMPARATIVE SCENARIOS AND RECOMMENDATIONS

Full Report

This project is funded by the European Union

A project implemented by

Istituto Affari Internazionali (IAI)
Swedish Institute of International Affairs (UI)
Fondation pour la Recherche Stratégique (FRS)
Center for Strategic and International Studies (CSIS)

This publication has been produced with the assistance of the European Union within the framework of the Pilot Project on Transatlantic Methods for Handling Global Challenges. The contents of this publication are the sole responsibility of IAI, UI, FRS, and CSIS, and can in no way be taken to reflect the views of the European Union.

CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The partnership between the European Union (EU) and the United States is of central importance in addressing a multitude of complex global challenges. Despite recurrent ups and downs, EU-U.S. cooperation remains the most economically significant and integrated relationship in the world. Europe and the United States have long been drivers of global economic prosperity, accounting for half of the world's gross domestic product (GDP), 40 percent of trade, and 80 percent of official development assistance. Yet it has been the political and security arenas that have always provided the crucial test of the partnership's effectiveness, durability, and solidarity. The capstone of this partnership was the inauguration of the New Transatlantic Agenda in 1995, which has emerged as a core element of the transatlantic relationship by promoting and encouraging a transatlantic response to global security challenges and promoting, *inter alia*, peace and stability.

In the spirit of the New Transatlantic Agenda and within the framework of the European Commission's pilot project, "Transatlantic Methods for Handling Global Challenges in the European Union and United States," an effort was undertaken to assess the current state of the EU-U.S. security relationship and offer recommendations on fostering common approaches and enhancing its capacity to deal with emerging challenges. The research, "EU-U.S. Security Strategies: Comparative Scenarios and Recommendations," was undertaken by a transatlantic team led by the Istituto Affari Internazionali (IAI) in Rome and including scholars from the Center for Strategic and International Studies (CSIS) in Washington, the French Fondation pour la Recherche Stratégique (FRS), and the Swedish Institute of International Affairs (UI).

Generously funded by the European Commission's Directorate General External Relations (DG RELEX), the main purpose of the "EU-U.S. Security Strategies" project was to provide European and American policymakers with insight, inputs, ideas, and tools to enhance and deepen transatlantic dialogue on four security issues of common concern for the European Union and the United States and to identify potential transatlantic convergences. The four subject areas were identified as follows:

- The **definition of external security and related European and American implementation models**. The research partners examined how Europeans and Americans have defined external security and conducted strategic security reviews. They compared recent American and French national security reviews, the 2003 European Security Strategy (ESS) and its subsequent review in 2008, and the 2010 NATO Strategic Concept.
- The **nexus between internal and external security** and how various threats can be addressed by the EU and the United States. The research team examined the blurring borders between internal and external security and cross-border threats in the areas of cyber security, biosecurity, pandemic preparedness and response, and disaster preparation and response.

- Current **trends in the defense and security market and related industrial perspectives** in Europe and the United States. The research team examined the American and European security and defense industrial bases and determined that both are undergoing a comprehensive restructuring to better respond to contemporary challenges with the security industrial base and market requiring the more dramatic transformation. Both the EU and the United States are struggling to make the security market more efficient, with different methods and with mixed success.
- **EU-U.S. cooperation for today's transatlantic security challenges**. The research team assessed transatlantic cooperation on four complex security problems, including a nuclear-armed Iran, Afghanistan, the Haiti earthquake and natural disasters, and piracy off the coast of Somalia and suggest that the evolving global security environment requires better organization and enhanced capability within the EU and a stronger, direct EU-U.S. security relationship.

KEY FINDINGS

Despite extensive transatlantic security cooperation, the research team identified existing gaps and has put forward specific recommendations to enhance transatlantic dialogue and EU-U.S. cooperation. It is clear that strategies and rhetoric must be put into practice requiring policy makers to place greater emphasis on operational and tactical cooperation on the ground. Moreover, the EU-U.S. partnership must be a driver to boost development of technological and industrial—and thus operational—capabilities. As the EU strengthens into a coherent and cohesive counterpart to the United States (e.g., the nascent European External Action Service will provide such important strengthening), the following overarching project recommendations could provide useful insights to concerned EU and U.S. policymakers into the many rich and diverse opportunities to strengthen the EU-U.S. partnership in the security field:

- **Develop a European strategic security and defense review or White Paper** that would become a foundational element of a comprehensive transatlantic strategic security and defense review.
- **Increase EU-U.S. operational coordination and training**, agree on shared definitions and concepts, and build issue-specific cooperative structures in the areas of cyber security, biosecurity, disaster preparedness and response, and pandemic influenza that foster systematic exchanges of lessons-learned and best practices.
- **Improve governance of the transatlantic security sector** and efficiency of the industrial base to enhance its understanding of emerging requirements, efficiency, and responsiveness; strengthen the regulatory environment; and avoid restrictive and protectionist practices to produce a more open and competitive transatlantic security market.
- **Develop an EU–NATO security agreement** to allow for easy exchange of classified information and enhance operational effectiveness. Undertake routine EU–U.S. security consultations, exchanges of situation awareness reports, and exercises to enhance transatlantic response capabilities, augment EU crisis response capabilities, and integrate them with NATO's comprehensive approach to complex security and humanitarian operations.

The main findings of the research team reconfirmed the critical role that both the EU and the United States play in the international security arena despite a reduction of traditional security threats. Without doubt, an effective and solid EU-U.S. partnership remains the essential link in identifying and addressing current and future emerging threats as well as implementing new security paradigms. Moreover, as European and American security is so mutually intertwined and interdependent, practiced coordination and consistent action is crucial to protect the transatlantic space and project security globally.

The following provides a more detailed summary of the key judgments and findings of each specific security issue that was examined.

ISSUE 1
DEFINITION OF EXTERNAL SECURITY AND IMPLEMENTATION MODEL

Research Leader: Center for Strategic and International Studies (CSIS)

In the post–Cold War era, European and North American states as well as international organizations such as the EU and NATO had to deal with a more and more complex and uncertain security environment, where strategic surprises have become more the norm. The need to rethink strategic goals, adjust strategies, and reorganize policies and bureaucracies has increased. As a result, the number and importance of strategic security reviews have increased at both the national and international levels.

The CSIS-led research team examined the evolution of how Europe and the United States have defined external security and how each conduct strategic security reviews. For the purposes of this project, external security was viewed as one country's national security whereby traditional external threats emanating from outside a national or multinational organization's borders (e.g., defense) are combined with internal security challenges (e.g., homeland security, resilience). The research team initiated a comprehensive comparison of two national and two multinational security strategic reviews. The two national security strategies that were reviewed were the 2008 French White Paper on Defense and National Security (*Livre blanc sur la défense et la sécurité nationale*) and the 2002 and 2010 U.S. National Security Strategies (NSS). The multinational strategies that were analyzed included the 2003 European Security Strategy (ESS) and its subsequent review in 2008 and the 2010 NATO Strategic Concept.

Each of the four strategic reviews were placed in their own historical context to better frame the political environment in which they were written, with special attention given to any particular legislative or other mandatory requirements. As described by Camille Grand (Fondation pour la Recherche Stratégique, or FRS) in his contribution, in France there is no legal obligation to produce a strategic security review document. French strategic analysis and policies are mostly derived from presidential and other senior official speeches. The *Livre Blanc* was only the third such formal strategic review to occur since the 1970s, making the review a significant event. The 2008 paper was developed at the direction of a newly elected president who wished to develop a greater national consensus around France's defense and security policy.

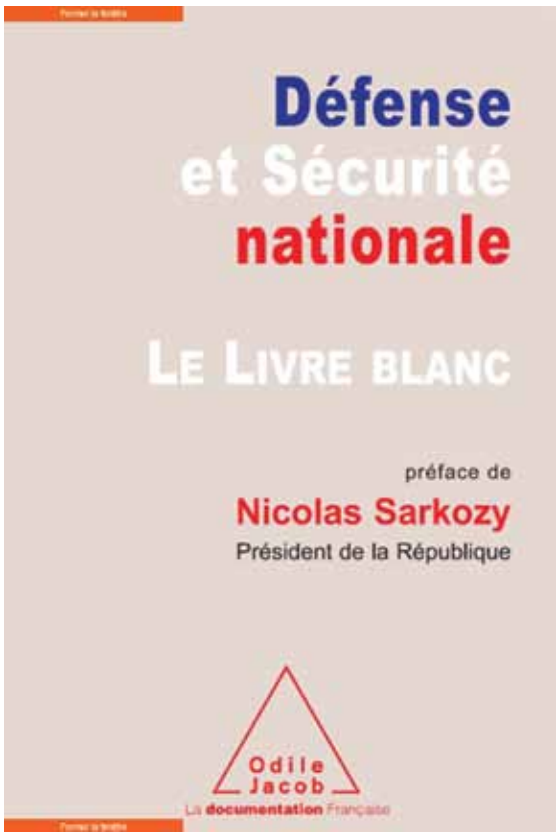
In contrast, Heather Conley, Manuel Lafont-Rapnouil, and Michael Cass-Anthony (CSIS) highlight that the U.S. NSS is mandated by legislation requiring the Executive Branch to provide a national security strategy to Congress on an annual basis. The NSS represents the first in a series of strategic reviews, closely followed by the Quadrennial Defense Review (QDR), which provides more direct guidance to the annual defense budget process. Typically, a new American president uses the NSS to frame the global strategic environment and prescribe America's ability to meet the challenges of this environment while differentiating, repudiating, or justifying past policies and actions.

Multilaterally, as recalled by Stefano Silvestri and Alessandro Marrone (Istituto Affari Internazionali, or IAI), NATO does not

have a formalized time schedule to conduct its strategic reviews; rather, it undertakes them at irregular intervals in response to a particularly complex set of international challenges. For example, NATO's 1967 Strategic Concept was not changed for 24 years. However, to adapt to the rapid changes in global security following the end of the Cold War, NATO has undertaken three strategic reviews in 1991, 1999, and 2010.

Mark Rhinard and Erik Brattberg (Swedish Institute of International Affairs, or UI) illustrate that although the first formal attempt by the EU to undertake its own strategic review was in 2003, the concept of developing an EU-wide foreign and security policy existed a decade earlier as articulated in the Maastricht Treaty, and later reaffirmed in the Lisbon Treaty. The need to better coordinate EU member states in order to gain more global influence, coupled with the political imperative to shape a European policy independent of American thought in the wake of the invasion of Iraq in 2003, led to the development of the strategic review initiated by the then EU high representative Javier Solana.

All four strategic reviews were shaped by their own unique bureaucratic and political processes, which had a dramatic impact on its strategic value and final effect. Prior to the drafting of the *Livre Blanc*, French president Nicholas Sarkozy appointed a commission chaired by a widely respected and leading official to shape the strategic review. The commission was composed of representatives of government agencies, parliamentarians, academics, and respected individuals and held publicly televised and online hearings as well as a wide range of consultations and visits to the field, including abroad, to discuss key issues and gain valuable input. The American process, however, is much more insular, occurs behind closed doors, and is led by the White House National Security Staff. In 2010, the process was led by the deputy national security advisor for strategic communications with input from various departments (e.g., the State and Defense Departments and intelligence agencies). When the final strategic document is being readied, high-level administration officials brief members of Congress and key allies on its findings before its public release.



French White Paper on Defense and National Security (2008), http://www.ladocumentationfrancaise.fr/catalogue/9782738121851/index.shtml.

Like the French approach, NATO tasked an outside entity, a Group of Experts, led by former U.S. secretary of state Madeleine Albright, to provide input (in the form of a report, *NATO 2020: Assured Security; Dynamic Engagement*) to the NATO secretary general prior to the official drafting of the Strategic Concept. The Group of Experts consulted with senior officials in NATO capitals—and in Russia—and held several seminars that included

NATO Secretary General Anders Fogh Rasmussen presents the 2010 NATO Strategic Concept to the media.

©NATO, http://www.nato.int/cps/en/natolive/photos_68423.htm.

European and American think tanks and experts on a select set of critical questions. This inclusive process allowed many stakeholders, even non-NATO members, to provide input into the process. For the EU in 2003, the strategic review process was more exclusive with only a small group of individuals involved in the drafting process. This very streamlined and less bureaucratic approach allowed the strategy draft to be completed in a very short period of time. The draft document was then shared with select European think tanks, and three external workshops were held to elicit comment and feedback. Following the workshops, the draft was made available to member states for comment, where additional issues were added and other more pronounced issues were diluted to ensure consensus on the final document, *A Secure Europe in a Better World*.

There were several common elements across all four strategic reviews regarding strategic content and new strategic vocabulary and thinking. First and foremost was the widening of the scope of national security to combine external and internal security strategies, to acknowledge that the traditional barrier between foreign and domestic security has been removed. There was strong evidence of the introduction of new strategic vocabulary in the wake of September 11, 2001, and the importance of the role of crisis in propelling new strategic thinking. New terms such as the "global war on terrorism," "preemptive actions," and "resilience" were introduced into strategic documents. The term "resilience," meaning to "adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption," originated in the UK, was adopted in the *Livre Blanc,* and now has been embraced in the United States. Similarly, the European use of the term "comprehensive approach" to characterize use of all available strategic tools has found its way into recent U.S. security documents as a "whole of government" approach.

For the *Livre Blanc*, the lasting impact was the establishment of a national security concept for France, which laid the groundwork for its decision to reintegrate into NATO's military structure and had substantial impact on reorganizing France's national security structure. For the U.S. 2002 and 2010 NSS, there was also substantial reorganization and creation of new security organizations, such as the Department

of Homeland Security and the Director of National Intelligence which was an effort to integrate external and internal security. However, it is difficult to make definitive judgments on the impact of any multilateral strategic review. For NATO, the 2010 Strategic Concept underscores strategic continuity and core capabilities while simultaneously (and slowly) adapting to changes in the security environment, such as cyber security and counterinsurgency operations. For the EU's first attempt at a strategic review, it is even more difficult as the strategy contained no mechanism for evaluation or review and appears to be more aspirational in approach.

During the Cold War era, most strategic security reviews were classified documents. Today, strategic reviews are more valued for their ability to educate the general public about current and future threats to national security and provide a venue for governments and multilateral organizations to offer their vision of how best to meet these challenges. Moreover, it is an exercise that brings disparate elements of the bureaucracy together to find common ground and strategic understanding; in essence, the process creates an enduring strategic culture that adds value to the day-to-day work of any complex organization. Finally, a strategic review had a profound impact on bureaucratic structures, whether it is creating new, streamlining current, or downsizing old.

There were several areas of concern noted in each strategic review analysis. In particular, strategic reviews can tend to be backward-looking and reactive documents that justify previous actions or budget decisions. A successful strategic review must look boldly into the future; identify new emerging security trends; and make the necessary adjustments to policy and budget lines. This is why it appears to be increasingly important to seek the advice and counsel of outside experts and organizations. An insular review exercise tends to validate previous decisions and lacks political credibility; an open, transparent process that embraces new opinions and challenges long-held precepts ensures a document with strategic durability and buy-in from a broader policy community. However, even the most prescient of strategic documents will not be successful if it is not tethered to budgetary resources to implement stated strategic objectives. National strategies, such as the U.S. NSS and the *Livre Blanc*, did a much better job at connecting strategic objectives to resource allocation. In fact, the *Livre Blanc* explicitly states the procurement schedule that will meet its strategic objectives. The U.S. NSS is not explicit in budgetary terms, but subsequent strategic documents like the QDR and the Defense Department's budget do provide that direct correlation between strategy and resources. For the multilateral organizations, it is much more difficult to ensure that budgets meet objectives. The ESS does not appear to have led to an increased budget or renewed purpose for certain declared actions or missions. NATO appears to have more directly connected budget allocations when new missions are identified, such as missile defense, and the creation of a Center of Excellence on Cyber Security, but national governments decide their resource allocation to a given program.

There was strong consensus that what is absent in the plethora of national and multinational strategic security reviews is a truly transatlantic strategic security and defense review whereby a more structured transatlantic venue is created for discussion of strategic concepts, principles, and priorities. While the NATO Strategic Concept provides a transatlantic collective defense bridge, this document does not adequately capture the transformation of the EU in the external and internal security fields institutionally. Moreover, the 2010 NATO Strategic Concept does not address internal security as a NATO core task although it states that terrorism and the disruption of vital communication are threats to NATO. A Transatlantic White Paper could

address internal security threats and cyber security and become the basis for a joint EU–NATO assessment of global threats, risks, and strategic priorities.

Before a Transatlantic White Paper can be developed, it will be essential for the European Union, in the post-Lisbon Treaty era, to undertake a European White Paper at the request of the European Council and under the leadership of the EU high representative. There would be a very strong "value of the process" in the development of such a European White Paper by building greater consensus and clarity among EU member states on the growing role of the EU in the security and defense arena and encouraging greater synergy between national security strategies and the EU's overarching strategy. Moreover, it would be an excellent bureaucratic "team building" exercise for the European External Action Service (EEAS), bringing together commission, council, and member state professionals in a focused, collaborative effort. It is strongly recommended that the EU Council, like the NATO Strategic Concept and the *Livre Blanc*, establish an expert group or commission that would include current and former European officials (to include select members of the European Parliament) and highly respected business, nongovernmental, and academic officials prior to the official drafting of the European White Paper. It is vital that the process be given an appropriate amount of time (e.g., six months or more) for extended consultations both within Europe and with Europe's strategic partners, like the United States and Russia, and effective outreach to the European think-tank community. Importantly, consultations should continue throughout the drafting process. Finally, although such a European White Paper must, as its first priority, be strategic in outlook and focus on a few strategic priorities to ensure subsequent adequate resource allocation (rather than an exhaustive, least-common-denominator list of issues), security reviews now perform a much greater public diplomacy role. A European White Paper would educate Europeans on the current and future security and threat environment, articulate how the EU will address these threats, and inform other governments of the EU's analysis and policy prescriptions.

ISSUE 2
THE INTERNAL/EXTERNAL SECURITY NEXUS: A COMPARATIVE APPROACH

Research Leader: Swedish Institute of International Affairs (UI)

Europe and North America increasingly face new forms of threats. Whether we speak of global terrorism and regional instability, transcontinental criminal networks, cyber sabotage, or even the effects of climate change and global pandemics, the trend seems evident: modern threats increasingly originate from opaque sources, cross political and sectoral borders with ease, and destabilize the critical infrastructures of our societies. This has caused researchers and politicians on both sides of the Atlantic to reassess the strict separation of external and internal security goals embedded in structures, policies, and practices.

Prioritization of such security threats is now found in the strategic sights of policymakers in both the EU and the United States. For example, the European Security Strategy, as well as the EU's new Internal Security Strategy, argues for the dissolution of that separation, pleading for a more comprehensive security approach. The U.S. Quadrennial Homeland Security Review has cast cross-border threats into the spotlight, calling for an "integrated" approach to combating threats that cross the foreign/domestic divide. Yet each strategy needs to move from rhetoric to reality via implementation and policy change.

This section explores strategic rhetoric and assesses implementation in both the EU and the United States as well as on a transatlantic level. Each contribution takes up a different security issue (cyber security, biosecurity, pandemics, and natural disasters) in order to outline the latest policy developments, analyze gaps and overlaps on either side of the Atlantic, and assess the prospects for improved transatlantic cooperation.

The overall findings of the studies indicate a higher-than-expected degree to which both the EU and United States are following rhetoric with action on the question of cross-border threats. Having professed the importance of bridging the divide between internal and external security threats, each bloc is taking concrete practical steps toward that end. From "whole of government" approaches to international teamwork, both the EU and United States are addressing the internal-external security nexus more rigorously than ever before.

Nevertheless, as the studies make clear, weaknesses remain on both sides of the Atlantic and in the transatlantic relationship. Our findings point to a general need to continue raising awareness on cross-border threats (even as public attention wanes), to pursue common threat assessments across the Atlantic, to identify capacity gaps in both the EU and United States, to engage in joint exercises, and to prioritize efforts to improve cooperation between the EU, United States, and NATO.

The first contribution by Federica Di Camillo and Valérie Miranda (IAI) examines cyber attacks, a growing threat to governments because of the transnational and interconnected nature of critical information infrastructures. Although cyber-related issues have hardly been present in EU strategic rhetoric so far, it is nevertheless possible to identify an increasing awareness of the immediacy of cyber threats as mirrored by the establishment of dedicated agencies and by the commitments

West Point Cadets participate in the 9th annual Cyber Defense Exercise.

©John Pellino/DOIM MMB, http://www.flickr.com/photos/west_point/3594452283/.

outlined in recent documents endorsed by the European Commission. The authors argue that within the wide realm of cyber security, EU policies follow a four-pronged approach encompassing specific network and information security measures, Critical Information Infrastructure Protection (CIIP), the fight against cyber crime, and, on the regulatory side, the framework for electronic communications (including data protection and privacy issues).

In the United States, the authors show that cyber security has emerged as a top national security priority. In contrast to the EU, U.S. strategic documents deal quite extensively with cyber issues, adopting similar definitions and advancing very similar expectations. Recent U.S. efforts in the cyber security domain have particularly been directed at bridging the historically separated cyber defense missions with law enforcement, intelligence, and counter-intelligence. The U.S. government has also taken steps toward enhanced cooperation across its agencies and departments as well as with the private sector—namely, with the defense industrial base and critical infrastructures stakeholders—to better identify cyber threats. The authors conclude by noting that while EU and U.S. approaches to cyber security bear much in common, transatlantic cooperation needs to be improved. Suggested routes include:

- achieving a conceptual and semantic harmonization of cyber issues as a preliminary step to attaining legal harmonization;
- devoting higher priority and attention to cyber security on the transatlantic agenda, not least through the creation of a U.S.-EU Cyber Security Council along the lines of the U.S.-EU Energy Council in the transatlantic summit process;
- fostering transatlantic cooperation at the operational level—namely, setting up joint exercises and exchanges between the related U.S. and EU agencies and encouraging the exchange of best practices between the Computer Emergency Response Teams (CERTs) on both sides of the Atlantic.

The second contribution, by Elisande Nexon and Jean-François Daguzan (FRS), focuses on biosecurity threats. The 2001 anthrax attacks in the United States exposed the threat of biological weapons and revealed vulnerabilities. The authors note that in the EU, strategic rhetoric on biosecurity has increased over the past decade and is taken into account in the EU Strategy against the Proliferation of WMD of 2003 and the adoption of New Lines for Action in 2008, aimed at further improving the implementation of the strategy. The EU has also produced a Green Paper on Bio-Preparedness and, in 2009, an EU Chemical, Biological, Radiological, and Nuclear Action Plan (CBRN). In the United States, which has a number of strategies, directives, and orders that deal with biosecurity, the key strategic document is the National Strategy for Countering Biological Threats, released in 2009, which sets out strategic guidance for federal entities in charge of implementation of biosecurity policies. The United States also has a number of structures explicitly dealing with bio security, including the National Science and Technology Council (NSTC), the

National Science Advisory Board for Biosecurity (NSABB), Center for Disease Control (CDC), and the U.S. National Institutes of Health (NIH).

The authors' analysis reveals that the EU and the United States hold similar threat perceptions and display compatible security apparatuses for biosecurity. Both view biopreparedness as a priority, and an "all-hazards" approach is favored, taking into account the full spectrum of biological risks, from natural outbreaks to accidental contaminations and release and misuse. Nevertheless, the United States and the EU should seek to

- adopt common definitions and terms of reference in order to improve communication and avoid misunderstanding;
- carry out oversight of all CBRN outreach, cooperative initiatives, and activities in order to improve coordination and enhance transatlantic dialogue;
- recognize the importance of engaging industrial and scientific communities in transatlantic initiatives and dialogues.

The third chapter, written by Mark Rhinard and Erik Brattberg (UI), examines whether the EU and United States are turning words into action on the issue of pandemic threats. Following recent pandemic outbreaks, European policymakers have taken steps toward enhancing European cooperation on pandemic preparedness and response, including strengthening surveillance and early alert and early response capacities. Nevertheless, a tension remains in the relationship between national and EU level responses to pandemics. In particular, legally binding measures were viewed with scepticism by some EU member states. In the United States, steps have been taken to enhance preparedness and response, focusing on surveillance, shared standards, decisionmaking structures, and early alert and early response capacities. Although the U.S. government has taken a strategic approach to

Flu and H1N1 vaccinations being given at the Wiesbaden clinic in Germany.

© Carol E. Davis/ USACE Europe District, http://www.flickr.com/photos/europedistrict/4092914530/

pandemic preparation, several shortcomings remain, especially when it comes to vaccine production.

In brief, the findings indicate that EU and U.S. strategic rhetoric on pandemic influenza is fairly consistent and closely aligned. Most EU and U.S. cooperation takes place through the World Health Organization (WHO), where both sides have taken a leading role in new initiatives and seek to encourage cooperation among recalcitrant countries. However, there is little direct U.S.-EU cooperation in the area of common policies or operational capacity sharing beyond an occasional exchange of experts. Key recommendations therefore include the following:

- build relationships between EU health agencies, such as the nascent European Centre for Disease Prevention and Control (ECDC), and U.S. agencies, including the Centers for Disease Control (CDC);
- establish U.S.-EU expert working groups and task forces for tackling specific pandemic threats;
- operate as a constructive transatlantic leadership team within other international

French rescue worker in the rubble of the Hotel Montana, Port-au-Prince, Haiti.

©F.de la Mure/MAEE http://www.flickr.com/photos/francediplomatie/4287643903/.

organizations. This cooperative relationship should be enshrined in regular caucuses of EU and U.S. officials before and during WHO events, for example, and nurtured through partnerships with officials from international organizations.

Finally, Rick "Ozzie" Nelson and Ben Bodurian (CSIS) examine how the EU and United States have approached disaster preparation and response. The authors note that in the last several years an important evolution has occurred in the treatment of natural disasters in EU security policy, with disaster preparation and relief having assumed greater importance in high-level official documents and public declarations. With these changes, EU institutions have looked to take a stronger role in ensuring collective security on the continent. In this context, the Solidarity Clause might serve an important role in fostering unity of effort in the face of a major natural disaster in Europe, requiring assistance from other member states. Like their counterparts in the EU, policymakers in the United States have increasingly highlighted the threat that natural disasters pose to national and global security. High-level strategic documents have moved to frame disaster preparation and response as part an "all-hazards" and "whole-of-government" approach to security. This is an ambitious framework; it requires heightening coordination and cooperation between the myriad constituencies in charge of countering disasters and other threats. Finally, transatlantic cooperation on natural disaster response is discussed both in the context of disasters occurring "at home" in Europe and North America as well as disasters taking place overseas, such as the 2004 Tsunami and the 2010 Haiti earthquake, and how transatlantic cooperation can be strengthened there. Key recommendations include the following:

- strengthen coordination among foreign governments, nongovernmental organizations, and host nation officials;
- increase efforts to identify, in conjunction with the UN, EU, and United States, the capacities, specialties, and limitations of various response stakeholders before disasters strike—this will help minimize redundancies and ensure that no vital needs or requirements go unaddressed;
- integrate local officials into the disaster response effort, especially in cases where disasters occur in developing or poor countries.

Looking across the studies for this research team, common findings emerge that point toward areas for enhanced transatlantic attention in the years ahead. Those findings can be summarized as follows:

- *Agree on shared definitions and concepts.* The EU and United States should work

toward shared definitions of threats and shared methodologies for managing them in a comprehensive way. Shared definitions would alleviate, for example, differing problem definitions (e.g., cyber) and transatlantic miscommunication and misunderstandings (e.g., biosecurity) that currently impair efficient transatlantic cooperation. If possible, shared definitions should lead to common threat assessments for the threats examined by the research team.

- *Build issue-specific cooperative structures.* Historically, the EU and United States have found success when focusing their joint efforts on specific challenges. An EU-U.S. Cyber Security Council would bring necessary priority and attention to that issue, for instance, while improved relations between EU and U.S. disaster management communities would enhance readiness across the Atlantic. Cooperation need not be permanent or wide-ranging; ad hoc cooperative structures (e.g., task forces) have worked well in the area of pandemic control.
- *Increase operational coordination and training.* The research team agreed on the importance of regular exercises to improve operational coordination. This includes training directed toward building capacity in concerned agencies in the EU and United States so that cooperation in times of crisis is more familiar and seamless. This includes training for disaster management preparation, cyber response teams, pandemic control procedures, and biosecurity breach situations. Such training should take place bilaterally, between EU institutions and the United States and between the EU and NATO. A key part of the training should include the sharing of lessons learned and "best practices" from a transatlantic perspective.

ISSUE 3
INDUSTRY TOWARD SECURITY

Research Leader: Istituto Affari Internazionali (IAI)

The wave of terrorist attacks that started in September 2001 provoked a rethinking of the concepts of internal and external security. The two policy areas, often separated in the past, are increasingly seen as overlapping. This change has far-reaching implications for the security and defense industrial bases: both are restructuring to better respond to the security challenges in Western societies. The security industrial base and market, in particular, will be subject to the more dramatic rebuilding, as its structure is far less developed than that of the defense market. Both the EU and the United States are working to make the security market more mature and efficient, with different approaches and mixed success. However, the transatlantic community needs a thriving security industrial base if it wants to successfully overcome the challenges it faces.

This is the scenario that the IAI-led research team developed in order to provide as complete a picture as possible of the evolution of the security industry and market, identify the main obstacles to its development on both sides of the Atlantic, and provide ideas and recommendations to overcome these obstacles. The research team focused on different aspects of the market's evolution to ensure a comprehensive assessment. An introductory paper describes the security sector, and three additional contributions deal, respectively, with public-private partnerships in the sector, the regulatory environment, and the development of industrial policies in the security sector.

The first paper, *The Security Market in the EU and the U.S.*, produced by Hélène Masson and Lucia Marta (FRS), provides a complete picture of the current security market both from the demand and supply sides, based on the most recently available data. The authors provide an in-depth analysis of the main industrial actors and of the main procurement agencies, devoting particular attention to the transatlantic dimension of the market. The analysis describes a very fragmented market in terms of both customer base and industry on both sides of the Atlantic. The paper also underscores the uncertainty regarding the actual size of the market, which hampers efforts toward market restructuring.

The second paper, *Challenges to Agenda-Setting Priorities: Toward Effective Public-Private Partnerships for Security in the EU and United States,* by Jan Joel Andersson and Erik Brattberg (UI), focuses on the relationship between governments and the security industry. Their research attempts to evaluate whether this relationship is sufficiently structured to allow a fruitful exchange of ideas between the two stakeholders. The paper, in fact, posits the assumption that transparent and fruitful communications between demand and supply are essential if the industrial base is to provide governments with needed capabilities. Customer-supplier relations in the defense field are used as a point of comparison. After reviewing the emerging security industry-government relationship, the authors conclude that the diversity of buyer profiles and consequent lack of predictability of the security demand represent a significant challenge for the industry, which should itself be more involved in agenda-

Port of Seattle.

©flickr user redyamflan, http://www.flickr.com/photos/10216416@N00/3535683153/.

setting activities as well as in the formulation of requirements.

The third paper, *The Regulatory and Acquisition Environment for Security in the EU and United States,* by David Berteau, Guy Ben-Ari, and Priscilla Hermann (CSIS) and Sandra Mezzadri (IAI), provides an assessment of the regulatory environments for the security industry in the United States and the EU. Government regulations have a direct impact on the industrial base and its ability to develop and field security-related capabilities. The paper identifies various regulatory shortcomings on both sides of the Atlantic: insufficient acquisition oversight and cost estimation capabilities as well as overreliance on external contractors in the United States; and an inadequate level of standardization and liability protection as well as poor transparency on public procurement practices and procedures in the EU. The paper also highlights some regulatory weaknesses common to both the EU and the United States; these include unclear definitions of security versus defense goods, bureaucratic barriers to entry, and an insufficient public-private dialogue. The paper advocates for collaborative EU-U.S. efforts to develop common solutions in these areas.

Finally the fourth paper, *Transatlantic Industrial Policies in the Security Sector*, by Valerio Briani and Nicolò Sartori (IAI), outlines how the U.S. government and EU institutions approach the development of a more mature security market. The paper begins by analyzing the distinct characteristics of the defense and security markets—as in the UI paper, the defense sector is considered the point of reference. The document then outlines how the United States and the EU are developing their respective markets by adopting two very different approaches. While the EU is slowly but surely developing a security industrial policy as a part of the more encompassing European industrial policy, the U.S. government favors a more institution-centered approach, largely recoiling from intervening in the sector. However, in both cases the chosen approach has resulted in a security sector that is more closely modeled in structure to the defense sector.

Each of the above-mentioned contributions includes a number of policy suggestions and ideas on how to improve the governance of the security sector and the efficiency of the industrial base. Most of the policy recommendations are applicable both to the United States and the EU and can be summarized as follows:

- *Improve industry's engagement in the governance of the security sector*. Enhance communication so that the security industry is more conscious of the capability requirements, more efficient thanks to predictable and stable demand, and more responsive to the market.
- *Enhance the regulatory environment*. Business leaders need a sound regulatory environment, with clear and simple regulations, in order to be able to make the right investments. Industry would also benefit from less fragmented demand, which can also be reached through proper regulatory action.
- *Avoid competitive and/or protectionist practices*. European and American security needs are similar. Both can benefit from a more open and competitive transatlantic security market. Any attempt to introduce protectionist elements (such as prohibitive export regulations or "buy domestic" acquisition practices) will be counterproductive.

Security screening at Denver airport, March 23, 2009.

©flickr user Inha Leex Hale, http://www.flickr.com/photos/sixmilliondollardan/3382932556/.

ISSUE 4
THE TRANSATLANTIC RELATIONSHIP AND EU-U.S. SECURITY COOPERATION

Research Leader: Fondation pour la Recherche Stratégique (FRS)

The disappearance of the existential threat that led to the establishment of NATO and spurred the development of the EU has meant that political consensus between the two sides of the Atlantic can no longer be guaranteed when confronting new international challenges. The evolving global security environment requires better organization within the EU and increased European investment in strategic civil and military capacities as well as a stronger EU-U.S. relationship. Such a pragmatic approach to the transatlantic relationship would have a profound effect on Europe's profile in the world and the EU's ability to make a positive contribution to the maintenance of international stability alongside the United States.

To better analyze the emerging security dynamics, the FRS-led research team undertook four detailed case studies that examined transatlantic cooperation with respect to complex security problems of widely differing character and magnitude. The cases assessed contributions by the European Union and its member states and the United States to international efforts to stabilize and develop Afghanistan since 2001, dissuade Iran from acquiring nuclear weapons over the past five years, provide humanitarian relief to Haiti in the aftermath of the devastating January 2010 earthquake, and combat piracy off the coast of Somalia since 2008. Each case examines the stakes, interests, and levels of commitment of EU members and the United States and assesses the degree of convergence of these commitments. Moreover, the four cases considered key variables, proposed plausible scenarios of evolution, and outlined several implications for the transatlantic partnership.

In his analysis *The Nuclear Standoff with Iran and the Future of Transatlantic Security Responsibility-Sharing*, Riccardo Alcaro (IAI) suggests that transatlantic divergence does matter: "The initial fractiousness of the transatlantic front made it easier for Iran to advance its nuclear expertise." The second lesson he draws is that "even when the United States and the European Union are able to agree upon a common line, this is of little help if their strategic objectives remain distant." Moreover, the "EU/European political and economic assets represent a critical, if not fundamental, crisis management resource, in particular when the United States is short of options." And finally, there are real limits to transatlantic security cooperation in the sense that "several EU member states are unlikely to buy the argument that the failure of the European years-long effort to persuade Iran to come clean on its nuclear ambitions has rendered an attack unavoidable . . . . So, an attack against Iran is likely to undo, or at least jeopardise, whatever benefit may have accrued to the transatlantic partnership from the E3/EU+3 process."

In their analysis *Afghanistan: A Stress Test for Transatlantic Security Cooperation,* Stephen Flanagan, T.J. Cipoletti, and Amanda Tuninetti (CSIS) develop the idea that the "Afghan engagement has highlighted the limits of the EU as an actor in semi-permissive environments and exposed its lack of doctrine and capacity in security sector reform." The authors argue that "at the same time, NATO has consistently

German and American forces near Camp Marmal, Mazir e Sharif Airfield, Afghanistan.

©ISAFmedia, http://www.flickr.com/photos/isafmedia/5125441010/.

underperformed in this field as well, and the lack of civilian capacity in NATO is well known." Still they note that "there is growing U.S.-European convergence in political engagement with the Afghan government and civilian assistance efforts, but shortcomings in the integration of military and civilian stabilization and reconstruction efforts persist." They conclude that "while NATO-EU cooperation in Afghanistan has not provided a template for future engagements, it has proved valuable in advancing the transformation of European armed forces." In a sense, Afghanistan "has highlighted a number of difficulties in transatlantic security cooperation in dealing with emerging global challenges. Differences in conceptual understanding of the conflict and the nature of engagement have led to asymmetrical and incompatible human and financial contributions, threatening not only the goal of stabilizing Afghanistan, but also the future of EU-U.S. security cooperation. Without agreement on goals and strategy, future transatlantic missions will likely encounter some of the same challenges that have hampered the engagement in Afghanistan." Therefore, the authors make several recommendations:

- The EU countries should expand their commitment to training the Afghan national security forces, particularly the police, and supporting the development of the rule of law, in order to ensure the success of the transition plan agreed to at the Lisbon ISAF-Afghanistan Summit.
- Funding and staffing for the EU's crisis response capabilities, including the Civilian Planning and Conduct Capability, should be augmented and better integrated with the development of NATO's comprehensive approach and new civilian planning capability.
- An EU-NATO security agreement should be concluded to allow for easy exchange of classified information and overcome other operational limitations that are diminishing the security and effectiveness of EU personnel in the field and the success of combined EU-NATO missions.

In the case study *EU-U.S. Response to the Haiti Earthquake: A Comparative Analysis*, Erik Brattberg and Bengt Sundelius (UI) argue that policies to prevent and manage a complex humanitarian crisis require taking into account the objectives of state security, societal security, and human safety at the domestic and international levels and at the "intermestic" level as societies become increasingly inte-

Member of European Union Assessment Team Arrives in Petit-Goâve, Haiti, January 2010.

©UN Photo/Logan Abassi. http://www.flickr.com/photos/un_photo/4293300049/.

grated. For these types of humanitarian crises, the authors offer these recommendations:

- The EU and the United States should "consider developing more pre-established agreements built around a 'lead partner' criteria for different parts of the world."
- "The continental Operation Centers in Washington and in Brussels" should be linked "through regular exchanges of situation awareness reports and through interactive training workshops and joint training exercises."
- The United States and the EU Commission should establish "protocols directly rather than with individual EU member states to signal U.S. support for EU-wide coordination."
- "The strategic dialogue between the U.S. Agency for International Development (USAID) and the Director General for the European Commission's Office of Humanitarian Aid and Civil Protection (DG ECHO) should be expanded to include other relevant institutions for emergency relief and preparedness."

Finally, in *The Fight against Piracy off Somalia: A Consensual but Asymmetric Engagement,* Philippe Gros (FRS) argues that "the transatlantic partnership is necessary for the present fight against piracy off Somalia, not only for naval anti-piracy operations, but also for the broader comprehensive approach to tackle such problems." But it is an asymmetric partnership as the "EU as an institution clearly co-leads the effort and, in relative terms, its members commit more resources than the U.S." Indeed, the United States does not consider piracy as a critical security threat. Beyond the defense of direct economic interests, Europe's level of commitment in this area is due to the type of engagement, "primarily a law enforcement operation with a very limited use of force, undertaken under the umbrella of the consensus of nearly the entire international community." Therefore, the anti-piracy mission "fits perfectly with the enduring common denominator between strategic cultures of EU partners," may not represent a new durable step of the EU's Common Security and Defense Policy (CSDP), and does not require a rebalancing of the transatlantic security agenda. However, the relative stalemate of the current "comprehensive" strategy, which combines naval containment and engagement with Somalia's weak Transitional Federal Government (TFG)—although satisfying for many—may lead over time to other options that would stress this asymmetric but consensual partnership.

Hopelessly surrounded and outgunned, Somalian pirates surrender to HMS Cumberland's Royal Marines boarding team in the Gulf of Aden, February 2009.

©MoD /UK Ministry of Defence, http://www.flickr.com/photos/defenceimages/5036079383/.

Both the Iran and Afghanistan cases illustrate the importance of shared strategic assessments and agreement on goals in dealing with various security challenges. It may not always be possible to reach common assessments and develop common goals, but the differences that have at times limited transatlantic cooperation can be narrowed by undertaking more common EU-U.S. strategic assessments and consultations between NATO's North Atlantic Council (NAC) and the EU's Political and Security Committee (PSC) on emerging security challenges. It should also be recognized that, when agreement on goals cannot be reached, Europe and the United States should refrain from public recrimination that would otherwise undermine its cohesion. It is imperative that transatlantic policymakers devote more energy to better understanding and limiting negative effects from a lack of transatlantic convergence.

The Somali piracy, Afghan, and Haiti cases all highlight the need for better integration of civil and military capabilities to address complex security and humanitarian contingencies. As NATO moves forward with the development of its "comprehensive approach," it is recommended that a parallel EU-U.S. effort be undertaken to take stock of how civilian crisis response and management capabilities can be better integrated.

In summary, when the four research areas are examined together, it is clear that the partnership between the EU and the United States is absolutely essential in addressing the challenges of a complex, multipolar security environment. Therefore, it is equally essential that the EU-U.S. partnership receive the necessary political priority and attention that a relationship of this magnitude deserves.

LIST OF ACRONYMS

ABSA	American Biological Safety Association
ACT	Allied Command Transformation
AIS	Automatic Identification Systems
ALF	Acquisition Life Cycles Framework
AMISOM	African Union Mission in Somalia
ANA	Afghan National Army
ANCOP	Afghan National Civil Order Police
ANP	Afghan National Police
ARB	Acquisition Review Board
ARP	Acquisition Review Process
ASD	Aerospace and Defence Industries Association
ATS	Automated Targeting System
BEAR	Biometric Enhancement for Airport-Risk Reduction
BEP	Biosecurity Engagement Program
BMD	Borders and Maritime Division Focus Areas
BMLB	Biosafety in Microbiological and Biomedical Laboratories
BS&S/TADR	Biosecurity and Biosafety/Biological Weapons Threat Agent Detection
BSIA	British Security Industry Association
BSL	Biosafety-Level
BTWC	Biological and Toxins Weapons Convention
CAGR	Compound annual growth rate
CBD	Chemical and Biological Division Focus Areas
CBO	Congressional Budget Office
CBRN	Chemical, Biological, Radiological, Nuclear

CC-Mar	Allied Maritime Component Command
CDC	U.S. Centers for Disease Control
CERTs	Computer Emergency Response Teams
CFSP	Common Foreign and Security Policy
CGPCS	Contact Group on Piracy off the Coast of Somalia
CID	Command, Control, and Interoperability Focus Areas
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructure Protection
CIKR	Critical Infrastructure and Key Resources
CMF	Combined Maritime Force
CNCI	Comprehensive National Cyber security Initiative
COIN	Counterinsurgency
C-PAT	Customs-Trade Partnership Against Terrorism
CPM	Civil Protection Mechanism
CPR	Cyberspace Policy Review
CRS	Congressional Research Service
CSC	Coordination Support Committee
CSDP	Common Security and Defence Policy
CSI	Container Security Initiative
CSIS	Center for Strategic and International Studies
CTF	Combined Task Force
CWA	CEN Workshop Agreement
DARPA	Defense Advanced Research Projects Agency
DCI	Development Cooperation Instrument
DDoS	Distributed Denial of Service
DFARS	Department of Defense has the Defense Federal Acquisition Regulation Supplement
DG	Directorate General
DG Sanco	Directorate General for Health and Consumers
DHS	Department of Homeland Security
DIYbio	Do it yourself bio
DNDO	Domestic Nuclear Detection Office
DoD	Department of Defense
DRC	Democratic Republic of Congo
DSTs	District Support Teams
EADRCC	Euro-Atlantic Disaster Response Coordination Centre
EADRCC	Euro-Atlantic Disaster Response Coordination Centre
EADRCC	Euro-Atlantic Disaster Response Coordination Centre

EADRU	Euro-Atlantic Disaster Response Unit
EADRU	Euro-Atlantic Disaster Response Unit
EAPC	Euro-Atlantic Partnership Council
EAPC	Euro-Atlantic Partnership Council
EC	European Commission
ECCP	European Cyber Crime Platform
ECDC	European Centre for Disease Prevention and Control
ECHO	European Union Humanitarian Aid and Civil Protection Office
ECI	European Critical Infrastructures
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EDTIB	European Defence, Technological and Industrial Base
EEAS	European External Action Service
EECTF	European Electronic Crime Task Force
EFSA	European Food Safety Agency
EMEA	European Medical Evaluations Agency
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ESDP	European Security and Defence Policy
ESRAB	European Security Research Advisory Board
ESRIA	European Security Research and Innovation Agenda
ESRIF	European Security Research and Innovation Forum
ESS	European Security Strategy
ESTA	Electronic System for Travel Authorization
EU	European Union
EU ISS	European Union Institute for Security Studies
EUCO	EU Haiti coordination cell
EUMARFOR	EU Maritime Force
EU-NAVFOR	European naval force
EUROGENDFOR	European Gendarmerie Force
EUROJUST	EU Judicial Cooperation Unit
EUROPOL	European Police Office
EUTM	EU Training Mission
EWRS	Early Warning and Response System
EXD	Explosives Division Focus Areas
FAR	Federal Acquisition Regulation
FDA	Federal Drug Administration
FEMA	Federal Emergency Management Agency

FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FRS	Fondation pour la Recherche Strategique
FY	Fiscal Year
GAO	Government Accountability Office
GDP	Gross Domestic Product
GHSI	Global Health Security Initiative
GMP	*Global Maritime Partnership*
GoA	Gulf of Aden
GoP	Group of Personalities
HEOF	Health Emergency Operations Facility
HFD	Human Factors Division Focus Areas
HHS	Health and Human Services
HSAM	Homeland Security Acquisition Manual
HSAR	Homeland Security Acquisition Regulation
HSARPA	Homeland Security Advanced Research Projects Agency
HSC	Health Security Committee (
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
IAEA	International Atomic Energy Agency
IAI	Istituto Affari Internazionali
ICAO	International Civil Aviation Organization
ICROS	Internet Crime Reporting Online System
ICT	Information and Communication Technologies
IED	Improvised Explosive Devises
IfS	Instrument for Stability
IGD	Infrastructure and Geophysical Division Focus Areas
INS	Immigration and Naturalization Service
IPAPI	International Partnership on Avian and Pandemic Influenza
IRTC	Internationally Recommended Transit Corridor
ISA	Iran Sanctions Act
ISAF	International Security Assistance Force
ISI	Inter Services Intelligence
ISPS Code	International Ship and Port Facility Security Code

ISS	Internal Security Strategy
JCF -Lisbon	Allied Joint Force Command Lisbon
LoI	Letter of Intent
LRTI	Long-range identification and tracking
LWR	Light Water Reactor
MEPs	Members of the European Parliament
MIC	Monitoring and Information Centre
MINUSTAH	United Nations Stabilization Mission in Haiti
MoD	Ministry of Defence
MS	Member State
MSAM	Major Systems Acquisition Manual
MSCHOA	Maritime Security Center Horn of Africa
MSTA	Maritime Port Security Transportation
NAC	North Atlantic Council
NADR	Non-proliferation, Anti-terrorism, Demining, and Related Programs
NATO	North Atlantic Treaty Organisation
NCSD	National Cyber Security Division
NIH	National Institutes of Health
NIMS	National Incident Management System
NIS	Network and Information Security
NPT	Nuclear Non-Proliferation Treaty
NRF	National Response Framework
NRP	National Response Plan
NSABB	National Science Advisory Board for Biosecurity
NSHQ	NATO Special Operations Headquarters
NSHS	National Strategy for Homeland Security
NSS	National Security Strategy
NSTC	National Science and Technology Council
NTM-A	NATO Training Mission Afghanistan
OBA	Office of Biotechnology Activities
OCCAR	Organisation Conjointe de Coopération en matière d'Armement
OCHA	Office for the Coordination of Humanitarian Affairs
OEF	Operation Enduring Freedom
OFDA	Office of U.S. Foreign Disaster Assistance

OHQ	Operational Headquarters
OMA	Office of Military Affairs
OMLTs	Operational Mentoring and Liaison Teams
PASR	Preparatory Action for Security Research
PHS	Public Health Service
POMLTs	Police Operational Mentor and Liaison Teams
PPP	Public-Private Partnerships
PRR	Preparedness, Response, and Recovery
PRTs	Provincial Reconstruction Teams
PUCs	Persons Under Control
QDDR	Quadrennial Diplomacy and Development Review
QDR	Quadrennial Defense Review
QHSR	Quadrennial Homeland Security Review
R&D	Research & Development
R&T	Research and Technology
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RFID	Radio Frequency IDentification
RMT	Response Management Team
S&T	Science and Technology
S/CRS	Office of the Coordinator for Reconstruction and Stabilization
SAEFTY	Support Anti-terrorism by Fostering Effective Technologies
SAFE	Security and Accountability for Every
SAP	Select Agent Program
SAR	Select Agent Regulations
SAR	Search and Rescue
SARS	Severe Acute Respiratory Syndrome
SC	Strategic Concept
SDSR	Strategic Defence and Security Review
SHADE	*Shared Awareness and Deconfliction*
SIA	Security Industry Association
SIS II	Second generation Schengen Information System
Sit Cen	Joint Situation Centre
SME	Small and Medium Enterprises
SNMG	Standing NATO Maritime Groups

SOUTHCOM	U.S. Southern Command
SSN	Submarine Nuclear-Powered
SUA	Suppression of Unlawful Acts
TCA	Trade and Cooperation Agreement
TFEU	Treaty on the Functioning of the European Union
TFG	Transitional Federal Government
TSA	Transportation Security Administration
U.S.-VISIT	United States Visitor and Immigrant Status Indicator Technology Program
UI	Swedish Institute for International Affairs
UIC	Union of Islamic Courts
UKMTO	UK Maritime Trade Operations
UN	United Nations
UNCLOS	United Nations Convention on the Law Of the Sea
UNDP	United Nations Development Programme
UNODC	UN Office on Drugs and Crimes
UNSCR	United Nations Security Council Resolution
USAID	U.S. Agency for International Development
USAMRIID	U.S. Army Medical Research Institute for Infectious Diseases
VIS	Visa Information System
VP	Vice-President
WEU	Western European Union
WHO	World Health Organisation
WMD	Weapons of Mass Destruction
WTO	World Trade Organisation

ISSUE 1

THE DEFINITION OF EXTERNAL SECURITY AND ITS IMPLEMENTATION MODEL

INTRODUCTION

Heather A. Conley, *Senior Fellow and Director of the Europe Program, CSIS*

The process by which national governments and multinational organizations undertake strategic reviews, assess their external or national security and develop strategic rationales, goals and objectives profoundly influences the review's ultimate assessment of the threat environment and its policy impact. The United States and Europe possess fundamentally and historically different review processes, purposes, strategic communities and cultures, and therefore the strategic reviews that are produced are quite diverse. However, greater transatlantic alignment of both strategic assessment and review processes can produce improved cooperative models and operational synergies.

This chapter examines how Europe and the United States define external security and how each conduct strategic security reviews. The paper is divided into two sections: the first section provides analysis of two national (French and American) strategic reviews and the second section assesses two multinational (the European Union and NATO) strategic security reviews. To overcome the challenges of analyzing four very different strategic reviews, the authors analyzed their respective strategic reviews to determine: (1) the situational and historical context in which the review occurred, (2) the process, purpose and value of the review, (3) the content, terminology and conceptual framework of each review and (4) the impact and net effect of the review. From this analysis, several emerging trends and common themes were identified as were common challenges to the articulation and implementation of each security review.

In the first section, Camille Grand, Director of the Paris-based *Fondation pour la Recherche Stratégique (FRS),* describes the 2008 French White Paper on Defense and National Security (*Livre blanc sur la défense et la sécurité nationale*) as an historic review which last occurred in France in 1994. Similarly, the 2008 French assessment was commissioned by a newly elected president; it combined the concepts of both defense and national security for the first time; and, an external commission was tasked to draft the *Livre Blanc*, utilizing the assessment as both an opportunity to redefine French strategy (which led to French military re-integration with NATO) and as a public diplomacy tool. In his list of recommendations, Mr. Grand makes a persuasive argument for instituting external commissions which combine experts and senior government officials and allowing for an extended consultative process to ensure strong buy-in from policymakers, the public and allies. He further suggests that the European Union should initiate a similar White Paper process, which could be the launching point for a Euro-Atlantic White Paper.

Heather Conley, Senior Fellow and Director of the Europe Program, and Manuel Lafont-Rapnouil, Visiting Fellow, of the Center for Strategic and International Studies (CSIS) in Washington, D.C. examine the 2002 and 2010 U.S. National Security Strategies (NSS) and describe the complex nature of American strategic security reviews. There are striking differences and similarities between the two U.S. National Security Strategies initiated by two American administrations with dissimilar tactical approaches to national security policy yet confront a similar and daunting threat environment. The authors examined the internal consistency of the two strategies, the strategic durability of the threat assessments, significant organizational restructuring, and its budgetary impact. In their conclusion, they argue that, as the United States continues to fully integrate the concept of homeland and national security and minimize the distinction between domestic and foreign affairs, there is a growing commonality between Europe and the United States both in assessing the international security environment as one of growing complexity and calling for greater international cooperation and partnerships. The authors call for greater international consultation by U.S. officials before, during and following the drafting of U.S. National Security Strategy to maximize collaboration and gain a better common understanding of strategic terminology, the current threat assessment, and best implementation practices.

In the second section, Mark Rhinard, Senior Research Fellow and Erik Brattberg, Research Assistant of Swedish Institute of International Affairs (UI) in Stockholm, assess the first overarching strategic framework to guide European security policymakers in 2003 and its 2008 "review." The 2003 European Security Strategy (ESS) and its subsequent review in 2008 were deemed necessary due to the EU's ongoing institutional and organizational development, the launch of the EU's first military operation outside of Europe and in reaction to the U.S. invasion of Iraq. The process surrounding the ESS was insular and controlled by a very small number of senior EU officials, although select European think-tanks were later engaged in a consultative process. The final document was relatively brief (fifteen pages) yet lacked strategic prioritization and was not tethered to budgetary resources in any meaningful way. From this experience, the authors urge the full utilization of think-tanks in both Europe and the United States when strategic reviews are initiated and recommend creating a 'transatlantic white paper' to identify critical transatlantic issues that can be integrated into respective national and multinational strategies.

Finally, authors Stefano Silvestri, President, and Alessandro Marrone, Researcher, of the Istituto Affari Internazionali (IAI) in Rome, analyze the 2010 NATO Strategic Concept. Because the international security environment has grown more complex, they argue that it has become increasingly difficult to forge a solid transatlantic consensus on NATO's future role which has led its strategic review process to become a political exercise that redefines core tasks and develops key partnerships, particularly with Russia, in contrast to its previous military activity. The authors emphasize the growing importance of the role of public diplomacy and cite NATO's use of external officials and extensive consultations as an example of NATO's growing effectiveness in this arena. The authors conclude by strongly recommending greater EU-NATO strategic cooperation by initially undertaking a common strategic review of theatre operations that both organizations conduct with the eventual implementation of a joint EU-NATO assessment of threats, risks and strategic priorities.

THE FRENCH CASE: LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE

Camille Grand, *Director, FRS*

Introduction

Before delving into the 2008 *White Paper on Defense and National Security*, it is important to underline that France does not have an outstanding track record in producing formal strategy papers, which have not been part of French military tradition or strategic culture. When tracing the roots and turning points of French security policy and strategy, officials and commentators alike tend to refer more to speeches delivered by the President or other senior political figures (Prime minister, defense minister, etc). Moreover, there are no mandatory processes to produce any such document, and the executive branch is under no obligation to produce regular reports or reviews for parliamentary purposes. The only thing which comes close to such a mandatory process is the five-year procurement bill which usually contains an opening chapter dealing with the strategic environment.

As an example, nuclear policy has been primarily defined and explained through a series of major "nuclear" speeches by the seven presidents of the Fifth Republic (since 1958) which often preceded formal strategy documents or White papers: De Gaulle in 1959, Mitterrand in 1983 and 1994, Chirac in 1996 and 2001 (Ile Longue), and Sarkozy in 2008 (Cherbourg) delivered such speeches. This applies as well to other fields of national security strategy. President Sarkozy rolled out his decision to re-integrate French forces in NATO's military structures in a speech at a public event hosted by the *Fondation pour la Recherche Stratégique* in March 2009. However, these speeches should not be interpreted as a process which ignores inter-agency debates or as a by-product of the French presidential regime restricting parliamentary action when it comes to foreign and security policy: far from it. These speeches are carefully drafted and often reflect fairly accurately the end-product of long decision making processes.

Having pointed at some French distinctiveness, it is however fair to admit that France has nevertheless is entering a period of normalization by preparing White Papers on a more regular pace and adopting more open processes. In the last few years, there was a *White paper on internal security and terrorism* in 2006, a *White paper on foreign policy* in 2008 and the 2008 *White paper on defense and national security*. It can't therefore be excluded that in the future such documents will be adopted on a more regular basis.

Historical Context

Since the early days of the Fifth Republic, France has only adopted three defense white papers, on average one every seventeen years! The first one was commissioned and released in 1972 by President Pompidou. The second one only came 22 years after, in 1994; it was prepared and released in a strange period, during a "cohabitation" between a socialist president (Francois Mitterrand) and a conservative parliamentary majority and government led by a Gaullist Prime minister (Edouard Balladur). The most recent one was decided by President Sarkozy after his 2007 election and released in 2008. Since there are no legal obligations to produce such reviews, the White papers are always very significant events and are always decided at the highest political level with specific policy and political objectives, although policy decisions might be taken after the release of the paper itself.

The most significant historical evolution is the visible name change which reflects a set of broader strategic issues: the 1972 White Paper was a *Livre blanc sur la défense nationale* (National defense white paper), the 1994 paper was a *Livre blanc sur la défense* (Defense White Paper) and the 2008 was a *Livre blanc sur la défense et la sécurité nationale* (National security and defense white paper) incorporating national security and defense.

The 1972 *Livre blanc* was very much focused on defense policy and nuclear deterrence, and served a sole purpose: to formalize the Gaullist legacy after de Gaulle had resigned (1969) and died (1970) as if after his death it had become important to put in writing the core principles of the Gaullist defense policy legacy after France had become a nuclear weapon state.

After the end of the division of Europe during the Cold War, in 1994 France undertook a reassessment of its strategy and force structure which prepared the 1996 decisions to:

1. transition to all-professional armed forces,
2. reduce nuclear forces and,
3. build up a substantial force projection capability, in keeping with the new strategic situation.

Interestingly, the 1994 *Livre blanc* did not address these decisions as political disagreement remained in the cohabitation era as the socialist President Mitterrand opposed two of the three major policy choices (professionalization of the armed forces and resumption of nuclear testing to finalize the post-cold war modernization of nuclear forces).

The 2008 White Paper also came into being during a specific political era -- the post-Chirac period. After a 12-year long presidency, President Sarkozy wanted to provoke changes at all levels of government including in the national security sector. The *Livre blanc* was a tool to drive change and build a new national consensus around defense and security. Unfortunately consensus was not reached as socialist parliamentarians left the expert Commission to protest that some decisions with regard to nuclear policy and Afghanistan had already been taken by the government before the White Paper was released. This move nevertheless should not be interpreted as an overall disagreement as it was motivated by domestic political constraints. In the end, the 2008 White Paper represented a fairly wide mainstream consensus among French elites and decision-makers that went beyond political lines.

The Process and Purpose of the 2008 French Livre Blanc sur la défense et la sécurité nationale

In August 2007, the newly elected French President, Nicolas Sarkozy, set up a Commission entrusted with the crafting of a White Paper on Defense and National Security. Chaired by Jean-Claude Mallet (former *Secrétaire général de la défense nationale*, i.e., top national security adviser to the Prime minister), the Commission was given a broad mandate and few limitations to fulfill its task, without many taboos. The composition of the Commission reflected this innovative approach: in addition to the representatives of the relevant government agencies and of the armed forces, parliamentarians and qualified individuals from academia and strategic think-tanks were actively involved in the work of the Commission along with independent experts and personalities with an industrial background. In a break with past practice, the Commission proceeded with far-ranging publicly televised and on-line hearings of some 52 personalities from 14 countries and 5 continents. Numerous closed-door consultations were also held. Members of the Commission proceeded with more than twenty visits in the field in defense and national security units and facilities, in France and abroad on the various theatres of operations where French forces are engaged. The Commission's website received more than 250,000 individual visits, bearing witness of the public interest in defense and security affairs; the corresponding on-line forum provided the Commission with useful input. Exchanges with trusted foreign partner-states and with the European Union and NATO were part of this unprecedented comprehensive process.

New Strategic and Conceptual Thinking

At the outcome of this process, the White Paper substantially redefined French strategy in a 15-year perspective, embracing both defense and national security. It included foreign security and domestic security, military and civilian means, tools and approaches and responded to risks emanating from either States or non-State actors. The White Paper dealt with active, deliberate threats but also with the security implications of major disasters and catastrophes of a non-intentional nature.

The definition of a comprehensive security strategy is a consequence of the challenges of our times, faced by France together with its allies and partners, and the fundamental changes of the age of globalization as reflected in an in-depth, wide-ranging strategic adaptation. Some key findings can be extracted from the 2008 *Livre Blanc*:

1. The world has changed profoundly since the publication of the previous White Paper in 1994, in particular due to the impact of globalization. The formidable acceleration of information exchanges, the increased trade in goods and services as well as the rapid movement of people, have transformed our economic, social and political environment in both positive and negative ways, as well as the paradigms of national and international security. The hierarchy of powers has changed and will continue to evolve. The world is not necessarily more dangerous, but it has become more unstable, more unforeseeable. New crises, in particular from the Middle East to Pakistan have come to the fore and have become more inter-connected. Jihadism-inspired terrorism aimed directly at France and Europe places France in a situation of greater direct vulnerability. In this context, the White Paper attempted to capture the strategic threat

assessment for the next fifteen years to come, and to understand the consequences as part of a comprehensive new defense and security policy.

2. One major innovation was that security interests are assessed globally without restricting the analysis to defense issues. A national security strategy is defined in order to provide responses to "*all the risks and threats which could endanger the life of the Nation*." The scope of national security includes defense policy, but is not limited to it. In order to better ensure the defense of French interests and the mission of protecting its population, the national security strategy calls upon interior security policy, for anything which is not directly related to individual security of persons and property or law and order, as well as the civil security policy. Other policies such as foreign policy and economic policy also contribute directly to national security.

3. The national security strategy includes five strategic functions for the defense and security forces: knowledge and anticipation, prevention, deterrence, protection and intervention. The combination of these five functions must be flexible and evolve over time, adapting to the changes in the strategic environment. One major change is that the White Paper will henceforth be updated before the discussion of each new Military Program and Interior Security Bills.

4. Intelligence, knowledge and anticipation represent a new strategic function and have become a priority. In a world characterized by uncertainty and instability, knowledge represents the first line of defense. Knowledge guarantees autonomy in decision-making and enables France to preserve its strategic initiative. It is knowledge which must be provided as early on as possible to decision-makers, military commanders and those in charge of internal and civil security in order to go from prediction to informed action. Intelligence of all kinds, including from space and prospective studies, takes on major importance.

5. Protection of both the population and territory is at the very heart of France's strategy as the country is directly exposed to new vulnerabilities. The goal is to protect the nation in times of major crisis while increasing its resilience defined as the "*capability of public authorities and the French society to respond to a major crisis and rapidly restore normal functioning*." Reinforcing resilience requires a change in the means and methods of surveillance used over the national territory including land, sea, air and now space and to develop a more rapid and wider in scope, response capability for French public authorities. Communication, information systems and civil warning systems lie at the centre of the crisis management and preparedness system. One new element is the coordination between civilian and military departments and agencies as a fundamental principle of the new strategy where operational goals to protect the population and nation are assigned jointly to both internal security services, civil security services and the armed forces.

6. As regards conflict prevention and intervention capabilities, the White Paper prioritizes the geographic axis stretching from the Atlantic Ocean, the Mediterranean Sea, the Arab-Persian Gulf to the Indian Ocean. This axis corresponds to the areas where the risks related to the strategic interests of France and Europe are the highest. The White Paper also takes into account the growing importance of Asia for national security and support presence and cooperation throughout this axis. In parallel, France will preserve its prevention and action capabilities on the Western and Eastern sea-boards of the African continent as well as in the Sahel, in particular to

fight against human and contraband trafficking and acts of terrorism. The White Paper also announced radical changes with regards to the existing system of French defense and military cooperation agreements to strengthen the partnership between Europe and Africa, focusing on the developing defense and security cooperation and peace-keeping capabilities in Africa. The White Paper also set forth a series of guidelines for the intervention of French armed forces in foreign theatres.

7. Nuclear deterrence remains an essential concept of national security. It is the ultimate guarantee of the security and independence of France. The sole purpose of the nuclear deterrent is to prevent any State-originated aggression against the vital interests of the nation, wherever it may come from and in whatever shape or form. Given the diversity of situations with which France might be confronted in an age of globalization, the credibility of the deterrent is based on the ability to provide the President with an autonomous and sufficiently wide and diversified range of assets and options. Even though there may not be any direct threat of aggression today against France, it is imperative to retain the capability to preserve the freedom of action of our nation if our vital interests are threatened with nuclear blackmail. France will have the means to develop its capability as long as nuclear weapons are necessary for its security. However, France has taken the initiative in the area of nuclear disarmament and shall continue to do so. France is particularly active in the fight against the proliferation of chemical, biological and nuclear weapons as well as of the missiles capable of delivering WMD.

8. The European ambition stands as a priority. Making the European Union a major player in crisis management and international security is one of the central tenets of France's security policy. France wants Europe to be equipped with the corresponding military and civilian capability. The White Paper recalls several concrete goals for European defense in the coming years: set up an overall intervention capability of 60,000 soldiers, deployable for one year; achieve the capability to deploy for a significant duration two or three peace-keeping or peace-enforcement operations and several civilian operations of lesser scope in separate theatres; increase the European planning and operational capability both military and civilian; and restructure the European defense industry. In addition, the White Paper emphasizes four priority areas for the protection of European citizens: the reinforcement of cooperation in the fight against terrorism and organized crime; the development of European civil protection capabilities; the coordination of the defense against cyber-attack; and the securing of energy and strategic raw materials supply. Lastly, the White Paper advocates the drafting of a European White Paper on defense and security.

9. The White Paper emphasizes that the European Union and NATO are complementary. France is committed to the reform of NATO. The White Paper acknowledges that Europe and NATO have changed considerably General de Gaulle withdrew French forces from the NATO integrated military command in 1996 and since the previous White Paper was published in 1994. The European Union has emerged as a major player in the international community. NATO has maintained its responsibility for the collective defense of the allies but is also a peacekeeping instrument (Afghanistan, Kosovo). There is no competition between NATO and the European Union. The two are complementary. It is imperative that both organizations come to grips with the complexity of international threats and crises.

10. This reality leads the White Paper to advocate the full participation of France in the structures of NATO. For the authors, this evolution will go hand in hand with the reinforcement of the European Union in the area of crisis management and the search for a new balance between the United States and Europe within NATO. With regard to France's position, the White Paper reaffirms the three main principles in direct continuity with those defined by General de Gaulle: complete independence of nuclear forces; full freedom of assessment, which implies the absence of automatic military commitment and the maintenance of assets allowing for strategic autonomy, in particular by increasing intelligence capabilities; and lastly, permanent freedom of decision which means that no French forces shall be permanently placed under NATO command in peace time.

11. The new format of French armed forces is to be determined on the basis of operational goals decided by the government based on the proposals made by the White Paper Commission. The main force levels proposed are as follows:

    a. An operational ground force (*Force Opérationelle Terrestre*) of 88,000 men, enabling a force-projection capability of 30,000 soldiers with six month notice, 5,000 soldiers on permanent operational alert, and the capability to mobilize 10,000 soldiers on the national territory to support civilian authorities in case of a major crisis;

    b. An aircraft-carrier group including combat, surveillance and rescue aircraft and helicopters, 18 frigates, six nuclear attack submarines (SSNs) and the capability to deploy one or two naval groups either for amphibious operations or for the protection of sea lines;

    c. A joint fleet of 300 combat aircraft, regrouping the combat aircrafts of both the Air Force and the Navy, which will allow the permanent deployment of 5 squadrons on national territory and a force projection capability of 70 combat aircraft.

12. The White Paper defines a consistent defense effort based on the dual concern of improving without delay the availability and modernization of the most frequently used equipment and launching programs related to intelligence and preparation for the future. The White Paper also calls for the launch of new programs, during the same timeframe, in the field of intelligence and anticipation (knowledge-based security, observation, electronic intelligence, early warning) on land, at sea and in the air with the development of surveillance and armed drones, as well as both offensive and defensive cyber-war capabilities. The White Paper states that France shall devote significant finances to its defense, consistent with the priorities and choices made for its operational capabilities. This statement gave a sense of assurance that defense spending would not decrease. During the initial period (2008-2012) annual resources should be constant in volume—that is, increase at the same pace as inflation. Then, during a second phase, starting in the year 2012, the budget will increase at the pace of 1% per year in volume, that is, 1% above the inflation rate. Between now and 2020, the aggregate funding devoted to defense excluding pensions will amount to €377 billion. The procurement budget will increase from an average of €15.5 billion in past years to €18 billion on average per year for the period 2009-2020, and will also impact defense personnel training and living conditions. However, these ambitious objectives now seem difficult to fully implement given the unforeseen global financial crisis which occurred following the release of the Livre blanc was released.

13. It also devoted significant sections to the importance of the French defense industry and emphasized that France must retain its industrial capabilities and its political autonomy, particularly in the areas of: nuclear deterrence, ballistic missiles, nuclear attack submarines, and cyber-security. It also recognized that individual European countries can no longer master every technology and capability at a national level and therefore, France believes that the European industrial and procurement framework must be prioritized in the areas of combat aircraft, drones, cruise missiles, satellites, electronic components etc., although procurement policy must include acquisitions on the world market.
14. Finally, it recommends the reorganization of public authorities in order to take into account this new national security strategy.

Based on these key finding the White Paper details precise specifications in terms of future procurement for force protection and land combat capabilities to include: drones for surveillance and combat drones for air-land operations, nuclear attack submarines (SSNs) carrying conventional cruise missiles (by 2020), four large amphibious ships (*Mistral* class) with 18 first-line frigates, detection and early warning capabilities aimed at ballistic missile capabilities, a single pool of 300 combat aircraft for the Air force and the Navy (*Rafale* and modernized *Mirage* 2000), and a doubling of funds available for space military programs (from a base of 380 million euros in 2008) is prescribed as well as the establishment of a Joint Space Command, a new concept of cyber-defense and the establishment of an offensive cyber-war capability, intelligence collection and signal interception, civilian and civil-military crisis management operations, a new system will combine targeted messages via SMS, media or e-mail together with the current modernized siren network, and an inter-ministerial Crisis Management Centre for the direction and control of crisis response operations on national territory.

All these policy recommendations derive from the following new security parameters which have been factored into the strategy enshrined in the *Livre blanc*:

- The growing interconnection between threats and risks: This is a direct consequence of globalization which removes barriers between conflicts and risks, much as it does in benign or positive fields such as trade and communication. These risks must be dealt with first by actions aimed at preventing the outbreak or spread of armed conflict. These risks of interdependence and the cascading effect of crises call for large-scale responses and the integration of economic, social, environmental, and security policies.
- The continuity between domestic and foreign security: The traditional distinction between domestic and foreign security has lost its relevance. This continuity has taken on strategic significance, of which France and Europe have to draw the full implications. Comprehensive strategies and the integration of the different dimensions of security are required.
- The possibility of sudden strategic surprises or strategic shocks: International uncertainty and instability lend plausibility to scenarios of strategic upsets and surprises which our defense and security systems may not be fully prepared to address. Apart from terrorism, the White Paper acknowledges that developments related to as the proliferation of weapons of mass destruction, cyber-warfare, and the emergence of new weapons as a result of technological breakthroughs will likely be found in a future strategic surprise scenario. The risk of a nuclear attack (breaking the "nuclear taboo") also cannot be ruled out. Many potential major regional

contingencies have the potential to degenerate into a world-wide strategic upset. The offensive use of outer-space, applications flowing from nanotechnologies, bio-technologies, massive strides forward in computer technology, new sources of vulnerability of space-based assets, come to mind as well. Other "black swan" events may well arise with substantial and unexpected strategic consequences.

– Developments impacting future military operations: Future military operations will increasingly be conducted for and in the midst of civilian population centers, generally in an urban environment. A more worrying trend is that current "peace operations" are increasingly lethal, which puts a premium on force protection. Superior technology does not, *per se*, guarantee operational superiority. The human factor will remain prevalent in complex international operations where all instruments of power and influence are brought to bear.

Ultimately all of these factors lead to the establishment of a new national security strategy. Its goal is to deal with the risks or threats which may affect the life of the nation. Its first aim is to defend population and territory. The second is to contribute to European and international security. The third is to defend the values of the French Republic which binds together the French people and their State: the principles of democracy, including individual and collective freedoms, respect of human dignity, solidarity, and justice.

These aims are achieved by:

– Defense policy, *in toto*. Defense policy has to ensure the security of the nation vis-à-vis the risk of an armed aggression, the fulfillment of our international defense commitments, the contribution of France to international peace and security, its participation in the protection of the population on French soil and French citizens abroad in support of domestic security and civil security organizations.

– Domestic security policy, in matters other than the day-to-day security of individuals and their property, and civil security policy. As part of national security, these policies must ensure on a permanent basis the protection of the population, the functioning of our public institutions and the maintenance of a degree of normality in the country's life in times of crisis, and defend the security interests of the nation against non-military threats.

– Other public policies, particularly diplomatic and economic policy, insofar as they contribute directly to national security.

There is an obvious and fundamental difference between security threats resulting from hostile intent and unintentional events, such as natural catastrophes. However, the need for anticipation, advance planning, preparation and timely action are the same in both instances. Terrorism in Europe is staged both from outside and within our societies. Large-scale criminal networks take advantage of borderless globalization. Energy security cannot be envisaged outside of a global perspective. Information systems are vulnerable regardless of borders. The same applies to natural disasters or health risks.

The Impact and Net Effect of Strategic Reviews

The last French White paper laid the groundwork for a major overhaul of the French national security strategy by establishing the very concept of national security at the core of the French approach to security. In terms of foreign and security policy, it played a decisive role in preparing the French "full participation" in NATO and the 2009 decision to reintegrate into NATO's command structure. Many organizational reforms were also undertaken following the recommendations of the White Paper and have led to the most significant transformations of the national security apparatus since the early days of the Fifth Republic. The 2008 White Paper will therefore remain a milestone in terms of defense reform and strategic review. It is likely to have shaped national security structures for an extended period of time.

Due to budgetary constraints, some of the White Paper's key prescriptions in terms of procurement or force structures have not been implemented in the last 3 years and could be further postponed or abandoned. This trend was already visible in the preparation of the 2009-2012 procurement bill, which fell short of implementing all recommendations of the White Paper. This was further emphasized when the global financial crisis hit. It should, however, be noted that the overall force structure and defense priorities have not been massively reviewed at this stage, and that political authorities continue to insist that key objectives will be met even though some procurements could face delays. This affirmation might not resist post-crisis budgetary reform, and remains to be tested beyond the 2012 presidential election.

The influence of the French White Paper beyond French borders is interesting to assess. There was great interest among the international security community and the Paper is often quoted as a reference document for other national strategic reviews in Europe and beyond. The value of its analytical framework is usually recognized and has not raised major criticism abroad.

Although they were adopted the very same year, the 2008 revised EU European Security Strategy (ESS) fell short of French expectations as the EU failed to endorse some of the recommendations of the French White Paper; Paris was unsuccessful in its attempt to launch the drafting of a genuinely new ESS; and only had limited successes in introducing fresh ideas and concepts into the ESS. The current ESS has been criticized in French security circles for its lack of ambition and its failure to truly tackle some major security challenges. The French continue to advocate the adoption of a *Livre blanc européen* on defense and security, which was a formal recommendation of the 2008 White Paper.

Within the NATO strategic concept process, France has so far been more successful. The choice of an influential member of the White Paper commission (Bruno Racine, Chairman of the National Library) as the "French" expert in the NATO Group of Experts on the Strategic Concept has led to the endorsement of some ideas derived from the *Livre blanc* in the Group's final report. Although it is difficult to identify direct ideas or quotations, the 2010 NATO Strategic Concept does reflect this indirect influence.

The French *Livre blanc* also influenced, to a certain degree, other national processes. The British 2010 *Strategic Defence and Security Review* (SDSR) does offer a very close assessment of the security environment which underscores the broadly similar approaches of the security and defense challenges that the two leading European players in the field perceive. Other national white papers in Europe

have benefited from exchanges with the French on the *Livre blanc,* a Dutch team for instance visited Paris for exchanges in preparation of their own white paper.

Searching for Transatlantic Methods

When discussing opportunities for a transatlantic cooperative effort, some useful lessons and recommendations can be drawn from the *Livre blanc* experience:

1. Time constraints should not be too tight for the strategic reviews. The *Livre blanc* process lasted more than six-months, which allowed extended consultations in France and abroad with officials and non-officials, and enabled the drafting process to take place without excessive time constraints. This also facilitated a consensus-building process.
2. A commission combining external experts and senior government representatives, military and non-military participants, proved a fruitful process balancing the creativity of outsiders with the realism (and sometime conservatism) of insiders and the other way around. This also facilitated validation of various recommendations and prescriptions by those policymakers on the Commission by facilitating the implementation of most of the recommendations.
3. Consultations abroad *during* the writing process, not just *after* the interagency debate had been closed, were extremely useful and fruitful according to the members of the Commission. They also facilitated future common approaches, as inputs may be fed into future strategic reviews.
4. The French Cartesian (or French garden) approach has proven quite efficient in developing policy recommendations from an in-depth assessment of the security environment and turning them into specific prescriptions.
5. Some concepts as the management of "strategic surprises" are probably relevant far beyond the French case, and are worthy to be considered by future strategic reviews.

In practical terms, a genuine transatlantic effort is difficult to envisage (beyond the NATO process) for a series of reasons. First, calendars which are often driven by domestic legal or political constraints do not match and it is very difficult to bring them much closer. Second, each strategic review serves a different purpose, and the fact that it is carried out by a nation state or an organization such as the EU or NATO differentiate both process and output of strategic reviews. Third, substantial differences related to security issues continue to exist both from a transatlantic perspective and within Europe itself.

It could however be useful to undertake policy actions aimed at fostering transatlantic cooperative efforts. First, the EU should initiate a strategic review and prepare a real EU White Paper/New Security Strategy which would serve as the basis of engagement with the U.S. and other partners on a consolidated EU analysis.

- It should also examine the feasibility of establishing a wise-men group (with officials and non-officials) on transatlantic security. The last NATO strategic concept remained focused on the role of the Alliance itself, but there is room to reflect on how U.S., EU, and EU

member states may share their understanding of security issues and creatively explore ways of cooperation.

- In this context, transatlantic ties between research institutions and policy-planning staffs should be expanded and deepened to create a solid web of formal and informal connections which facilitate a transatlantic security dialogue.
- Finally, security issues beyond the Euro-Atlantic area should be analyzed jointly. At times, Europe does not think in strategic terms on issues such as Asia, which is a good example of the type of problem that could be overcome through deeper dialogue. Asia has become a priority for the U.S. agenda, and it may represent a fruitful field of transatlantic engagement.

THE U.S. CASE: 2002 AND 2010 U.S. NATIONAL SECURITY STRATEGY

Heather A. Conley, *Senior Fellow, Director of the CSIS Europe Program*, with Manuel Lafont Rapnouil, *Visiting Fellow, CSIS Europe Program*, and Michael Cass-Anthony, *CSIS Europe Program*

Dating back to World War II and at a time when the United States was challenged both domestically as it emerged from the Great Depression and internationally as it fought militarily on two continents, the Roosevelt administration initiated a process that strategically assessed how America would meet future international security challenges. Since that time, the United States has developed a rich culture of strategic security planning. However, it was only in 1987 when the United States Congress formally required, under the auspices of the Goldwater-Nichols (Department of Defense Reorganization) Act[1], the Executive Branch to provide a National Security Strategy (NSS) annually to Congress. The NSS serves as the principle strategic tool through which an American administration defines U.S. "national security" and addresses issues related to its implementation.

A national security strategy relies first and foremost on a clear definition of what "external security" means. For the United States, external security is its national security and therefore its national security strategy identifies, defines and prioritizes these threats, identifies the constraints placed upon national security policy, and finally articulates policy recommendations on how to deal with these documented threats and constraints. The series of strategic documents that follow the strategic cornerstone of the NSS identify what is needed and what must be completed in terms of policy, legislative tools, human and financial resources, military capabilities, and administrative structures.

In recent years, the NSS has diminished as the penultimate U.S. national security document, although it most certainly plays a role in giving public voice to an American President's tactical approach to the conduct of foreign and security policy. Rather, the annual budget process, particularly the Defense Department's budgetary process, has become the most critical U.S. strategic document which shapes and prioritizes U.S. interests. Other major U.S. strategic documents, to include the Quadrennial Defense Review (QDR) and the recently launched Quadrennial Diplomacy and Development Review (QDDR), attempt to provide more direct strategic guidance to the annual budgeting process. But, regardless of their larger strategic impact, which can widely vary, U.S. strategic reviews do make one important contribution: they bring together a large number of agencies that are engaged in formulating national security policy and make them produce a final, unified

product. Simply put, there is an intrinsic "value of the process" to the national security community as a whole.

The following paper focuses on the formulation of U.S. national security strategies over an eight year period, beginning with the Bush administration's NSS released in 2002 and concluding with the recently produced NSS by the Obama administration which was released in May 2010. From a U.S. perspective, this paper will examine the historical context, purpose, value, and accomplishments (both attempted and achieved) in which strategic reviews take place as well as the identification of the noteworthy patterns of the American strategic model in the last decade and possible transatlantic applications to these patterns.

Historical Context

Over the past twenty years, the U.S. national security strategy has continuously referred to the global strategic environment in a post-Cold War context. In 1991, President George H.W. Bush referenced an international order after the fall of the iron curtain, "The Cold War is over, its core issue resolved. We have entered a new era, one whose outline would have been unimaginable only three years ago…this new era offers great hope, but this hope must be tempered by the even greater uncertainty we face."[2] The strategic environment was shaped by the creation of a new, yet unclear and uncertain world order that would challenge U.S. power both in its ability to ensure its security and to advance its declared national interests. These national interests consisted of promoting and disseminating democratic principles, preventing terrorists and terrorist networks from obtaining weapons of mass destruction, and engaging as well as strengthening international alliances. The NSSs of the 1990s prescribed America's capacity to shape this new world order into a more secure, prosperous and stable direction as "the United States remains the only state with truly global strength, reach and influence in every dimension -- political, economic and military. In these circumstances, our natural desire to share burdens more equitably with newly-strong friends does not relieve us of our own responsibilities."[3]

The 2002 NSS is perhaps the most interesting of America's national security strategic literature as it describes U.S. national security interests following the September 11th terrorist attacks. The 2002 NSS was meant to respond to a very different strategic environment than was envisioned in the 1990s. Although terrorist attacks were articulated in previous U.S. security strategies (the 1991 security strategy often mentions combating different forms of "international terrorism"), attacks of comparable audacity to the September 11 assault on the U.S. homeland were not considered. Beginning with the 2002 NSS and continuing to the most recent review, the United States has defined itself as being "at war" consistently and by two separate Administrations. The 2002 NSS notes that the U.S. is fighting a war against "terrorists of global reach;"[4] the 2006 NSS states in its introduction that "America is at war;" in 2010, the NSS declares that we are "at war with a specific network, Al-Qaida, and its terrorist affiliates…"[5]

The Obama Administration's 2010 NSS concentrates on a repudiation of and differentiation from the policies and overall tone of the previous administration and articulates its own framework for tackling new challenges. However, the politics of foreign policy differentiation are nothing new: they

are more the norm. It is interesting to note that the 2002 NSS was a reaction against the previous Clinton administration's policies in light of the 9/11 attacks. The tactical differences in approach from one American administration to another and the message these differences send to the world are essentially what makes these documents of value and interest perhaps more than the way the United States perceives the current and future state of play of the international environment.

The Process, Purpose and Value of U.S. Strategic Reviews

In theory, an American administration first formulates its overarching national security strategy and then subsequent strategic and budget reviews are developed to align national objectives with capabilities and means. Once the NSS is released, the major national security agencies, particularly the Defense Department, begin to develop their documents with an eye to minimizing gaps between objectives and means, eliminating budgeting redundancies and ensuring that agencies do not work at cross-purposes. All such documents are expected to derive from a shared and integrated strategic vision with the NSS serving as the point of alignment. This rich collection of strategic review documentation is meant to offer a comprehensive and articulated view of America's national security strategy and the means to achieve this strategy. Practice, however, can be different from theory. For example, when President Obama came into office in January 2009, the reverse strategic review order occurred: the Defense Department released its budget (May 2009); the Quadrennial Defense Review (QDR), a four-year strategic review of DoD's strategies and priorities was released (February 2010); and then the NSS was completed (May 2010).

Because the United States does not rely only upon the NSS, a broad and diverse array of strategic reviews is also considered an integral part of the strategic review landscape. The major U.S. strategic reviews are shown in the following table.

Major Strategic Documents as of 2010

	When was it instituted?	Who is in charge?	How often is it conducted?	For whom is it mandated?
National Security Strategy (NSS)	1987 Goldwater-Nichols Department of Defense Reorganization Act	White House (NSC)	Every year (in theory; in practice, NSS were not released in 1989, 1992, 2001, 2003, 2004, 2005, 2007, 2008 and 2009)	Congress
Quadrennial Defense Review (QDR)	1996	Department of Defense	Every four years (in theory; in practice 1996, 2001, 2006, and 2010)	Congress
Quadrennial Diplomacy and Development Review (QDDR)	2010	Department of State (with USAID)	Every four years First one completed 2010	The White House
Quadrennial Homeland Security Review (QHSR)	2010	Department of Homeland Security	Every four years First one completed 2010	Congress

Source: Heather A. Conley, CSIS.

Note: Other important U.S. strategic review documents include:

- **Quadrennial Intelligence Community Review** issued once every four years, this report is compiled by the Director of National Intelligence, and directly contributes to the QDR.
- **Nuclear Posture Review** is conducted by the Department of Defense in close consultation with the Departments of State and Energy. It looks at nuclear deterrence policy and strategy for the next five to ten years.
- **Ballistic Missile Defense Review** first released in 2010, with input from across the government, assesses the threats posed by ballistic missiles and coordinates a missile defense policy responsive to those threats. Its analysis feeds into the QDR report.
- **Space Posture Review** reviews and analyzes the space strategy from both a military as well as a national security perspective, in addition to researching new technologies. The report feeds directly into the QDR.
- **National Defense Strategy** provides a framework for achieving the objectives set forth in both the NSS and reflects the results of the QDR. It informs the National Military Strategy and is released every two years in order to provide the best assessment.
- **National Military Strategy** draws from the NSS and QDR and delivers the strategic aims of the armed services every two years.

Most of these documents are legislatively mandated and part of their content may be classified.

In light of this dizzying array of strategic documents, one could fairly argue that these reviews are simply an overgrown pile of bureaucratically constructed paper designed to fulfill Congressionally-mandated obligations and sooth certain political constituencies, rather than actually play a strategic role. This raises an important question: who exactly is the American audience for strategic reviews?

Clearly, there is a hierarchy of audiences: first and foremost, the U.S. Congress. Congress requests these documents from the administration as part of its oversight responsibilities but the strategic review is also designed to place each administration on the record (both in unclassified and classified forms) with its assessment of the challenges and how it believes U.S. strategy should meet these challenges. To underscore how important these reviews are to Congress, Secretary of State Hillary Clinton gave her views on the importance of the strategic review process as a Senator serving on the Armed Service Committee. She noted,

> … it became very clear to me that the QDR process that the Defense Department ran was an important tool for the Defense Department to not only exercise the discipline necessary to make the hard decisions to set forth the priorities, but provided a framework that was a very convincing one to those in the Congress, that there was a plan, people knew where they were headed, and they had the priorities requested aligned with the budget, and therefore, people were often very convinced that it made good sense to do whatever the Defense Department requested.[6]

The next audience of priority for these strategic reviews is the U.S. administration itself and the countless number of departments and agencies that must be engaged to write these often lengthy and complex reports. As noted earlier, there is an intrinsic "value of the process" in bringing the interagency community together to engage in a task, coordinating with one another and ensuring the multitude of strategic reviews are not contradictory. Just as the National Security Strategy involves a wide inter-agency process, each subaltern document involves its own mobilization of the relevant administrations and bureaucracies which reinforces a sense of ownership, ensures sufficient clarity of mission, provides consistency in implementation and secures the leadership's commitment to an agreed set of priorities and a subsequent strategy. Once the strategic document is finalized, the U.S. national security bureaucracy is provided with an overarching framework that the bureaucracy must (in theory) utilize in its future policy formulation. This may be particularly true with regards to the newly formed Quadrennial Homeland Security Review (QHSR) and the Quadrennial Diplomacy and Development Review (QDDR). Although it is premature to assess the QHSR and the QDDR, these new strategic efforts, at the administration's initiative, may be an administration's attempt to reorganize recalcitrant bureaucracies more than it is an attempt to be strategic and comprehensive.

The audience of growing importance for these strategic reviews (if they are publicly released in unclassified form) is foreign governments, the international media, the think-tank community, international opinion leaders, political pundits and, to a lesser extent, the American people themselves. The NSS, in particular, and the QDR initiate an important foreign policy conversation as these documents are closely scrutinized by other nations, friends and foes alike. These strategic reviews serve as an essential public diplomacy policy tool as they channel key policy messages to a wide range of international actors. All of these audiences influence the conduct of the American strategic review process, overtly and inadvertently, and on occasion, these external audiences can influence the final strategic project.

New Strategic and Conceptual Thinking

American national security strategies have helped shape new language and descriptions for today's foreign policy challenges. In the 2002 NSS, a significant number of new phrases and vocabulary emanated from the Bush administration's post–September 11 description of the world. For instance, the phrase "global war on terrorism" terminology was introduced[7]. In 2005, Secretary of Defense Rumsfeld promoted a change in wording to "Global Struggle Against Violent Extremism," but that phrase did not catch on, and the "War on Terror" expression was again used in the 2006 NSS; early on, the Obama administration decided to avoid using the term and replaced it with "Overseas Contingency Operations."[8] The 2010 NSS eventually uses the phrase "violent extremism."[9]

Any significant bureaucratic exercise, particularly one as important as the NSS, pays a great deal of attention to the selection of words and strategic terminology. Some newly introduced concepts, as was the case with the 2002 references to "preemptive actions" or to a "global war on terrorism" can become highly contentious internationally, but new terminology can also provide enduring terms, such as "coalitions of the willing." For instance, "free trade" is a recurring term in the 2002 and 2006 documents although this term does not appear in the Obama administration's strategy. Another case would be the 2010 NSS refers to Pakistan in most instances when Afghanistan is addressed. Noticeable wording and new terminology may reflect the administration's priorities, particularly "engagement" as opposed to unilateralism, and to signal a new initiative, "a world without nuclear weapons" or President Obama's Global Zero initiative. New areas of interest are the most fruitful areas to find fresh terminology, such as in the field of "cyberspace" and "cybersecurity"[10].

The following chart depicts the striking differences between the 2002 NSS (excluding for the moment the 2006 NSS which is similar to the 2002 in many respects) and the 2010 NSS on several critical issues:

NSS 2002	**NSS 2010**
A unipolar posture "forces of freedom," "unparalleled military strength," "preemptive actions"	An avowed need for international cooperation "engagement," "cooperation," "leadership," "partnerships" and "rules-based international system"
A focus on external threats	More attention paid to the domestic foundations of national security (including attention to homegrown radicalization)
Prioritization of hard security threats in general, and the risk of terrorists resorting to weapons of mass destruction in particular	A broader vision of national security that incorporates domestic policy challenges (e.g. environment, technology, and development)
A narrow vision of the national security toolbox "make use of every tool in our arsenal-military power, better homeland defenses, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing"	A broader, "smart power," "whole of government" approach "Our Armed Forces will always be a cornerstone of our security, but they must be complemented. Our security also depends upon diplomats who can act in every corner of the world, from grand capitals to dangerous outposts; development experts who can strengthen governance and support human dignity; and intelligence and law enforcement that can unravel plots, strengthen justice systems, and work seamlessly with other countries."

Source: Heather A. Conley, CSIS.

For some, the U.S. NSS appears to be less strategically relevant and designed more to be a political statement of intent, meaning that the greater the public fanfare associated with the unveiling of an American security strategy the greater the risk that the NSS becomes rhetorical window-dressing rather than a serious strategic document. Particularly on contentious or controversial policies, there is a temptation to use the NSS as an opportunity to posit grand expectations and ambitions that may or may not be achieved or reached. More often than not, the U.S. administration will use the occasion of a strategic review to espouse a more positive vision for the world and how U.S. policies and engagement will achieve this vision. This is particularly true for the 2010 NSS. The first chapter provides a description of "the world as it is" and then articulates "the world we [the U.S.] seek[s]." This phenomenon may be culturally specific in some respect to the United States as it has historically struggled between two different visions of its role in the world: a proactive, global leadership vision of the United States as a shining model or the more isolationist vision, designed to avoid foreign entanglements.

How common is it then for strategic terminology to migrate transatlantically (in both directions)? We can identify occasional examples. The 2010 NSS incorporates the concept of "resilience," which is defined as the "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption"[11]. This term was first found in a security strategy first officially endorsed by the U.K. in 2008[12] and adopted in the French National Security Strategy later that same year. It is a rare case when a foreign concept is imported to the U.S. for use in its official national security doctrine. In another example, the 2010 NSS makes reference to a "whole of government" approach to characterize strategy to make all the tools of U.S. power, military, economic and diplomatic more efficient and effective. Some could argue that this term was introduced much earlier in European security documents as taking a "comprehensive approach" when bringing all instruments of power together for greater intended effect.

The Impact and Net Effect of Strategic Reviews

Although the overall impact of a U.S. strategic review process is difficult to quantify, four measurements of success can be identified: internal consistency, strategic durability, organizational restructuring, and budgetary impact.

Internal consistency of strategic language is a significant measurement particularly given the wide array of required U.S. strategic review documents and coupled with the fact that not all reviews are conducted simultaneously or in a particular order. In fact, more narrowly focused reviews may be written well before overarching documents, such as the NSS, are completed. There was language consistency between the 2010 NSS and the 2010 QDR (despite the fact that the QDR was released prior to the NSS), both in substance (on the role of military power[13]) and in general strategic terminology (references to "engagement" and "a world free of nuclear weapons"). Another dimension of consistency is the relation between strategic language and the creation of implementation processes. The 2010 NSS articulates an ambition to integrate national and homeland security which was borne out in the administration's first attempt to undertake a Quadrennial Homeland Security Review (QHSR). Although the QHSR's first output was not entirely successful, it does respond to the call for greater integration of national and homeland strategies. More recently, the State Department

launched a Quadrennial Diplomacy and Development review (QDDR) to better integrate diplomacy and development more fully and strategically.

Strategic consistency can also be identified in either: (1) a theoretical (top-down) approach, whereby the strategic assessment affects how resources and capabilities are allocated or, (2) an organic (bottom-up) approach whereby budget data is examined and the implementation of the strategy is reflected "in the numbers," so to speak. Since the Obama administration's strategic approach was organic in nature, we can more readily observe whether the budget numbers conformed to the overarching NSS framework.

One of the strategic aims of the 2010 NSS was to attempt to rebalance U.S. foreign policy away from hard power-projection toward greater diplomatic and development engagement, so-called "smart power[14]" in order to achieve an integrated national security policy. Therefore, the budget should reflect an effort to shift resources away from the Defense Department (both in programs and personnel) to the State Department and the Agency for International Development (USAID) or an effort to increase or make existing resources more effective and efficient. Indeed, in the fiscal year 2010 International Affairs Budget and in its fiscal year 2011 request, the administration asked Congress for additional funds (the administration seeks to double foreign assistance by 2015) and in personnel (500 more positions at the State Department and 200 more personnel at USAID) in order to enhance civilian post-conflict capabilities. Clearly, there was internal consistency in the Obama administration's strategy. But overemphasis of budget analysis can be equally problematic: a strategy that looks like a shopping-list in order to be consistent with budget requests rather than a series of strategic priorities will likely be either trumped by the budget process or will miss its strategic target[15]. Moreover, the drive for international consistency (particularly through budgetary means) should not marginalize the need to adjust strategy by taking into account a new assessment of the international environment or a lessons learned process during implementation. A very clear example of the need to adjust a strategic framework was the 2002 NSS, which was redrafted following the September 11th attacks to reflect the changing priorities and security paradigm. Here, the NSS was not completely consistent with the 2001 QDR (which was released on September 30, 2001). Unfortunately, administrations often avoid adjusting strategy in the interest of being politically consistent. The 2006 NSS was a concerted effort to validate the course of the 2002 NSS when strategic adjustments were clearly needed and eventually took place in the 2010 NSS.

The second criteria, the durability and credibility of the strategic assessment, is best analyzed in hindsight. Does the strategic assessment remain valid over an extended period time? With hindsight, it is easy to point to shortcomings in the 2002 NSS, which dismissed too quickly the remaining challenges in Afghanistan and overlooked the non-proliferation crises in North Korea and in Iran. The 2002 NSS position on Russia would be characterized as overly optimistic, "Russia is in the midst of a hopeful transition, reaching for its democratic future and a partner in the war on terror."[16] But the 2006 NSS offered a more candid assessment identifying that "recent trends regrettably point toward a diminishing commitment to democratic freedoms and institutions"[17], therefore, an adjustment was clearly made. It will be another year or two before we can make similar assessments of the 2010 NSS: what did it get right or what did it get wrong? Even if the NSS was prescient in its assessment of risk and clairvoyant in its declaration of U.S. policy, it may still be insufficient to provide the necessary political "cover" for any given U.S. administration. For example, the 2000 NSS

correctly identified the threat of terrorist attacks against U.S. facilities, interests or individuals overseas, the grave risk of terrorists acquiring weapons of mass destruction, and the need for a "consequence management ability to significantly mitigate injury and damage" in case of an attack against the United States. However, there was a significant political backlash in the United States that America was unprepared and not on alert for this type of eventuality. Strategic surprises are a major concern for strategic planners. Forecasting in an uncertain, fluid and fast-paced environment is a difficult exercise although not making strategic choices or defining strategic priorities makes it impossible to build a durable and credible strategy in an environment of budget constraints.

The third leading indicator of the lasting impact of a strategic review is how bureaucratic structures and intergovernmental coordination are affected. Are organizations created, eliminated, or streamlined? Frequently, NSSs dedicate a section strictly to organizational structure. In the 2002 NSS, the section was entitled, "Transforming America's National Security Institutions" and in the 2010 NSS, it was called "Strengthening National Capacity." The most compelling example of organizational transformation and reform stems from the 2002 NSS' creation of the U.S. Department of Homeland Security and the position of Director of National Intelligence[18]. A growing trend in U.S. strategic thinking as a result of lessons learned in America's intervention in Iraq and in Afghanistan is the need for greater interagency coordination and more integrated action by relevant national security agencies, particularly a whole-of-government approach and greater intelligence integration. This approach is what is strategically driving the QDDR effort to clarify the respective role and mission of the State Department and USAID (to either separate or integrate these agencies) in order to create a more integrated approach to working more effectively with the military. Another example of organizational change due to the strategic need for greater post-conflict integrative demand is the creation of the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) in the Department of State. Although the organization was created, sufficient budget resources have not been allocated for the office to realize its potential to provide the civilian response or "surge" the Defense Department has requested to ensure a more comprehensive crisis management policy.

The final measurement for a NSS is an assessment of its overall performance, measured not only in terms of accomplishing its stated goals but also in tangible outcomes. Obviously, no strategy is fully successful. But it is clear that a strategy which is vague, its objectives too broad and encompassing, and which focuses more on means than ends is doomed to fail. To be as successful as possible, a strategic document must accurately define the challenges and effectively articulate what is to be done to meet those challenges. Subsequent reviews must convey clearly defined and measurable, short and medium-term goals that respond to the stated challenges as well as the means and resources to accomplish them. For example, if a NSS identifies terrorism as a threat and suggests a robust counter-terrorism strategy, then the QDR and subsequent defense budget would include increasing intelligence, surveillance and reconnaissance resources, acquiring additional predator drones and enhancing other key enabler capabilities.

In the 2002 NSS, America's national strategy derived from a combination of two assessments: the U.S. held unprecedented and unequaled strength and influence in the world and the greatest challenges were threats posed by global terrorism, weapons of mass destruction, and authoritarian regimes, "We know from history that deterrence can fail; and we know from experience that some enemies cannot be deterred"[19]. The document emphasized the need for alliances, coalitions, working

with others, cooperative action, "this path is not America's alone. It is open to all.[20]" In response to a profound national shock, the 2002 NSS sought deep organizational transformation: "The major institutions of American national security were designed in a different era to meet different requirements. All of them must be transformed[21]" and placed extraordinary emphasis on hard power projection: "It is time to reaffirm the essential role of American military strength[22]"and intelligence. Diplomacy was primarily viewed as a means to more effectively communicate, with a view to helping the Muslim world understand the United States and its ideals as a counterweight to extremism. In analytical hindsight, America did transform its bureaucracy and relied heavily on its military might. But the U.S. government did not work with alliances and partners, particularly in Europe, and its efforts to reach out to the Muslim world and implement more effective public diplomacy was negligible.

The 2010 NSS identifies a need for a more balanced vision of the national security toolbox, utilizing the whole-of-government approach to "update, balance and integrate all of the tools of American power[23]" while expanding the notion of national security to include homeland security and economic issues, including trade and energy. Well before the release of the 2010 NSS, the Obama Administration requested, under the authority of Presidential Study Directive 1, a study analyzing a merger of the National Security Council and the Homeland Security Council. In May 2009, President Obama approved the merger[24], creating the National Security Staff (NSS). The NSS also mentions the importance of ensuring accountability of policy ownership both within the administration and beyond. Coordination across U.S. departments and agencies, "alignment of resources with our national security strategy, adapting the education and training of national security professionals to equip them to meet modern challenges, reviewing authorities and mechanisms to implement and coordinate assistance programs[25]" are mentioned as important examples of the 2010 NSS's call to align actions and words[26]. Finally, the 2010 NSS also outlines a new strategy of engagement with "adversarial governments" which would place the United States in a much more favorable negotiating position, "Through engagement, we can create opportunities to resolve differences, strengthen the international community's support for our actions, learn about the intentions and nature of closed regimes, and plainly demonstrate to the public within those nations that their governments are to blame for their isolation."[27] It is too early to predict how the 2010 NSS will perform. Due to the delay in its release, the 2010 NSS has had to codify the new administration's strategy and policies. Its efforts to engage with adversarial governments, such as Iran, North Korea or Burma, have thus far not produced results at this early stage.

Searching for Transatlantic Methods

Whereas the U.S. refers to its "national security," most countries would use the term "international security" or, at least, to the formulation of their "foreign policy." As a concept, *national* security is relatively new in both France and the UK. In a more technical perspective, American strategic thinking converges with Europe on the need to integrate external and internal security. Such a concern was already visible in the 2002 NSS ("Today, the distinction between domestic and foreign affairs is diminishing[28]"), but is even more obvious in the 2010 NSS. Transatlantically, the national security concept also has been broadened to fully integrate homeland security concerns.

The 2010 NSS and a growing body of European bilateral and multilateral strategic reviews demonstrate a growing commonality regarding the international security environment, with emphasis on its complexity, uncertainty and fluidity. The 2010 NSS also echoes European calls for more international cooperation and partnerships, in stating that "the very fluidity within the international system that breeds new challenges must be approached as an opportunity to forge new international cooperation"[29], although the U.S. strategy does not go so far as to call for "effective multilateralism" found in the European Security Strategy.

Because the United States and Europe face similar challenges and constraints, American and European strategic documents demand a flexible, whole-of-government approach but frequently receive external criticism for not having clear strategic and budget priorities. The most recent U.S. discussion on creating greater synergies between diplomacy and development budgets may hint at increasing similarities between the United States and Europe. The focus on improving the balancing of resources and identifying greater organizational efficiencies in the U.S. speak to the EU's current experience and experiment with creating the European External Action Service.

However, some important transatlantic differences remain, particularly on the use of force. Although there are important tactical differences in approach, the 2010 NSS does not radically alter the traditional U.S. view on the use of military force, "The United States must reserve the right to act unilaterally if necessary to defend our nation and our interests, yet we will also seek to adhere to standards that govern the use of force"[30]. The United States continues to see itself as a "nation at war" which has operational consequences and gives the U.S. military a significant if not dominant role in the implementation of U.S. foreign policy.

There is one particular transatlantic method that would be especially helpful during the strategic review process: consultation with other governments *prior to* the completion of the document. For example, the French White Paper committee held a series of meetings with U.S. officials and experts, as well as other senior officials from Europe, the EU, NATO, Asia, the Middle East and Africa during the drafting process. Prior to the public release of the U.S. QDR, Defense Department officials visited several European capitals to provide an overview of the document. There is a critical difference between informing another government and opinion leaders about a finalized strategic document and inserting the consultative process into a point in the review process prior to finalization. While other governments clearly appreciate receiving information before the general public, allies and partners are unable to provide input to shape the final product. An allied government does not have to endorse a particular threat assessment or approve a new concept or approach, but an ally should have an opportunity to comment on it. Another important opportunity would be for the senior officials and experts tapped to draft American and European strategic documents to meet for a candid discussion of the challenges and opportunities of drafting these documents prior to the initiation of the process in order to develop better common understanding of strategic terminology, concepts and threat assessment. This would assist in the transatlantic migration of strategic concepts and best implementation practices.

REVIEWING EUROPEAN SECURITY STRATEGIES

Erik Brattberg, *Research Assistant, UI*, and Mark Rhinard, *Head of Europe Program and Senior Research Fellow, UI*

Introduction

Strategic thinking on security matters is not new to the European Union, but previous strategic statements were limited to individual issues or regional challenges. The EU turned over a new leaf when it published the European Security Strategy, the EU's first attempt to formulate an explicit, overarching strategic framework to guide security policymaking.

This paper provides an overview of both the 2003 European Security Strategy (ESS) and its 2008 'review'.[31] The paper's aim is to illuminate the process by which these strategies were initiated, formulated, implemented and reviewed, as well as to ask whether those strategies have had the desired effects. This aim is situated within a broader goal: to improve transatlantic understanding of these processes with the hope of integrating transatlantic security concerns into future review processes.

Towards these stated ends, this paper examines each strategy (or revision) in terms of the situational and historical context in which it was conceived, the process by which it took shape, the final content of the strategy, and its effect on outcomes. Each section concludes with suggestions for integrating transatlantic security concerns through better U.S. and EU coordination.

The authors find that each strategy went through an elite-led and fairly insular formulation process, with little input from actors outside the EU institutions (or even outside of selected national capitals). One exception is the ESS, which was formulated by an 'inner core' of EU policymakers, but with systematic consultation with European think-tanks. Although finding consensus on a strategic statement amongst 15/25/27 member states is an accomplishment in itself, common weaknesses remain: (a) the strategies have had little impact on other policy or operational outcomes, as currently measured, and (b) the lack of wider consultation undermines the integrating potential of such strategies in a transatlantic context.

European Security Strategy (2003)

Situational and Historical Context

Although novel in the European Union context, the ESS did not emerge from a strategic void. The idea that a coherent set of shared ideas and principles should guide European foreign policy decision-making existed for at least a decade prior to the adoption of the ESS. In the Maastricht Treaty (1993), for instance, European governments sought to build a new 'pillar' for EU foreign policy-making, complete with distinct procedures and security-oriented policy officials. The Amsterdam Treaty (1997) subsequently reformed this 'Common Foreign and Security Policy (CFSP)' pillar and introduced the notion of 'common strategies' designed to set goals, priorities, and means to frame joint actions and common positions. Such strategies were subsequently created for Russia (1999), Ukraine (1999), and the Mediterranean region (2000). In 2003, the EU created a European Strategy Against the Proliferation of WMD, and by 2005 a European Neighbourhood Policy and the EU Counter-terrorism Strategy had been put in place, each with a 'strategic' dimension.

The EU's institutional developments also played a role in paving the way for the ESS. Growth of the EU's European Security and Defense Policy (ESDP) organizational apparatus, for example, led to an institutionalized web of new officials, committees, and processes focused solely on external security matters.[32] These institutions provided the foundation and resources for new ways to consider, formulate, and debate strategic concepts that included military officials more familiar with thinking in strategic terms. Ironically, the European Commission, the EU institution more traditionally associated with strategic and long-term thinking on the European stage, was sidelined from ESDP matters further highlights the need for more strategic and conceptual capacity-building on EU security in general.

Other institutional developments further enabled the potential for more comprehensive, strategic security thinking in the EU. By early 2003, the European Convention, a major undertaking aimed at producing a 'Constitution for Europe', was wrapping up its deliberations and moving towards an intergovernmental conference to reform the EU's founding treaties. The deliberations largely focused on security and defense issues, with many delegates voicing support for new conceptualizations of security and a better defined articulation of Europe's security role in the world. Many debates took place in the working group on defense, chaired by Michel Barnier, which was tasked with considering the winding down of the Western European Union (WEU) and the transfer of its security commitments to the EU. These debates opened up intellectual space for strategic thinking, making explicit calls for the formulation of a strategic concept[33] appear more feasible than ever before[34].

The launch of the EU's first military operation outside of Europe in the summer of 2003 to the Democratic Republic of Congo (DRC) also contributed to development of the EU's global security role and more defined strategic statements. The mobilization of the DRC mission, which took place without NATO participation and involved a level of troop risk not seen before, further raised awareness of the need for more coherent strategic thinking. The mobilization of the DRC mission (and the risk of EU troops being put in harm's way) had the affect of 'breaking the taboo on strategic thinking at the European level', bringing to light the need to align national and European objectives.[35]

International events at the turn of the millennium revealed a widening gap between the EU's practical tools and its vision of its own security role. This 'strategic gap', which might be tolerable in national systems familiar with setting vague goals and generic principles, led increasingly to an EU external policy 'unable to coordinate member state resources and translate this into actual influence'[36] which 'lacked direction, determination, and consistency'[37]. Previous strategic statements were too fragmented as the EU was becoming more ambitious in its global role.

Within ESDP -- which had become the main tool of the EU's security projection -- military and civilian capacities were being developed without an overall set of strategic principles for when they would be used, for what purposes, and towards what long-term goals. For example, the Headline Goal agreed to in Helsinki in 1999 was a purely operational statement. Or, one might also review Article 11 of the Treaty on the European Union (TEU), but that too only reiterated the Petersburg Tasks which indicates what kinds of missions the EU can launch (e.g., humanitarian tasks, rescue operations, peacekeeping, and peacemaking) and includes no guidelines for judging when they should be deployed[38]. It had become increasingly clear that the EU lacks an overarching strategic framework for rationalizing its role in international security matters.

If the context was ripe for a strategic statement on the EU's role in the world, the U.S. invasion of Iraq propelled the process of working towards such a statement, sparking a crisis in Europe and testing the coherence of the EU. Several EU states (notably the UK, Spain and Poland) joined the American-led 'coalition of the willing' whereas other EU states (e.g. Belgium, France and Germany) opposed a military invasion in the absence of a UN mandate and before all other options had been exhausted. One way to soothe tensions and repair diplomatic wounds was to initiate a process of reaffirming what binds EU member states together in terms of foreign policy. All member states could agree to such an endeavor: for some governments, a European strategic statement would allow them to distance themselves from U.S. security perspectives; for other member states, a European strategy would allow them, through an expanded security worldview, to demonstrate solidarity with the U.S. in terms of tackling new security threats. From there, the process of devising a security strategy was born.

Process

In what came to be known as the 'Rhodes Agreement for a strategic concept', Javier Solana was tasked by the EU foreign ministers on 2-3 May 2003 with drafting a document identifying key traits and security challenges facing the EU, and making recommendations for an overall European Security Strategy.

The drafting team formed by Solana was a fairly small group and kept under close control by a few key individuals, including Robert Cooper, Director-General, Politico-Military Affairs in the Council Secretariat. The perceived advantage of this style of process was that it offered the chance of preserving a 'personal' and non-bureaucratic approach to drafting. The team worked quickly and after one month had produced a first draft. 'A Secure Europe in a Better World', was unveiled by Solana at a Council meeting on 16 June 2003. Subsequently, the Thessaloniki European Council agreed on 20 June 2003 (without substantial discussion) to endorse the recommendations and to commission Solana with presenting the document for adoption by heads of state and government in December 2003. In the meanwhile, Solana was asked to work with 'Member States and the Commission' to refine

the text, which 'should also encapsulate Member States' interests and citizens' priorities[39]. The remaining time from October to December was used for internal discussion among member states and with the Commission and Council officials. Insider accounts suggest harried discussions and considerable tensions between Solana's policy unit (directly appointed by Solana) and the Council's permanent civil servants.

Following the Thessaloniki European Council, Solana turned to select European think tanks to solicit expert opinion on the draft. Three research workshops were held in Rome (19 September 2003), Paris (6-7 October 2003), and Stockholm (20 October 2003) under the overall coordination of the EU Institute for Security Studies (EU ISS) in Paris. Participants included academics and experts from Europe and beyond, including the U.S. The first workshop, which was held in Rome, focused on the threats facing Europe. Conference proceedings show that participants agreed that terrorism had become a major global threat and should remain high on the ESS threat list; they also agreed that threats like terrorism had to be understood and addressed within a broader socio-political context: 'Terrorism is rooted not so much in poverty as in political hopelessness.'

The participants also discussed WMD non-proliferation and organized crime. There was general agreement that Europe is both a base and a target for organized crime, terrorism and other threats. Debate emerged, however, around the definition of terrorism; the use of military pre-emption, especially against suspected illegal WMD facilities; and the need for EU priorities in its neighborhood, notably its Eastern neighborhood. Finally, the workshop participants recommended that the document should focus less on al-Qaeda and acknowledge that terrorism does not only target Europe and the U.S. They stressed the need to consider giving some negative security guarantees, in order to deter some states from engaging in weapons proliferation; and they further encouraged following up the EU Security Strategy with specific Action Plans (with a regional focus) or policy papers on structural issues (such as aid and conditionality).[40]

The Paris workshop focused on the EU's global objectives, including the importance of effective multilateralism, preventive engagement, working through the United Nations, and the need to secure a UN mandate prior to military engagement in external crises. Discussion also covered the importance of the EU's engagement in the Balkans, the Mediterranean and the Middle East, and especially with Russia and its neighbours. The debate focused on the role of pre-emptive deployment, whether to pursue an EU seat at the UN Security Council, the role of future EU foreign policy high representatives, the link between enlargement and security, and the nature of the EU's cooperation with the U.S. and Russia. The participants encouraged Solana to stress the importance of the UN, both militarily and politically, and to emphasize the EU's unfinished role in the Balkans.[41]

Finally, the Stockholm workshop focused on capabilities and coherence of EU foreign policy. Participants here agreed that the price of non-coherence in Europe is unsustainably high (in CFSP), that civilian capabilities in Europe require further development, and that the EU needs to prioritize strategic partnerships. The debate revolved around how to finance security policy (whether more or better spending is necessary), how to better use the EU's diplomatic force and its delegations, what NATO's role should be, and the nature of the transatlantic relationship. The workshop recommended that the final ESS must emphasize the links between internal and external security, focus more on Russia, and pay tribute to the OSCE as an important partner for the normative dimension of foreign policy.[42]

In the period following the expert workshops and the adoption of the final draft, member states were also invited to provide input. According to some experts, the reason the ESS is vague on a number of points is because consensus could not be found amongst member states. Conversely, some issues were included in the ESS only because of potentially strong criticism if they had been excluded. The final draft was adopted by the European Council in December 2003, titled 'A Secure Europe in a Better World'[43]. At the time, governments recommended several priority areas for action (see below), but no specific deadlines or procedural instructions were presented.

Content

There are some notable differences in content between the first and second public drafts of the ESS, partly as the result of consultation with think-tanks. Most noticeably, the references to 'pre-emption' were removed to instead include 'prevention'. Furthermore, state failure and organized crime became separate entries in the list of key threats (while regional conflicts was added as a threat), and proliferation of WMD was downgraded from the 'single most important threat' to the 'potentially the greatest threat'. References to a new European defense agency were also softened, and a distinction between 'old' and 'new' terrorism was removed.

The ESS is a relatively short document with only 15 pages of text. After a brief introduction, the current security environment is detailed. Then, a discussion takes place on the EU's strategic objectives and the strategy concludes with a section on the policy implications for Europe. When discussing the security environment, the ESS distinguishes between 'global challenges' and 'key threats'. Global challenges include the security-development nexus, competition for natural resources, and energy dependence, whereas the five key threats identified by the strategy are terrorism, proliferation of WMDs, regional conflicts, state failure, and organized crime. The strategy presents three strategic objectives for the Union to defend its security and promote its values. These are: addressing threats through a mixture of instruments, building security in the neighborhood, and promoting an international order based on effective multilateralism. Finally, the strategy notes that the EU must become more active in pursuing its strategic interests, more capable, especially in terms of military capabilities, more coherent, by bringing together the various instruments and capacities, and better at working together with its partners, including the U.S. but also Russia and the rising powers in Asia, Africa and Latin America.

The ESS represents, for the first time, an explicit, overarching statement on the EU's external security perspective. Moreover, it is one of the more pithy policy statements ever made by EU governments. It managed to bring together 15 diverse governments to outline a set of shared goals in international affairs. It contains a common threat assessment, and agrees on principles for global action even if not stipulating specific steps forward or conditions for triggering EU involvement. The process leading to the ESS, and the ESS itself, must be judged a success by these criteria.

However, the ESS remains vague on a number of key points (as mentioned above, mainly because consensus could not be found). Moreover, some issues were included in the ESS only because there would have been strong criticism from abroad had they been excluded. Most noticeably, the ESS contains no meaningful statement regarding Europe's view on the nature of transatlantic relations (especially on whether approval should be given to non Security Council-mandated military interventions by the U.S.) or on the degree of independence of the EU as an international actor.

Some analysts have challenged the claim that the ESS represents a 'real security strategy'[44]. They argue that while a strategy typically defines goals and sets priorities for policy objectives, and describes the means to be used and under what conditions they will be used, the ESS contains goals without setting any priorities. Furthermore, regarding means by which to implement the strategy, the ESS lists some tools but does not elucidate under what conditions these will be applied[45].

Effects on Outcomes

By most accounts, the practical effect of the ESS has been limited. Originally intended to be a 'living document' subject to subsequent revisions, the ESS contains no mechanisms for review or evaluation of the strategy. When endorsing the ESS at its December 2003 meeting, the European Council decided that a follow-up up should focus initially on four priority areas for implementation: 'effective multilateralism' with the UN at its core, terrorism, the Middle East and Bosnia-Herzegovina. In this regard, a number of strategies and policies, including the European Neighborhood Policy, the EU Counter-terrorism Strategy, and the strategy on WMD proliferation were subsequently adopted (but not all related directly to imperatives contained in the ESS). It is even more difficult, as noted in the next section, to assess the effects of the ESS on actual EU policymaking and resource allocation. With regard to the policy implications outlined in the ESS, it is difficult to assess how much more 'active', 'capable', and 'coherent' the EU is today compared to how it was in 2003. The effects of the Lisbon Treaty, including the creation of the External Action Service and the position of foreign policy High Representative/Vice President, may have significant bearing on the influence of the ESS, but these developments are too recent to fully assess their impact.

ESS Review (2008)

Situational and Historical Context

As discussed above, the ESS was never intended to be a static document. In the years following the adoption of the Strategy in 2003, a number of key developments took place, both within the Union and abroad. One particularly important development was the enlargement of the EU, from 15 to 27 member states, in 2004 and 2007. One rationale for reviewing the ESS was to enhance these new members' sense of ownership of the document.[46] Another argument for reviewing the strategy was to update it in light of the evolving security environment. In particular, Russia's role in its regional zone of interest was seen as troubling by many EU states, who wanted the new strategy to take a harsher stance toward Russia. The debate around Russia intensified following the Russian-Georgian conflict in August 2008. Similar to the process in 2003, individual personalities played a major role in pushing for revision. Sweden's Carl Bildt and France's Nicolas Sarkozy were especially supportive of revising the ESS. In addition to inter-state warfare in Europe's neighborhood, the emergence of post-modern security threats such as the possibility of a global pandemic, climate change and the global financial crisis – all of which the ESS said little or nothing about – prompted arguments that a revision was necessary.

Not all governments agreed on the need to revise the strategy, however. Some countries, including Germany, feared that reopening the ESS would unleash an uncomfortable debate about Russia, creating or even reinforcing divisions between new and old member states. Other concerns included

the risk of the ESS being watered down into a less successful product and that rewriting the ESS would hamper efforts to approve the Lisbon Treaty. Finally, some countries had reservations about Solana's drafting method (e.g. a small team and revision by a committee of member states), and concerns about the breadth of a drafting mandate.[47] In fact, Solana himself appears to have been reluctant to update the ESS for fears that the policy climate was not conducive to such an undertaking.

The European Council finally agreed on a compromise: to write an 'Implementation Report' on the ESS. Such a report would not replace the ESS, but rather examine how it has fared in practice, and discuss what more needed to be done. For the sake of simplicity, and with some caveats discussed below, this paper refers to the Implementation Report as the 'ESS Review'.

Process

The drafting team for the ESS Review was slightly larger than the initial ESS process. It included several Commission representatives and a similar mix of practitioners and experts. Similar to the 2003 process, a number of high-profile seminars hosted by the European Union Institute for Security Studies (EU ISS) were held during the latter half of 2008. Rome (5-6 June) provided an overview of the security environment, Natolin (27-28 June) focused on the neighborhood, Helsinki (18-19 September) focused on ESDP, and Paris (2-3 October) focused on EU strategic considerations.

However, the drafting process suffered from a lack of political will to review the ESS. Unlike the 2003 process, the institutional expert groups in 2008 lacked a draft from which to work, and therefore discussions lacked focus. Workshop topics were broad and unwieldy. The absence of member state consensus on both the need to revise the ESS and the nature of the current security environment undermined meaningful debate, both in the workshops and in the broader policy community. As a result of these impediments, the role of think-tanks in the revision process proved to be less influential than in 2003. Recommendations were wide-ranging and lacked specificity, resulting in fewer recommendations being adopted in the final document. Doubts again surfaced as to whether the EU had an adequate platform, and process for discussing and debating strategic questions.

Nevertheless, the ESS review process was completed and the 'implementation report' endorsed by the European Council on 12 December 2008 as the 'Report on the Implementation of the European Security Strategy'.

Content

At first glance, the two documents – the 2003 ESS and the 2008 Implementation Report on the European Security Strategy – look quite similar. They share similar titles and follow roughly the same structure. However, the Implementation Report[48] should not be confused as a revision or update of the ESS. The ESS Review did manage to slightly expand the scope of the threats to include non-strategic threats such as cyber-security, climate change, and pandemics. By some accounts, this expansion was driven not just by functional realities, but also by the fact that different departments within the Commission (allowed a greater role in the 2008 ESS Review) pushed 'their' respective threat. Furthermore, the implementation report included a broader inventory of tools and resources as the means by which the EU could pursue security goals.

On the other hand, the report offers neither guidance as to the kind of situations where military instruments may be called upon nor does it acknowledge the considerable difficulties facing the pursuit of security policy in the EU, not least regarding issues of institutional coordination. It offers few concrete recommendations for change and does not, despite loud criticism following the 2003 ESS, include any mechanisms for follow up and review. As such, the implementation report cannot be described as a 'strategic review' in the sense that it does not assess effectiveness, address the interaction between sub-strategies, policies and actions, or define the EU's foreign policy priorities.

Whereas the ESS considered terrorism a top priority, the ESS Review lumps terrorism together with organized crime. WMD proliferation, however, has been upgraded to a top priority again. Another notable change between the ESS and the ESS Review is that 'failed states' and 'regional conflicts' have been replaced by 'energy security' and 'climate change'. At the same time, the ESS Review offers little advice on prioritization of threats. When it comes to 'preventive engagement' the ESS report uses the same language as the ESS, but also lists sanctions, diplomacy and aid as tools. It also reiterates the importance of multilateralism and stresses partnerships.

It is also interesting to note that the ESS implementation report does not make a reference to a European 'strategic culture' or 'security culture' but instead introduces the concept of 'human security'. Some experts have interpreted this shift in language as an indicator of the EU moving away from its great power ambitions, as outlined in the ESS, and/or downplaying the importance of the transatlantic relationship[49].

Effects on Outcomes

The ESS Review notes that the ESS remains a work in progress and that the EU still needs to become more capable, coherent and active international actor in order to implement the strategy. While the ESS Review covers a wide range of threats, some member states have been reluctant to discuss threats such as energy and climate change, fearing the ill-effects of 'securitizing' EU policies in these areas. It still remains to be seen to what extent the new External Action Service and the High Representative/Vice President will facilitate new strategic-level debates.

One positive note is the EU's move towards achieving an aim highlighted in both the ESS and the ESS Review: the formation of strategic partnerships with rising powers. For instance, High Representative/Vice President Catherine Ashton visited India in June 2010 in an effort to boost and institutionalise relations with that country. EU's attempt to establish strategic partnerships with other developed and developing countries around the world, however, is still very much an ongoing process.

Patterns and Policy Recommendations

This brief analysis of the ESS and the ESS Review reveals some common patterns in terms of the context in which each strategy was initiated, the process through each strategy was formulated, the key concepts and substance of each strategy, and the effects on action and outcome.

Situational and Historical Context: Both strategies were initiated at a time of uncertainty, and even insecurity, about the future of European security cooperation. The initiation of a strategy was

seen largely in terms of procedural benefits: bringing governments together to affirm a common set of concepts and principles. The actual effect of the strategy (see below), or a desire to change the course of European security action, were secondary to the act of agreeing on a common policy.

Process: Both strategies were created (and, in the case of the ESS, revised) in elite-led, insular processes. This stems from the perception that achieving agreement among 15 (and then 25/27) national governments requires a closed process. An exception can be found in the original formulation of the ESS, when Solana's team organized a series of topic-specific seminars in cooperation with European think-tanks. Most indications confirm that the results from those sessions were fed into the formulation process in a meaningful way. That model of practitioner-academic interaction succeeded rather well (although was given less of a priority in the ESS Review). Also the model of circulating a draft text during the ESS drafting process was deemed successful.

Content: The content of both strategies reflects the need to reconcile many different national positions. For the ESS, this is apparent in the use of broad, encompassing, and sometimes rather vague formulations of threats and principles, as well as a lack of precision in describing when the EU is likely to act and with what instruments. The documents are rather short on details and imperatives, which in turn undermine the impact of each strategy. On a positive note, the ESS has much in common with the recent U.S. National Security Strategy in terms of threat assessment and a focus on multilateralism. Such commonalities should provide stepping stones towards more coordinated security strategies in the future.

Effect on Outcomes: The effect of each strategy on actual outcomes (policy, budgets, and behavior) is difficult to measure, and the ESS has not been in existence long enough to make an informed judgment. Thus far there is little evidence to show that the ESS has led to significant policy reforms, increased budget, or renewed energy for certain missions or actions. On the contrary, there is a widely perceived slowdown in momentum for the CSDP (Common Security and Defense Policy, formerly the ESDP), for example.[50] Much of this has to do with Europe's preoccupation with the implementation of the Lisbon Treaty which may give renewed impetus to the ESS and possibly lead to a revision. The new High Representative, and External Action Service, requires more strategic guidance than ever before as it takes shape with unclear capacities and aims.

Recommendations

The purpose of the preceding analysis was to improve understanding of European Union-level strategic review processes, with the aim of improving transatlantic coherence on security questions. This analysis suggests areas where improvements can be made toward that end.

1. When future strategic reviews are initiated, utilize think-tanks in the U.S. and EU to cultivate transatlantic links. Those links can provide the foundation for policymakers to meet and discuss commonalities, shared perspectives, and possible obstacles to strategic coherences. When bringing in outside experts, it may be wise to circulate a 'straw-man text' providing a base for discussions.

2. In advance of reviewing their respective security strategies, EU and U.S. officials should each consider floating a 'transatlantic white paper' to pre-identify key transatlantic issues that can be discussed and fed into their respective strategies.
3. Build a more structured transatlantic venue for the discussion of strategic concepts, principles, and priorities. Currently there are few venues for strategic thinking outside of NATO. A new venue (a council, 'dialogue', or the like), perhaps along the lines of the EU-U.S. summit process, could be designed to facilitate broader security discussions and forge common views between the U.S. and EU.
4. The previous recommendation is predicated on the need for the EU to build its own strategic debate forum. On the European side, there are few European level venues for considering strategic questions. A 'strategic culture', along with government officials charged with strategic thinking, has yet to emerge at the European level. An annual European security conference, to advise a group of EU-level policy advisors dedicated to long-term planning, could be initiated.
5. Create a review process as a way to translate security strategies into tangible policy steps and then to evaluate progress on a regular basis. Such a process would go a long way towards rectifying the current problem of strategy-making as a process in and of itself, typically with little or no follow-up.

THE 2010 NATO STRATEGIC CONCEPT

Stefano Silvestri, *President, IAI*, and Alessandro Marrone, *Researcher, IAI*

Historical Context

The NATO Strategic Concep2t (SC) is the main document providing political and operational guidance to the Alliance. The most current SC was adopted at the Lisbon Summit in 2010, while the previous one dated back to 1999. Throughout NATO's history the Alliance has adopted Strategic Concepts at irregular intervals, when NATO members became convinced that major internal or external strategic changes required them to undertake an urgent – albeit complex and sensitive – political process. .

The international system has recently seen the emergence of new powers such as China and the re-emergence of old ones like Russia. Globalization has encouraged a redistribution of economic power but a corresponding effective global governance structure has not yet been created. This underlying international development affects many issues which NATO must address ranging from relations with Russia to international crisis management.

The greatest shock was the 2001 terrorist attack against the U.S., which caused the activation of the Article 5 provision by the Alliance for the first time in its history. In the years following, the NATO intervention in Afghanistan has become by far the largest Allied operation in terms of troops deployed, casualties suffered and prolonged military efforts. The operation has also had a deep impact on the Alliance's capabilities, finances, organization and doctrines.

Since 1999, NATO has enlarged its membership to 13 Central and Eastern European countries. This process, together with EU enlargement, has contributed to peace and stability in Europe but also has had a complex impact on the Alliance. The expansion of member nations from 15 to 28 required the Alliance to seriously consider more national security priorities and threats, and, due to different threat perceptions among NATO members, it is more difficult to achieve a common vision and strong Alliance cohesion. The war between Russia and Georgia in 2008 signalled a less benign European security environment which influenced the security perceptions of the new Eastern European NATO members and underscored the need to enhance strategic reassurance among some NATO members vis-à-vis Russia. However, other member states would have rather devoted additional NATO energies and efforts to out-of-area operations.

A fundamental part of the strategic review context is the current status of transatlantic relations and relations between NATO and the EU. In the latter case, the nature of the two organizations remains very different, as do their respective political mandates despite the fact that 21 states are members of both organizations. Nevertheless it seems that a certain degree of compatibility is emerging, particularly within the framework of complex operations and with the so-called "comprehensive approach," as the EU has a wider set of policy tools to address contemporary threats and challenges. On the ground, a pragmatic cooperation often takes place where EU and NATO missions are deployed together, for example in the Gulf of Aden and in the Western Balkans. However, there are problematic political dimensions due to the different membership composition of the two organizations—for example, Turkey is a member of NATO but not the EU and the Republic of Cyprus is a member of the EU but not NATO with both countries preventing the two organizations from working together. Unfortunately, these issues simply cannot be resolved by officials who are implementing operational requirements. On a positive note, the reinsertion of France in NATO's integrated military command has contributed to improved relations between Americans and Europeans and between the two organizations, after the tensions that occurred during the Iraq crisis subsided.

Another important change in the security environment is the increasing importance of new threats such as cyber attacks. Beyond the 2007 Estonian case, a number of examples have prompted cyber-security to be placed as a top NATO priority, and the Alliance is establishing structures and instruments to deal with this new threat. The EU has similar concerns on cyber security, though considered strictly related to internal security[51].

Finally, the U.S. appears to be less interested than in the past in European security per se and more interested in having an effective European contribution to global security issues: a challenge that the Europeans are still debating. Meanwhile, European countries are reducing their defense budgets in order to reduce the amount of sovereign debts accumulated over the past decade. Therefore, the effect on NATO will be an overall reduction of the defense resources available and a widening of the transatlantic defense capabilities gap since very few European countries in 2010 spend more than 2% of their GDP on defense (some NATO members spend less than 1% GDP), in comparison to the 4.3% that the U.S. spends on defense. This has a direct impact on NATO capacities, finances and ambitions, as well as on transatlantic solidarity, which undermines the possibility of significant burden sharing.

As a whole, the international security environment seems to be less benign and more complex today than in 1999, making it more difficult to forge a solid transatlantic consensus on NATO's role.

Process

While all Strategic Concepts have been approved by the North Atlantic Council (NAC) at the level of Heads of State and Government, there is no legal or institutional template which defines the NATO strategic review process, and which actors and bodies must be included in the process.

Traditionally, the strategic review involves a complex set of political, diplomatic and bureaucratic negotiations. Subject to NATO's functioning and rationale, this process does not happen in a vacuum,

rather it draws from the daily work of negotiations in various NATO committees, past adopted practices and previously released communiqués. To a certain extent, the strategic review process codifies past decisions and activities and organizes NATO's evolution into a new, coherent and overarching document.

Since the 1990's, possibly because external threats were less evident and compelling, the elaboration of the SC has become more of a political exercise than a military one, dealing with the redefinition of core tasks, institution building, enlargement, and partnerships. In contrast, strict defence planning draws less attention. Thus, the political-diplomatic structure of the Alliance has increased its role in the elaboration of the SC. The "public diplomacy" character of the process has gained more and more importance in the last two decades.

The 2010 strategic review has been further modified, if compared with 1999. Rather than beginning negotiations directly within the NATO structures, the NATO Heads of State and Government approved the concept that a Group of Experts appointed by Secretary General Anders Fogh Rasmussen would offer advice and insights on the new Strategic Concept to NATO. Former U.S. Secretary of State Madeleine Albright chaired the Group, which included diplomats and experts from the private sector and academia. Working in close coordination with the Secretary General, the Group organized several seminars with officials from NATO and member states, relevant stakeholders and members of the transatlantic defense policy community. The Group presented its report "*NATO 2020: Assured Security; Dynamic Engagement*" to the NAC in May 2010[52].

Following the presentation of the Expert's report, the strategic review process was led by the Secretary General[53]. First, he consulted the member states directly to collect and solicit feedback on the Group's report. Second, he wrote a draft of the SC and discussed it with the NAC at the level of Defense and Foreign Affairs Ministers where he received general approval and further input. Finally, in November 2010 the NATO Heads of State and Governments approved the new SC "*Active Engagement, Modern Defence*"[54]. Broadly speaking, the final document had been largely drawn from the work done by the Group of Experts, underlining the significance of this innovative procedure.

NATO's military committees were also consulted and had been involved in the strategic review through consultations by the Group of Experts and the Secretary General, and they publicly outlined their proposals on the 2010 SC and the future of NATO. Also, other Alliance bodies have adopted a proactive role: the NATO Parliamentary Assembly, for example, released a set of proposals and recommendations regarding the Strategic Concept[55].

Overall, the 2010 process was more inclusive than in the past. In fact, the Group of Experts involved a large portion of the transatlantic defense community, including not only diplomats and military personnel but also academics, and individuals from think tanks and the private sector. In addition, partners such as the EU had the opportunity to provide input to the Alliance's strategic review. Moreover, the process increased NATO's transparency with respect to the wider public and used information sharing technology, such as a dedicated official NATO website.

This thorough and inclusive process had three main purposes. First, it improved the quality of the Strategic Concept through the gathering of new ideas and external contributions from a wider range of policy actors. Second, it strengthened the practice of "consensus building" by involving national polities at the initial phase, and reduced disagreements among member states also at this initial stage.

This consensual process allowed for early support for the SC's preliminary findings which facilitated the final approval of the SC and avoided difficult last-minute negotiations.

Finally, the process produced a more durable result in terms of "public diplomacy." Out of area operations, particularly in Afghanistan, with great costs both in personal sacrifice and treasure, have eroded positive public opinion regarding NATO. The economic crisis and the increasing weight of public debts also negatively impacts the level of NATO member's defense spending. The Alliance's *raison d'être,* which was existentially straightforward when Soviet troops threatened Western Europe, has become less and less evident in the current situation where the fundamental NATO goal of Europe whole, free and at peace has been almost achieved. The new Strategic Concept process attempted to increase domestic consensus in favour of the Alliance, demonstrating NATO's openness and transparency. This public diplomacy effort also has a positive "external" dimension, aimed at potential partner and third countries, particularly Russia and the Middle East, which project an image of NATO as security provider rather than as a risk or threat itself[56].

In fact, this process is not an absolute novelty. Interestingly, the NATO strategic review had *de facto* replicated the EU practice, involving relevant stakeholders in the drafting of European directives and regulations from the very beginning.

Content

While the 1999 SC was meant to justify NATO out of area operations in its new role as global security provider, the 2010 SC aimed to strike a balance between a pro-active posture, including operations and partnerships and the Alliance's traditional core task of collective defense.

The 2010 SC presents some similarities and some innovative thinking with respect to the 1999 document, as it attempted to balance different priorities and formulate strategic guidelines in an evolutionary rather than revolutionary way.

First, the document redefines the Alliance's "*core tasks.*" Collective defense is the first task listed in the SC, reinforcing the very *raison d'être* of NATO established in the Article 5 of the Washington Treaty and re-stated by every Strategic Concept, including the 1999 and 2010 ones. Yet the newest SC renews its affirmation that "*NATO will deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or of the Alliance as a whole.*"[57] This formula intentionally allows NATO leaders to include, on a case-by-case basis, new security threats under the Article 5 umbrella. For example, the capability to defend member states against ballistic missile attacks is defined in the SC as a "*core element of our collective defence*"[58]. Also cyber attacks represent another emerging security challenge included in the SC priorities, and it is recognized that core NATO defense tasks include the development of capabilities intended to defend member states and Alliance structures against cyber attacks.

A second core task outlined in the Strategic Concept is crisis management. This innovation with respect to the Washington Treaty was introduced in the Alliance's strategy by the 1999 SC when NATO initiated the first out-of-area operations in the Balkans and has been retained by the 2010 document. This core task not only includes crisis management and prevention, but also stabilization

operations and support for reconstruction in post-conflict situations. The scope of out of area operations is broadened when taking into account the kind of mission NATO is currently managing in Afghanistan.

The last NATO core task established by the 2010 SC is "*cooperative security.*" Under this broad definition, cooperation and partnership activities are re-introduced as Alliance tasks (first included in the 1999 SC) and have risen in importance in the last decade. Cooperative security also includes the continuation of the "*open door policy*" (the further expansion of NATO membership), disarmament, arms control and non-proliferation. The inclusion of these policies among the NATO core tasks enhances their importance in the Alliance's strategy but does not necessarily imply radical changes in NATO's rationale and management of these challenges. For example, any enlargement decision must be approved on a case by case basis by the NAC.

However, possibly the greatest innovation of the new SC is its format. First, it is a relatively brief document compared to the 1999 one, narrowing its focus on a few fundamental guidelines and leaving a large part of the implementation provisions to the Declaration approved by the heads of state and government in Lisbon together with the SC. The thinking behind this strategy was that subsequent NATO Summits would elaborate on and update the existing Strategic Concept, while leaving the SC as unchanged as possible. It was believed that this method would provide the necessary flexibility to concretely adapt NATO strategy to changing circumstances, and avoid the possibility that an overly detailed or prescriptive Strategic Concept would become rapidly obsolete. Moreover a relatively short SC document makes it more easily read and reviewed by the general public, consistent with public diplomacy objectives.

Following the outlined core tasks, the SC provides a general assessment of the security environment. With respect to the 1999 SC, there was an implicit prioritisation of threats and risks that emerged; however, the lack of a more explicit prioritisation would have been difficult due to the requirement of achieving the unanimous consent of all 28 members.

The 2010 SC also specifies how NATO shall deal with each of its three core tasks. On defense and deterrence, a large part of the guidelines are traditional elements concerning NATO's military posture, such as conventional capabilities, nuclear deterrence, and the need for more expeditionary military forces. However, the goal to develop new capacities to deal with emerging threats, such as ballistic missile, cyber and terrorist threats is not new. Beyond the usual emphasis on comprehensive approach, the SC does take a new approach regarding crisis management as NATO seeks to develop an internal civilian capability, aimed to act as liaison with actors such as the EU, and to complement Alliance's military operations should other partners be unwilling or unable to act in support of NATO operations. Finally, on cooperative security, the most interesting new development arises from the decision to further develop partnerships, particularly in the NATO commitment to be "*open to consultation with any partner country on security issue of common concern*," and to give to operational partners a "*structural role*" in shaping the strategy and the decisions on common missions[59].

Overall, the main value of the new SC is that it takes stock of the changes that have occurred in the security environment since 1999, adapts and updates NATO tasks and posture. There is no dramatic break from the previous 1999 document; on the contrary, there is a clear effort to stress continuity. The emphasis on continuity is justified by two main reasons. First, diverging threat

perceptions among the Allies require the SC to strike a balance between "conservative" and "innovative" positions. This balance forges a kind of "*acquis atlantique*"[60], consolidated through previous strategic reviews, which weighs powerfully against any "new thinking" and avoids all risky, dramatic and contentious strategic shifts. Second, there is a strong "conservative" bias within all defense establishments which is found in their doctrines, structures and capabilities. Furthermore, the defense community is normally very reluctant to completely scrap older military capabilities and platforms, even if they appear of limited in their utility in present circumstances on the basis that it would be difficult if not impossible to rebuild them rapidly should a need for them re-emerge abruptly. The consequence of this mentality, however, is that new ideas and initiative have to carry forward the burden of the old, fighting for scarce resources and sometimes even adopting less than optimal strategies in the name of strategic continuity. That is why the new SC also has the appearance of a complex patchwork than the smoothness of completely coherent tissue. A case in point, but not the only one, may be the decision to keep tactical nuclear weapons based on the European territory.

Impact

The NATO SC, like the European Security Strategy, is a non-legally binding document adopted by consensus within an international framework. Although it is too early to reasonably assess the impact of the Strategic Concept approved on November, 2010, we have attempted to measure the effect of the 1999 strategic review. Traditionally, the Strategic Concept has played some role by providing political guidance for future decisions with the caveat that as far as security and defence are concerned. Therefore, the SC has a limited impact on the development and operations of NATO and an even more limited effect on member states. Because NATO and the EU remain strictly multilateral forums where decision-making is very different and distinct from unilateral, national processes, it is extremely difficult to measure the "net effect" of the strategic review as well as its success.

The 1999 strategic review has arguably influenced the Alliance' policies and posture in several ways, but it is difficult to measure how much as well as the existence of causal links between it and subsequent NATO operations and evolutions. In that sense, it appears more useful to assess five "likely" effects of the 1999 SC.

First, the 1999 SC performed a "consensus building" function among the Allies. The political compromises reached through the strategic review identified common ground among different national perceptions, priorities and agendas creating an *acquis atlantique*. However, the changes occurring in the international security scene—the enlargement of NATO and the impact of new strategic priorities—are challenging the old "*acquis*" and driving the need for a new consensus. Although single SC can deliver such a perfect result, the review process—begun in 1991 further developed in the 1999 and 2010 Strategic Concepts—has most likely helped to maintain the Alliance cohesion and permitted NATO to confront the necessary changes in an orderly and cooperative way.

Second, the 1999 SC has, to a certain extent, justified the old threats and challenges and prepared the way for the new, non-Article 5 and out-of-area operational challenges. The 1999 SC certainly has contributed in making the case for these new tasks of the Alliance which was almost unthinkable 20 years ago and quite contested 12 years ago, but finally included in the NATO core task by the 2010

SC. Despite important disagreements, for instance on Iraq, NATO unanimously agreed to embark on several out-of-area and non-Article 5 missions, such as the maritime operation Ocean Shield and the peace enforcing mission in Kosovo.

Third, the 1999 SC influenced the national security strategies of several NATO member states, particularly the smaller and newer countries. A European country with limited global projection and military capabilities may usefully shape its defence and security policy on the basis of NATO's concepts to better align its domestic assessment with NATO's strategic outlook. It may sometimes be just a "declaratory policy," but it suggests a process of "socialization" of the military, diplomatic and political national elites which is convergent with NATO interests.

Fourth, the 1999 SC performed a "public diplomacy" function, contributing to making the case for the continued relevance of the Alliance in the future. Moreover, one purpose of the SC was to create a new official narrative and demonstrate to NATO members' domestic audiences and non-NATO publics that NATO was placing greater emphasis on "cooperation," "partnership," "dialogue," "peace," and "security" in order to explain and support NATO's purpose, role and operations.

Fifth, the 1999 SC accompanied the structural changes and organizational developments of the Alliance. In 2002, the Allied Command Transformation (ACT) was established to lead the transformation of NATO's military structure, forces, capabilities and doctrines advocated by the SC. The new SC tasks NATO to "*engage in a process of continual reform, to streamline structures, improve working methods and maximize efficiency*"[61], thus "authorizing" the ongoing negotiations on the reorganization of NATO headquarters, commands, agencies, committees and structures, mainly aimed to cope with cuts in the member states' defense budgets. The Lisbon declaration on the implementation of the SC states that the Alliance will reduce its standing personnel in the headquarters by 35%, and NATO agencies will be reduced from 14 to 3. The only certainly that one can glean from the effect of the 1999 SC is that it had no effect on member states' defense budgets which continued to decrease despite the call for adequate military forces and resources.

Key Variables

This chapter will analyze four key variables which have influenced NATO strategic review in 2010: political leadership, institutional context, bottom-up pressure and public opinion.

Political Leadership

In 2010, political leadership played a fundamental role in initiating the strategic review. Undertaking this process is risky, because it forces actors to confront sensitive and uncomfortable issues. The NATO strategic review, like the EU and French ones, is not a periodical exercise to be undertaken at regular intervals, as happens with the American QDR. Therefore, the beginning of a strategic review largely depends on political decisions taken at the highest level of policy-making.

In the NATO case, deep divisions among member states caused by the war in Iraq made it almost impossible to undertake a common strategic review. Promising significant changes to U.S. foreign policy and emphasizing multilateralism, the election of Barack Obama removed an important political obstacle coupled with the electoral victories of German Chancellor Angela Merkel and French

President Nicolas Sarkozy also played a role in creating a transatlantic "rapprochement." In 2006 Chancellor Merkel declared that a new NATO strategic rethinking was necessary and in 2008 President Sarkozy made the decision to reintegrate France into NATO's integrated military command. As a result, the 2009 Strasburg-Kehl Summit Declaration on Alliance Security initiated and provided procedural framework for the 2010 strategic review.

Institutional Context

NATO's organization and the roles of its internal structures, such as the Secretary General and the NAC, have a significant impact on all its activities including the strategic concept. NATO works under strong intergovernmental control and strategic decisions are only taken within the NAC and by consensus.

The NATO Secretary General increased his role in the 2010 strategic review marking the first time that a Secretary General was in charge of drafting the SC which in the past had been primarily accomplished within NATO committees and particularly by the NAC. Nevertheless, the NAC remained the main decision-making body of the Alliance, and it made the final modifications to the SC draft during the meeting of Defense and Foreign Affairs Ministers. Later the Heads of State and Government gathered within the NAC format in Lisbon for the last word and final approval of the SC.

The Secretary General generally has less power than his counterparts in the European Commission. Because the position is unable to exert political pressure on its members, the NATO Secretary General's role depends mainly on his personal, political ability and leadership quality as he performs the role of secretariat which can exert only a limited role as chairman of the NAC as a consensus builder. In no case does the Secretary General have the power to force the NAC or an individual member states to perform a task it does not wish to do.

Bottom-up Pressure

NATO already began to deal with non-traditional security challenges during the 1990s by implementing out-of-area operations and establishing new structures well before the 2010 SC provided such guidelines. Examples of this include non-Article 5 operations in the Balkans and the establishment of a new NATO division on emerging threats prior to the inclusion of energy or cyber security as a challenge to NATO. Following the September 11 terrorist attacks, the evolution and transformation of NATO has been increasingly operational and mission-driven.

It was also widely recognized within[62] and outside of NATO that the Alliance had to take stock of its recent practices, lessons learned on the ground, as well as its doctrinal and organizational evolution. In that sense, the "bottom-up" pressure was a key variable for the 2010 strategic review because it created the need to initiate a strategic review and provided part of the content of the new SC. For example, the experience in Afghanistan ensured that stabilization operations and reconstruction support would be part of the 2010 SC as they fall under the "crisis management" section as core tasks.

Within a crisis management context, a comparison can be made between NATO and the EU. On the one hand, the two organizations work in similar ways: there is a "mission creep" dynamic from

past or present tasks which create the need to undertake further missions. For the EU, the "neo-functionalist" theory explains how the tasks connected to the single market goals would push for further European integration. For NATO at the end of the Cold War, the Alliance expanded its tasks and its areas of interests, reaching a range of activities never dreamed of in 1949. On the other hand, the process is different. In the EU framework the EC launches top-down initiatives through "*white paper*," directives, strategies, institution building, which later on became part of the Community "*acquis*," also through a constant update and upgrade of the treaties. In contrast, at NATO the pressure comes mainly from the need to tackle new and unexpected security crises or challenges—from piracy in the Gulf of Aden to cyberattacks against member states—which in turn lead to new NATO missions, operations and structures before the codification in the Alliance's official strategy. Moreover, NATO has never modified the 60 year-old provisions of the Washington Treaty. The Washington Treaty remains a very short and simple document with NATO relying on SCs and its political leadership to steer its evolution.

Public Opinion

The last key variable to consider is public opinion in NATO member states. This is not to say that European or North American public opinion have directly shaped the 2010 SC as there is little interest in NATO strategy among the wider public. It is exactly this lack of interest and the corresponding scarcity of support to NATO military operations and member states' defense policies that represents a key variable. Indeed, one of the reasons NATO carried out the latest strategic review in a more open way was to reach out as much as possible both to the security policy community and to the general public. This has largely influenced the content and the language of the 2010 Strategic Concept as well as its length.

Recommendations

In the light of the previous analysis, it is possible to draw some policy recommendations aimed at improving cooperation between NATO, EU and member states in Europe and North America with particular regards to the actions the EU can undertake in the near future.

Doing a European Strategic Review

The EU should undertake a new strategic review of its security and defense policy. This review is necessary to take stock of the changes which have occurred in the security environment, the evolution of EU to include its enlargement and the approval of the Lisbon Treaty, and the strategic security reviews carried on by France, the U.S. and NATO after the ESS was released in 2003. Security strategies have become more important as the strategic environment gets more complex and the need for international cooperation grows while available resources are constrained.

The creation of a new ESS should be aimed to fulfill four tasks which the 2010 SC pursued regarding NATO: 1) build consensus among member states on the EU's role in the security field; 2) provide guidelines for the evolution of EU security and defense policy; 3) encourage the convergence of national security strategies; 4) improve domestic public opinion perceptions of the EU at home and in third countries through public diplomacy. The public diplomacy goal should be secondary with

regards to strategic prioritization. The contested issues have to be discussed among member states, because a "hollow consensus," (meaning a few EU member states feel strongly about an issue and push for an outcome while other member states either do not express an opinion or care about the issue but "go along" from a political standpoint) does not help strengthen the EU's foreign and security policy. In order to fulfill these goals, the strategic review should receive a strong political mandate by the EC, the Council and the European Parliament, and these institutions should maintain their full involvement during the process. The EES should also adopt an open and inclusive process, including the appointment of an *ad hoc* group of experts.

In addition, a new ESS would hopefully clarify an EU vision on several security issues and facilitate cooperation with counterparts such as NATO or the U.S. on issues of common interest. A specific part of the new ESS should be focused on relations with NATO, as the 2010 SC does with the partnership with the EU, in order to define the Union's policy towards the Alliance and provide new impetus for cooperation.

Building up a Better EU-NATO Strategic Cooperation

Better EU-NATO strategic cooperation should be pursued as the two institutions not only share the same values but they also share 21 member states, 21 sets of armed forces and taxpayers. So far there has been no satisfactory coordination at the highest level between the two institutions. Improved cooperation should be employed on a range of activities where the complementary nature of the two organizations would facilitate a cost-effective and comprehensive approach. This implies more regular participation of each organization's representatives in each other's committees at various levels, where security issues of common interest are debated; deeper communication and exchange of views between the two military staffs, also through enhanced liaison offices[63]; and more coordination with regards to crisis management, in terms of prevention, intervention and post-intervention.

The 2010 SC welcomes an active and effective EU, as well as the entry into force of the Lisbon Treaty, while recommending the fullest involvement of NATO members which are not EU members in the efforts to address common security challenges[64]. It also pledges NATO to work to "*strengthen the strategic partnership with the EU, in the spirit of full mutual openness, transparency, complementarity and respect for the autonomy and institutional integrity of both organizations*"[65]. Such an approach by NATO, underlined by the invitation of the President of the EU Council to the NAC meeting in Lisbon, paves the way for better EU-NATO strategic cooperation but the institutional partnership needs concrete follow-up actions.

Having Closer Coordination between High Representative/VP and Secretary General

The two leaders responsible for security and defence policy, namely the EU High Representative and the NATO Secretary General, play important, if different, roles within their respective organizations in fostering cooperation among the two institutions.

Complete implementation of the Lisbon Treaty, including the establishment of the European External Action Service (EEAS) and the inclusion of the European Defence Agency (EDA) in the EU institutional framework, represents an opportunity to improve the EU's common security and defence policy (CSDP). At the same time, the current NATO Secretary General is very interested in

strengthening cooperation with the EU and particularly with the High Representative with the full approval of NATO expressed in the Lisbon Declaration. Productive meetings between Secretary General Rasmussen and High Representative Ashton have already taken place in 2010. As a result, it is feasible to seek closer coordination between the two individuals as a foundational element for better cooperation between the EU and NATO.

Riding the Bottom-up Pressure

The EU and NATO should undertake common strategic reviews of the operations they carry on in the same theatre. Putting aside the most problematic example represented by Afghanistan, the EU and NATO deploy anti-piracy maritime missions in the Somali basin and peace-keeping/peace building missions in the Balkans. At the operational level, more cooperation is likely to unfold based on the urgency of saving resources and avoiding duplication[66]. Moreover, the mantra of a comprehensive approach provides the necessary rationale for increased coordination and cooperation between the two organizations. Particularly, the establishment of a modest civilian capability within NATO envisaged by the 2010 SC should become an opportunity to improve the communications and cooperation in this domain between the EU and NATO, and thereby avoiding the possibility of a new useless competition.

A joint EU – NATO strategic review of on-going operations would have two positive effects. First, it would improve the management of missions in the Balkans and in the Somali basin and contribute to their overall mission success. Second, cooperation on the ground between the two organizations would continue to improve[67], and useful lessons could be learned to improve cooperation at the strategic level. Both organizations should be responsive to the bottom-up pressures to fuel further evolutions at the strategic level in order to push for a better high-level cooperation.

Making a Joint EU-NATO Threat Assessment

The EU and NATO should manage a joint assessment of threats, risks and strategic priorities. This exercise has already been carried out between NATO and Russia as it has positively contributed to fostering strategic convergence in the very initial phase of a security policy, namely the identification of the threats to address. This positive effect should be, in theory, even greater between NATO and the EU.

While the EU continues to work out its own threat assessment, in line with the provisions of the Lisbon Treaty and the entry into force of the new assistance and solidarity clauses, the compatibility of a common approach with NATO is highly useful. Working jointly with NATO could deepen common understanding between the two organisations.

Exploring Cooperation on Internal Security

A potentially fruitful area of cooperation between EU and NATO is internal security. The EU has been increasingly involved in this field in recent years. The 2010 SC does not consider internal security as a NATO core task but includes terrorism and the disruption of vital communication in the ranking of security threats which are usually considered by the EU as internal security matters. NATO leadership also recognizes that it does not have the leading role on challenges affecting the internal security of the Alliance.[68]. This paves the way for a fruitful cooperation in internal security, as both the

EU and NATO are interested in the issue while their competencies and assets are complementary thus avoiding duplication. The EU is particularly well placed to take the initiative and lead common efforts in this field.

Removing Indirect Obstacles

An indirect but very tough obstacle to improving cooperation between EU and NATO is the disagreement between Turkey and Cyprus. As Cyprus is part of the EU but not of NATO and the opposite is true for Turkey, the long standing dispute among the two hampers practical and strategic cooperation between the two organizations. In fact, both countries slow down, limit and even halt opportunities for cooperation on several dossiers between the two organizations because of their bilateral stalemate[69].

The EU, NATO, North American and European member states should make an additional effort to resolve this dispute which is not only a problem *per se* for the Euro-Atlantic area but also a relevant obstacle for transatlantic cooperation on security issues. Meanwhile, pragmatic steps could be taken to ease the respective concerns on EU-NATO cooperation. The EU should negotiate a framework agreement with Turkey on Turkish cooperation in support of CSDP, including data sharing and Turkish participation in EDA activities. This would ease Turkish concerns on enhancing strategic NATO cooperation with the EU as Ankara would no longer perceive the intra-EU dynamics regarding CSDP as a "black box." In parallel, NATO should negotiate a similar agreement with Cyprus to ease its security concerns about the Alliance's activities and Turkey's role.

Notes

[1] The Goldwater-Nichols Department of Defense Reorganization Act of 1986, sponsored by Sen. Barry Goldwater and Rep. Bill Nichols, caused a major defense reorganization, the most significant since the National Security Act of 1947. Operational authority was centralized through the Chairman of the Joint Chiefs as opposed to the service chiefs. The chairman was designated as the principal military advisor to the president, National Security Council and secretary of defense. The act established the position of vice-chairman and streamlined the operational chain of command from the president to the secretary of defense to the unified commanders.
[2] "National Security Strategy of the United States, August 1991," *Federation of American Scientists*, [http://www.fas.org/man/docs/918015-nss.htm].
[3] "National Security Strategy of the United States, August 1991," *Federation of American Scientists*, [http://www.fas.org/man/docs/918015-nss.htm].
[4] 2002 NSS, 5.
[5] 2010 NSS, 20.
[6] Hillary Clinton, "Town Hall on the Quadrennial Diplomacy and Development Review at the Department of State," Washington, DC, July 10, 2009, [http://www.state.gov/secretary/rm/2009a/july/125949.htm].
[7] The terms were not settled yet, and the 2002 NSS mentions "a war against terrorists of global reach" (p. 5), "war against global terrorism" (p. 7) or "global war on terrorism" (p. 27) as well as "war on terrorism" in several instances.
[8] Scott Wilson and Al Kamen, "'Global War On Terror' Is Given New Name," *Washington Post*, March 25, 2009.
[9] 2010 NSS, p. 20.
[10] 2010 NSS, p. 27.
[11] 2010 NSS, p. 18.

[12] Cabinet Office, "The National Security Strategy of the United Kingdom. Security in an interdependent world," March 2008, p. 41.
[13] 2010 QDR, pp. 9 ss.
[14] CSIS Commission on Smart Power, *A Smart, More Secure America*, November 6, 2007, [http://csis.org/files/media/csis/pubs/071106_csissmartpowerreport.pdf].
[15] Gordon Adams, "Assessing the QDR and 2011 defense budget," *Bulletin of the Atomic Scientists*, 2 March 2010, [http://www.thebulletin.org/node/8325].
[16] 2002 NSS, p. iv.
[17] 2006 NSS, p.44.
[18] National Commission on Terrorist Attacks Upon the United States, *Final Report*, July 22, 2004. The position was eventually established by the Intelligence Reform and Terrorism Prevention Act passed the same year.
[19] 2002 NSS, p. 30.
[20] 2002 NSS, p. 7.
[21] 2002 NSS, p. 29.
[22] 2002 NSS, p. 29.
[23] 2010 NSS, p. 14.
[24] 2010 NSS, p. 14.
[25] 2010 NSS, p. 14.
[26] Adm. Mike Mullen, "Strategic Communication: Getting Back to Basics," *Foreign Policy*, August 28, 2009, [http://www.foreignpolicy.com/articles/2009/08/28/strategic_communication_getting_back_to_basics].
[27] 2010 NSS, p. 11.
[28] 2002 NSS, p. 34.
[29] 2010 NSS, p. 9.
[30] 2010 NSS, p. 22.
[31] Another strategic statement from the EU pertains to the 'Internal Security Strategy' agreed in March 2010, the first of its kind and a possible corollary to the U.S. Homeland Security Strategy. For reasons of space constraints, however, we will not include the ISS in this particular study.
[32] Bailes, Alison (2005) 'The European Security Strategy: An Evolutionary History' SIPRI Policy Paper No. 10. [http://books.sipri.org/files/PP/SIPRIPP10.pdf].
[33] As was for instance done by Wim van Eekelen, a prominent member of the convention and former WEU Secretary-General.
[34] Biscop, Sven (2004) 'The European Security Strategy: Implementing a Distinctive Approach to Security', Royal Institute for International Relations, Brussels [http://www.eu-ldc.org/downloads/conference%202004/Session%204/biscop_paper.doc].
[35] Biscop, Sven (2004) 'The European Security Strategy: Implementing a Distinctive Approach to Security', Royal Institute for International Relations, Brussels, page 7. [http://www.eu-ldc.org/downloads/conference%202004/Session%204/biscop_paper.doc].
[36] Toje, Asle (2005) 'The 2003 European Union Security Strategy – a Critical Appraisal', *European Foreign Affairs* Review, 9 (1), 117:134.
[37] Biscop, Sven (2004) 'The European Security Strategy: Implementing a Distinctive Approach to Security', Royal Institute for International Relations, Brussels, Page 4. [http://www.eu-ldc.org/downloads/conference%202004/Session%204/biscop_paper.doc].
[38] Biscop, Sven (2004) 'The European Security Strategy: Implementing a Distinctive Approach to Security', Royal Institute for International Relations, Brussels, page 4. [http://www.eu-ldc.org/downloads/conference%202004/Session%204/biscop_paper.doc].
[39] (Presidency Conclusions, Thessaloniki European Council, 1 October 2003)
[40] Minutes from the seminar [in French] "Strategie de Securite de l'Union Europeenne" 2003 [http://www.iss.europa.eu/fileadmin/fichiers/pdf/seminars/ESS_seminar_reports/report-Rome.pdf]
[41] Minutes from the seminar [in French] "Strategie de Securite de l'Union Europeenne" 2003 [http://www.iss.europa.eu/fileadmin/fichiers/pdf/seminars/ESS_seminar_reports/report-Rome.pdf]
[42] Minutes from the seminar [in French] "Strategie de Securite de l'Union Europeenne" 2003 [http://www.iss.europa.eu/fileadmin/fichiers/pdf/seminars/ESS_seminar_reports/report-Rome.pdf]

[43] Council of the European Union "A Secure Europe in a Better World, European Security Strategy" December 12, 2003 [http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf].
[44] Toje, 2005
[45] Except in the case of failed states, where the strategy mentions that military instruments should be used to restore order.
[46] This is despite the fact that all candidate countries were involved in the 2003 drafting process.
[47] The instructions from governments to Solana in December 2007 were lukewarm, at best: 'Examine implementation of the ESS, and if necessary, ways to complement it'. According to Biscop, 'this caution betrays a lack of confidence on the part of the Member States in the strength of the EU's – and thus their own shared – strategic culture…' Biscop, Sven (2009) 'Odd Couple of Dynamic Duo? The EU and Strategy in Times of Crisis'. *European Foreign Affairs Review*, 14, 367-384.
[48] Council of the European Union. "Report on the Implementation of the European Security Strategy: Providing Security in a Changing World." Brussels, December11, 2008.
S407/08 [http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf].
[49] Toje, Asle (2010) 'The EU Security Strategy Revisited: Europe Hedging Its Bets', *European Foreign Affairs Review*, 15(1): 171-190.
[50] For a helpful overview of the state of play of the CSDP, see Greco et.al. (2010) 'EU Crisis Management: Institutions, and Capabilities in the Making', Istituto Affari Internazionali, Paper No. 19.
[51] This issue is assessed by UI's paper. Noticeably, the EC has financed through the Framework Programmes researches on protection of critical infrastructure, border control and maritime security.
[52] NATO Group of Experts, "NATO 2020: Assured Security; Dynamic Engagement" 2010.
[53] Private talks with officials at NATO HQ, Brussels, October 2010.
[54] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[55] NATO PA, "Proposals and Recommendations for a New NATO Strategic Concept" 2010.
[56] Private talks with officials at the NATO HQ, Brussels, June 2010.
[57] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[58] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[59] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[60] It can be defined as a sort of un-contested political and strategic understanding, established through the six decades of NATO existence. See: Shea, J. "NATO at Sixty – and beyond," in *NATO in Search of a Vision,* eds. Aybet G. and Moore R. R. Georgetown University Press, 2010.
[61] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[62] Private talks with officials at the NATO HQ, Brussels, June 2010.
[63] The liaison office of the EU Military Staff at NATO Supreme Headquarter Allied Command Europe (SHAPE), in 2010 was composed only by 5 officials, which have to deal with thousands of NATO military official there.
[64] Noticeably, in 2010 Turkey has become the largest contributor in terms of military personnel to the EU operation Althea in Western Balkans although it is not a EU member.
[65] NATO "Strategic Concept—Active Engagement, Modern Defence" 2010.
[66] Private talks with officials at NATO HQ, Brussels, June 2010.
[67] Private talks with officials at NATO HQ, Brussels, October 2010.
[68] Private talks with officials at NATO HQ, Brussels, June 2010.
[69] Private talks with officials at NATO HQ, Brussels, October 2010.

ISSUE 2

THE INTERNAL/EXTERNAL SECURITY NEXUS

INTRODUCTION

Mark Rhinard, *Head of the Europe Program and Senior Research Fellow, UI,* and Erik Brattberg, *Research Assistant, UI*

A changing threat environment has set the context for new thinking about security in both Europe and North America. Global populations are more intricately linked through travel, trade, and communication technology, making societies more vulnerable to threats that once seemed distant and containable. Such threats, sometimes called "new" security threats, are new only in respect to the fact that they do not resemble traditional interstate military threats. Instead, they can originate in complex ways, cross borders with ease, and emerge with a certain sense of inevitability. It should be no surprise, then, that such threats have increasingly made their way onto security policy agendas, generally, and into security strategies, specifically. This has caused researchers and politicians on both sides of the Atlantic to reassess the strict separation of external and internal security goals embedded in structures, policies and practices.

This part will explore the strategic rhetoric and assess implementation in both the EU and the United States as well as on a transatlantic level. Each contribution takes up one pertinent "new" security issue (cyber security, biosecurity, pandemic influenza, and natural disasters) in order to outline the latest policy developments, analyze gaps and overlaps in either side of the Atlantic, and assess the prospects for improved transatlantic cooperation. Each paper will first present the threat perceptions, policies, and capacities and discuss the strengths and weaknesses in the approaches to the threat in the EU and United States, respectively. The papers will then turn to the transatlantic context, exploring common policies and strategies, existing cooperation mechanisms and operational aspects. Based on this summary, an assessment will be made regarding inadequate conceptual, institutional, policy and operational links between the EU and United States. Finally some recommendations for addressing shortcomings are provided.

The first section by Federica Di Camillo and Valérie Miranda of the Istituto Affari Internazionali (IAI) focuses on cyber security. It demonstrates that while U.S. and EU approaches to cyber security bear much in common, transatlantic cooperation needs to be stepped up. To this end, some different routes are suggested. First, a conceptual and semantic harmonization of cyber-related issues is felt particularly urgent as a preliminary step towards legal harmonization. Second, cyber security should be given higher priority and attention on the transatlantic agenda, not least through the creation of a U.S.-EU Cyber Security Council along the lines of the U.S.-EU Energy Council in the transatlantic summit process. Last but not least, transatlantic cooperation should be enhanced also at the

operational level, setting up for instance joint exercises between the concerned agencies or encouraging the exchange of best practices between the Computer Emergency Response Teams (CERTs) on both sides of the Atlantic.

The second section by Elisande Nexon and Jean-François Daguzan of the Fondation pour la Recherche Stratégique (FRS) takes on the issue of biosecurity. Outlining the latest developments in the EU and United States regarding biosecurity threats, the authors argue that both the EU and the United States hold similar threat perceptions and display compatible security apparatuses for such threats. Nevertheless, the transatlantic partners should adopt common definitions and terms of reference in order to improve communication and avoid misunderstanding, and carry out oversight of all the biosecurity outreach and cooperation initiatives and activities programs in order to improve coordination. Finally, they should recognize the importance of involving industrial and scientific communities in transatlantic initiatives and dialogues.

In the third section, Mark Rhinard and Erik Brattberg of the Swedish Institute of International Affairs (UI) examine whether the EU and United States are turning words into action on the issue of pandemic threats. In brief, the findings indicate that EU and U.S. strategic rhetoric on pandemic influenza is consistent and closely aligned. Most EU and U.S. cooperation takes place through the World Health Organization (WHO), where both sides have taken a leading role in new initiatives and motivating cooperation amongst recalcitrant countries. However, there is little direct U.S.-EU cooperation in the area of common policies or operational capacity sharing, beyond occasional exchange of experts. Recommendations include building relationships between EU health agencies, such as the nascent European Centre for Disease Prevention and Control (ECDC), and U.S. agencies, including the U.S. Centers for Disease Control and Prevention (CDC).

Finally, Rick "Ozzie" Nelson and Ben Bodurian of the Center for Strategic and International Studies (CSIS) look at large-scale natural disasters. Noting that these types of disasters defy categorization as isolated or contained events, because they often result from ongoing environmental change and can wreak havoc in places far removed from the centre of crisis, the paper examines how the United States and the EU have approached disaster preparation and response. It asks what the key documents that articulate strategies and plans to deal with large-scale natural disasters are? How successful have the United States and EU been in their efforts to implement these policies? And finally, how effectively have both entities worked together to plan for and respond to natural disasters? The authors finally offer some answers to these trenchant questions and highlights prescriptions for policy change including specific recommendations for boosting coordination and cooperation with third countries and international organisations.

CYBER SECURITY: TOWARD EU-U.S. COOPERATION?

Federica Di Camillo, *Senior Fellow, IAI,* and Valérie Miranda, *Junior Researcher, IAI*

Introduction

In the last 50 years, the world economy has become increasingly dependent on digital information infrastructure. Computers and the internet have transformed economies and given developed countries great advantages. However, these positive developments have come at a cost. Indeed, the more dependent our societies have become on Information and Communication Technologies (ICTs), the more vulnerable are they to digital threats. Cyber security has thus become an urgent and high-level policy problem, posing many pertinent questions.

First, cyber security, a relatively comprehensive term, includes multifaceted threats that, whether intentional or not, are difficult to identify.

Second, ICTs are a fundamental part of today's critical infrastructures, being on the one hand targets of attacks and/or accidents—as cyber-infrastructures—and on the other a means to hit other critical infrastructures, which rely on them (such as transport, including air traffic; energy grids; water supply networks; nuclear plants; banking and financial systems). It is therefore necessary to consider the multiplier effect they may entail.

Third, large parts of these infrastructures are transnational and are thus critical for more than one single state. This is why a coherent international (e.g. transatlantic, approach) is required. Moreover, from a functional point of view, the current interconnectedness of systems creates fundamental interdependences that allow vulnerabilities to spread. Such geographical and functional "domino effects" caused by systems' vulnerabilities have an enormous potential impact. This in turn is reflected by the high degree of responsibility attached to private and public agencies in charge of systems/infrastructure management.

The aforementioned geographical, functional and responsibility aspects confirm another key feature of the cyber sector; namely the blurring borders between internal and external security (including the borders between security and defence as well as between cyber security and cyber warfare) of both a country and a geographic area.

This paper intends to assess the initiatives undertaken by the European Union (EU) and by the United States in the cyber security domain. Our analysis will be conducted on three main levels. We

will first examine the EU and U.S. strategic rhetoric to consider to what extent it deals with cyber security-related issues. We will then proceed to the policy level to see whether and how strategic claims have been met. The following step will be to look at a selection of agencies and mechanism on both sides of the Atlantic to understand how policies have been translated into practice. The final paragraph is devoted to transatlantic cooperation. After identifying its strengths and weaknesses, we put forward selected proposals and policy recommendations to further enhance transatlantic cooperation on cyber security.

Cyber Security in the European Union's Strategic Rhetoric

The European Union's attention towards cyber threats has increased over time even though it is not comparable to that of the United States. The four documents we analysed to assess to what extent cyber security has been dealt with at the European strategic level are the 2003 European Security Strategy (ESS),[1] the 2008 Report on its implementation,[2] the Council Declaration "*Statement on tighter international security*,"[3] and the 2010 Internal Security Strategy (ISS) for the European Union.[4]

As shown in table 1, the main result of our analysis is that so far cyber-related issues have been largely absent in the EU security strategic rhetoric and, when they are present, it is difficult to find clear cut definitions. Nonetheless, the EU has demonstrated a growing awareness of the immediacy of cyber threats; for example, if the 2003 ESS only mentions the general danger posed by the misuse of electronic networks, the 2008 document deals more extensively with cyber security and cyber attacks and the 2010 ISS even explicitly refers to cyber crime.

As to expectations, the 2008 Report on the ESS and the EU Council Declaration consistently ask for an increased protection and resilience of the European information networks by means of a more comprehensive European approach and tightened cooperation between the Members States as well as with international partners.

Table 1. Comparing the EU Strategic Documents

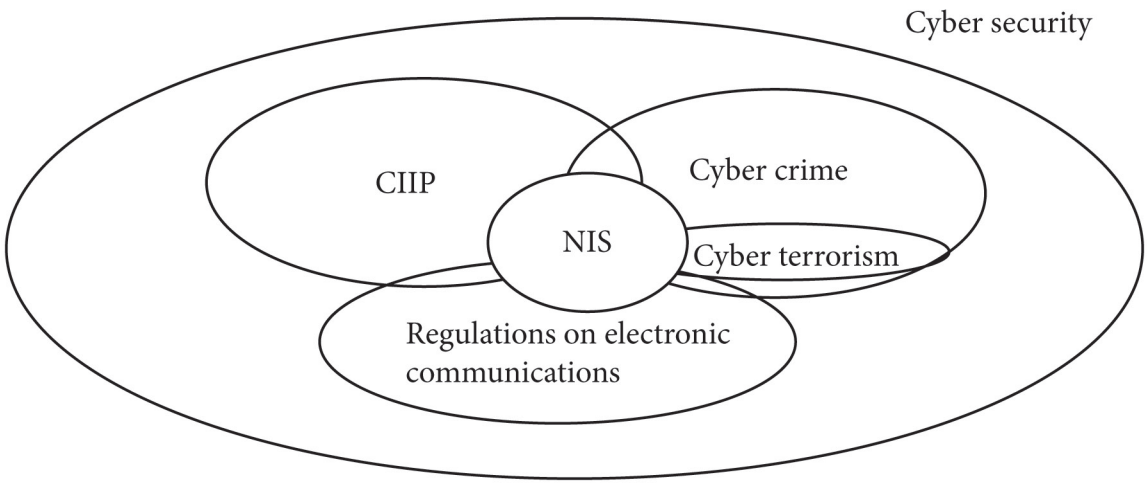
Document	Main Cyber References	Defintions	Expectations
A Secure Europe in a Better World: European Security Strategy (2003)	[…] European dependence on an interconnected infrastructure […] in information […]	//	//
	[…] terrorist movements are well-resourced, connected by electronic networks	//	//
Report on the Implementation of the European Security Strategy: Providing Security in a Changing World (2008)	Cyber security	"Modern economies are reliant on critical infrastructure including transport, communication and power supplies, but also the internet. […] attacks against private or government IT systems have given this a new dimension, as a potential new economic, political and military weapon […]"	More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation.
EU Council Declaration: Statement on Tighter International Security (2008)	[…] use of the internet by terrorist networks	//	[…] (to update legislation) to make recruitment and incitement to terrorism via the Internet a criminal offence
	Cyber attacks	≅ intrusions against public and private bodies	[…] increase the protection and resilience of our networks, by increasing operational cooperation between member states
Internal Security Strategy for the European Union: "Towards a European Security Model" (2010)	Cyber-crime	Global, technical, cross-border, anonymous threat to our information systems	//
	Terrorism […] propaganda over the internet	//	//
	New risks and threats such as […] ICT break down	//	//

Implementing Cyber Security in the EU: Main Policy Initiatives

In order to assess whether and how strategic expectations have been met as well as to have clear definitions of cyber categories and a description of the EU approach in this field, it is crucial to examine in depth cyber policy-oriented documents.

Within the wide realm of cyber security,[5] the EU is adopting a four-pronged approach, which encompasses Network and Information Security measures (NIS), Critical Information Infrastructure Protection (CIIP), the fight against cyber crime and, on the regulatory side, the framework for electronic communications (including data protection and privacy issues).[6]

Figure 1. The EU Approach to Cyber Security



The 2006 Strategy for a secure information society defines Network and Information Security (NIS) as "the ability of a network or an information system to resist (…) accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data (…)."[7]

Critical Information Infrastructure Protection (CIIP) is certainly crucial to this end as it consists of "the activities of infrastructure owners and operators to ensure the performance of critical information infrastructures (namely ICT systems that are that are critical infrastructures for themselves or that are essential for the operation of other critical infrastructures)[8] in case of failures, attacks or accidents above a defined minimum level of services."[9]

With respect to cyber crime, there is not yet a univocal definition across the EU, mainly due to member states' different domestic legislations.[10] However, in a 2007 Communication, the Commission defines it as all "criminal acts committed using electronic communications networks and

information systems or against such networks and systems."[11] Using quite an extensive approach, it further specifies three main categories: i) traditional forms of crime such as fraud and forgery, although in a cyber crime context; ii) the publication of illegal content over electronic media; iii) crimes unique to electronic networks, namely cyber attacks against information system, denial of service and hacking.[12]

As it emerges from the definitions, these "cyber sectors" are strictly interrelated, and often overlapping. It follows that the policy documents referring to them contain similar expectations on how to enhance the EU approach to the multifaceted cyber security challenges.[13] On the one hand, one of the most urgent objectives is to increase awareness on NIS issues. To this end, the Commission generally recommends promoting dialogue—also relying on specific bodies such as the European Network and Information Security Agency (ENISA, see § 6)—and to strengthen cooperation among national and European public and private actors (through so-called PPPs, Public-Private Partnerships). On the other—more operational—hand, the EU should aim to have a more coherent cyber governance model and enhance its preparedness and response capabilities. In this respect, it encourages the establishment of a European Information Sharing and Alert System, the set up of national and pan-European exercises as well as a reinforced cooperation between national Computer Emergency Response Teams (CERTs, see § 6).[14] Last but not least, additional suggested initiatives concern stronger financial investments in research and for the training of law enforcement and judicial authorities, stronger commitments towards legal harmonisation and the further definition of specific crime categories, such as identity theft.[15]

Cyber Security in the United States' Strategic Rhetoric

Recognizing the growing dependence of the United States on the information network and of the steady increase in the number of cyber attacks it has undergone in the last years,[16] the Obama administration has recently recalled that "digital infrastructure is a strategic national asset and that to defend is a national security priority."[17]

Differently from the EU, cyberspace and related threats are dealt with extensively in all the three main strategic U.S. reference documents: the White House's National Security Strategy (NSS, May 2010), the first-ever Department of Homeland Security (DHS) Quadrennial Homeland Security Review (QHSR, February 2010) and the Department of Defense (DoD) Quadrennial Defense Review (QDR, February 2010).

As table 2 clearly shows, the three documents offer quite a consistent view, even if tailored on their own domain of activity, that is the military and defence field for the DoD and the government and critical infrastructures protection's one for the DHS.

Although only the QDR contains an explicit definition of cyberspace as the global domain that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks, all the strategies describe the nature of possible cyber attacks. They may be carried out by both state and non-state actors (e.g., terrorist groups or organised crime) and may consist in the intrusion in or the disruption and exploitation of the U.S. critical information systems and networks.

As for expectations, in the light of past strategies and still existing gaps identified in the U.S. policy, four main points are raised up: enhancing the protection, security and resilience of the government and industry's information systems and networks; strengthening partnerships at both the international level (due to cyber threats' transnational nature) and the domestic one across Government agencies and private actors; increasing public awareness on cyber-related issues; finally, further investing in Research & Development and in human capital expertise.

Table 2. Comparing the U.S. Strategic Documents

Document	Main Cyber References	Definitions	Expectations
National Security Strategy (May 2010)	Secure cyberspace: it has a quite comprehensive view, generally speaking of "cyber threats"	Threats from individual criminal hackers to organised criminal groups, from terrorist networks to advanced nation states	To deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: 1. Investing in people and technologies to a. Better protect and improve the resilience of critical government and industry systems and networks 2. To strengthen international partnerships to 3. To strengthen partnerships with the Government and with the private sector
Quadrennial Homeland Security Review (February 2010)	Cyber attacks	Carried out by state or non state actors (individual, (terrorist) groups): • Intrusions in search of information to use against the United States • Spreading of malicious codes in an attempt to destroy, disrupt the national information infrastructure and threaten the delivery of critical service + steal money and information	
	Cyberspace	//	DHS' vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design

	Safeguarding and Securing Cyberspace (4th DHS mission)	//	1. Creating a Safe, Secure, and Resilient Cyber Environment 2. Promoting cybersecurity knowledge and innovation
	Cyberspace is also cited when speaking of critical infrastructures and related protection (1st DHS mission)	See above	1. Protect critical infrastructure: a. Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions—including linkages through cyberspace—from attacks or disruption.
Quadrennial Defense Review (February 2010)	Cyber domain	//	"more comprehensively monitor the air, land, maritime, space, and cyber domains for potential direct threats to the United States"
	Cyberspace	Global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks	//
	Cyberspace attacks	No clear-cut definition. It is only reported that they could target command and control systems and the cyberspace infrastructure supporting weapons system platforms.	DoD mission-critical systems and networks must perform and be resilient in the face of cyberspace attacks.
	§ Operate effectively in cyberspace	See above for the definition of cyberspace	1. Develop a comprehensive approach to DoD operations in cyberspace 2. Develop greater cyberspace awareness and expertise 3. Centralize command of cyberspace operations (USCYBERCOMMAND) 4. Enhance partnerships with other agencies and governments, in particular with the DHS.

Implementing Cyber Security in the United States: Main Policy Initiatives

The first significant U.S. efforts to address the risks of cyberspace date back to end of the 1990s—with Presidential Decision Directive 63 creating a coordinating structure within the White House—and to the early 2000s with the issue of the 2003 National Strategy to Secure Cyberspace,[18] which almost fell on deaf ears, and of Homeland Security Presidential Directive 7 that assigned to the DHS the responsibility of coordinating all national initiatives for critical infrastructure protection, cyber infrastructures included.

These initiatives were revitalised in the second half of 2000s by the Obama administration that endorsed in May 2009 the Cyberspace Policy Review (CPR), whose conclusion and recommendations were to inspire the abovementioned 2010 strategic documents. With a view to filling in the gaps in the U.S. cyber approach, the CPR puts forward a punctual near-term action plan that calls for a more centralised and consistent management of cyber-related issues across the wide array of U.S. federal departments and agencies; an updated national strategy to secure the ICT infrastructure and a cyber security incident response plan; the enhancement of public-private dialogue, and, last but not least, stronger investments in cutting-edge technologies.

The policy and operational activities currently under way to implement the Cyberspace Policy Review mainly build on the former classified Comprehensive National Cyber security Initiative (CNCI) launched by President Bush in January 2008 and then widened and made publicly available by Obama.[19] Besides trying to bridge the traditionally separated cyber defence missions with law enforcement, intelligence, counterintelligence capabilities, the CNCI outlines twelve major technical steps to enhance the security of the overall U.S. information network (here comprised of other critical infrastructures that heavily rely on information systems)[20] and strengthen the cyber security environment. In keeping with other documents, the proposed measures include the creation of a shared situational awareness of network vulnerabilities within the federal government; specific intrusion detection/prevention systems; government-wide cyber counterintelligence plans; major investments in R&D and training across the federal government.[21]

In addition to strategic and policy documents endorsed by the Executive branch, the debate on cyber-related issues continues in the Congress and in its sub-committees. One of the most recent and debated bills is the Cyber security Act of 2010, recently approved by the Senate Committee on Homeland Security and Governmental Affairs, whose recommendations are in line with those contained in the main policy documents surveyed above. [22]

Implementing Cyber Security: An Operational-level Selection of EU and U.S. Mechanisms and Agencies

With reference to policies' implementation, we will consider here a selection of the most significant aspects, such as the creation of dedicated agencies and mechanisms, exercises' planning, and the funding of related research.

Regarding the EU, the European Network and Information Security Agency (ENISA) was established in 2004.[23] It essentially works as a hub for information exchange among the EU member states, the European Commission[24] and the private sector, supporting them in their cooperation and in ensuring the security of Europe's Information Society.

The agency encounters probably two main limits. First, a low budget, around 8 million euro in 2010, with only 25 percent of funds devoted to its core activities.[25] Second, ENISA does not have—up to now—an operational role and does not deal with issues such as IT-terrorism, cyber crime, criminal law (done by member states and Europol) or personal data protection (done by the EDPS—European Data Protection Supervisor—and national Data Protection Authorities). It was not originally conceived to address citizens' protection but rather to maintain commercial and economic continuity (with a possible secondary impact on the former aspect). This was confirmed when a large-scale Distributed Denial of Service (DDoS) occurred in Estonia in 2007 and the main intervention was through NATO. Nevertheless, the European Commission has recently presented a proposal for a new directive to extend ENISA's mandate in terms of scope and duration (until 2017).[26]

Despite limits, ENISA provides an important framework for different initiatives in the CIIP field. First, it acts as a facilitator and information broker for the Computer Emergency Response Teams (CERTs),[27] the key tools to implement CIIP. In particular, the Agency aims to minimise the existing gaps by facilitating their establishment, training and implementation. It should be noted that while almost all CERTs are nation-based, only few of them are international, with the important exception of FIRST.[28] In this vein, ENISA has recently called for the establishment of a EU CERT to handle community-wide IT threats.[29]

Second, the first pan-European exercise on CIIP, Cyber Europe 2010, was successfully completed in September 2010 under ENISA's aegis. Participants in the exercise were public authorities of the EU member states and the scenario concerned incidents affecting the Internet availability in several European countries.[30] The interim findings and recommendations drawn from the exercise included the need to enhance cooperation, the exchange of information and of lessons learned among EU member states—with a view also to filling in the gaps existing among them—to involve private actors in and to allocate more time to planning and execution of the next exercise.[31]

With regard to the United States, due to the higher number of players involved, we will focus here on the most relevant and on those comparable with the European ones. Generally speaking, as called for by the CPR and the CNCI, recent U.S. initiatives aim at enhancing cooperation and coordination across the government's agencies and departments as well as with the private sector, namely the defence industrial base and critical infrastructures stakeholders.

In this respect, the reference point is the Department of Homeland Security (DHS), which coordinates, through the National Cyberspace Response system within the National Cyber Security Division (NCSD), all federal efforts in the field of CIIP, oversees the Government's implementation of all cyber policies, and supports agencies to this end. [32]

As for operational programmes, worthy of mentioning are the Cyber Security Preparedness and the National Cyber Alert System, which monitor 24/7 cyber infrastructures and disseminate relevant information to interested stakeholders. A crucial role is here played by the U.S.-CERT, a public-

private partnership which provides response, support and defence against cyber attacks for the Federal Civil Executive Branch (.gov).[33]

As far as exercises are concerned, Cyber Storm Exercise Series should be considered: The Cyber Storm III took place at the end of September 2010 and saw a significant participation of federal, state, international and private actors. Simulating large-scale cyber events and attacks on the government and the nation's critical infrastructure and key resources, it aimed at testing the U.S. system's resilience. Additionally, it was the primary vehicle to exercise the new cyber response mechanism (National Incident Cyber Response Plan) [34] and the new coordination hub (National Cyber security and Communication Integration Center), both created by the DHS.[35]

On the military side, the Pentagon, in May 2010, established under the U.S. strategic command a new Cyber Command, headed by Gen. Keith Alexander, Director of the National Security Agency (NSA), and budgeted $139 million. In an effort to coordinate civil and military cyber activities, the DHS and DoD have recently signed a cooperation agreement and the Obama administration appointed a so-called "Cyber Czar" [36] serving as Cyber security Coordinator within the National Security Staff (NSS) of the White House.

With regard to EU Research & Development on cyber issues, the EU Group of Personalities called for stronger investments in IT technologies against cyber attacks already in 2004.[37] This request was followed by similar ones in the reports of the European Security Research Advisory Board (ESRAB)[38] and of the European Security Research and Innovation Forum (ESRIF)[39] as well as in the core EU cyber policy documents. However, despite such formal commitments, substantial results have yet to be attained. As an example, the last Security Call under the Seventh Framework Programme devotes only one topic—out of nearly 50—to cyber security.[40]

In the United States the amount of Government funding to R&D is certainly higher with contributions from different federal department and agencies. Against this backdrop, one of the key initiative of the CNCI is to coordinate all cyber R&D, both classified and unclassified, and to redirect it where needed in order to avoid redundancies and identify gaps.

The Transatlantic Level: Recommendations

We will investigate here the extent of current transatlantic cooperation in the cybersecurity domain, advancing some policy recommendations to fill in the identified gaps.

As for institutional cooperation, the main framework of reference is represented by the EU-U.S. Annual Summits, an important occasion to discuss common challenges and foster mutual coordination. In the 2009 Summit, cyber security was for the first time identified as a global challenge and commitments to enhance mutual dialogue and prioritize areas of possible cooperation were undertaken. [41] The 2010 Summit seemed to proceed a step further with the establishment of an EU-U.S. Working Group on Cyber security and Cyber crime to address a number of specific priority areas.[42] Composition and tasks of such working group are still unknown. If it will take time to assess its real effectiveness, its denomination, implying the distinction between cyber security and cyber crime as two different fields of activities, already arises some concerns on the clarity and focus of its mandate. Furthermore, dealing with such challenging issues only at a working group level could be

questioned. Indeed, in order to maximize the results, it would be better also to "institutionalise" the dialogue on cyber security within the EU-U.S. Summit institutional framework, establishing, for example, a U.S.-EU Cyber security Council at ministerial level along the lines of the U.S.-EU Energy Council.[43] Such a Council could have limited tasks in the short to medium term—and then be upgraded—in order to act at the very least as a *permanent* consultation forum.

With regard to policies implementation, the EU and the United States, as we have seen, actually agree most initiatives to be undertaken for cyber security purposes. Measures such as public-private partnerships, public incentives to private investments in cyber security, including technology innovation, the enhancement of cooperation across various agencies and at the international level recur several times in both EU and U.S. strategic and policy discourses. However, apart from irregular consultations between the DHS, DoD and the Commission DGs for Media and Information Society and from dialogue within NATO,[44] common formal engagement is at present time limited.

At the agency level, the insufficient/difficult cooperation is perhaps also due to the still embryonic EU cyber security architecture, which prevents the EU from being a unique and cohesive counterpart for the United States.[45] This is why the proposals to strengthen, for instance, ENISA's mandate and eventually appoint a European Cyber security Coordinator[46] are welcome. Models for coordination on specific cyber aspects include some transatlantic initiatives recently set up at the bilateral level, such as the European Electronic Crime Task Force (EECTF), active in the field of cybercrime. Established in March 2010 as a joint effort of the Italian Post Office, the Italian Police and the U.S. Secret Service, EECTF aspires to involve as many EU member states as possible.

On the strictly operational side, there are currently no DHS-ENISA joint exercises, despite their same field of action (i.e. CIIP). A model for future initiatives in this sense could be the recent U.S. Cyber Storm III that already foresees international partners' participation. Besides this, information sharing and best practices' exchange between American and European CERTs should be enhanced, as a means to increase the bottom-up pressure to the final establishment of common policies in order to boost public-private partnerships and to raise private stakeholders' awareness of their crucial role in cyber security. The latter are indeed at the same time owners of roughly 85 percent of CIIs in the EU and the United States and providers of technological solutions.[47] The proposed establishment of a EU-wide CERT could therefore have a positive impact on transatlantic coordination.

Finally, stronger transatlantic cooperation is being achieved at experts' level, with meetings on CIIP and cyber-related aspects.[48] Yet these activities often seem too technical and lack a coherent framework, continuity over time and an effective dissemination of the results.

Another essential aspect for effective transatlantic cooperation on cyber security is the conceptual and semantic harmonization of cyber issues, as a preliminary step to attain legal harmonization. In light of the prevalence of U.S. sources,[49] this is felt as particular urgent on the EU side, [50] where overlaps and ambiguities often occur both due to the rapid evolution of those matters and to the different legal and cultural backgrounds of member states. A systematization is therefore needed, with a twofold objective: clearly identifying specific legal categories and boosting legal production.

Some progress towards harmonisation has already been made in the cyber crime sector, with the 2001 Council of Europe Convention on Cyber crime at the forefront. However, while the United

States actively participated in the drafting process and ratified the Convention in 2007, the EU is not part to the Convention on its own and many EU member states still have to ratify it.[51]

Semantic and legal (not least operational) consistency is crucial also for effective law enforcement in the cyber domain. A crucial actor in this sense is Europol, the EU's police Agency, that currently hosts the European Cyber Crime Platform (ECCP) which facilitates the collection, exchange and analysis of information with member states[52] and plans to create by 2013 a European Cyber Crime Centre to better coordinate at the EU level the fight against cyber crime.[53] For this same purpose, the promotion of international conventions could be a useful tool. They could for instance commit nations to allow Interpol investigations on their territories if suspected of being used as the base for cyber attacks.

The review or rather the establishment of the regulatory framework could be more complex for cyber attacks—as disruptions—including those carried out by terrorists. In such cases there are many elements to consider, being them at the borderline between internal and external security as well as between civilian and military competences and thus requiring a synergy of solutions. For example, when a civil response is more appropriate than a military one, and vice versa? When a state actually does not initiate an attack, but tacitly gives a private operator the go-ahead, is the state then legally responsible for the actions of the citizens actually operating on its behalf?[54]

From this overview, it seems clear that the United States is a step ahead of the EU in dealing with the cyber challenge. Whereas the former is carrying out efforts to systemise and make its cyber structures more consistent, the latter has still to build a comprehensive cyber security architecture.

A preliminary condition for effective transatlantic initiatives is therefore the conceptual and political harmonization within the EU, in order to prevent the un-coordinated presence of different national positions vis-à-vis the single U.S. partner. A single cyber security strategy reconciling all the EU actions in this field and referring to a cyber security coordinator would be needed. To this end, a debate could be launched through a Green paper or directly resorting to more binding instruments. A the same time, a massive awareness campaign on the manifold cyber challenges should be initiated amongst institutions, member states and private stakeholders, including private citizens.

Moving down to the policy level, it is now time to ensure the swift implementation of the recommendations already put forward in the EU and U.S. documents and the approval of those still in the pipeline. We refer in particular to the Action Plan on the 2009 Commission Communication on CIIP, to the key actions of the 2010 Digital Agenda for Europe, to the two recent proposal for directives on cyber attacks and on ENISA's mandate and the 2010 EC Communication on the ISS on the EU side, and to the Comprehensive National Cyber security Initiative, on the U.S. one. In addition, policy implementation efforts should be supported by adequate funding in Research and Development. Stronger efforts in this sense are required and deeper reflections on the possible synergies between civilian and military technologies should be conducted.

Cyber security-related issues will certainly be at the core of the international debates in the years to come. Even though questions seem to overwhelm answers right now, choosing the right questions is an indispensable task for the appropriate level of decisionmaking. Building a cyber security architecture and making the existing one more effective must definitely involve both the EU and the

United States working together. However, not taking up this challenge would entail far higher costs down the road.

BIOSECURITY IN A TRANSATLANTIC CONTEXT

Elisande Nexon, *Researcher, FRS,* and Jean-François Daguzan, *Senior Research Fellow, FRS*

Introduction

The 2001 anthrax letter attacks in the United States, followed by thousands of hoaxes worldwide, exposed the threat of biological weapons and revealed vulnerabilities. The last decade has also seen several outbreaks of infectious diseases, from SARS to H5N1 or H1N1, raising pandemic fears. Confronted to the sequels, governments have launched ambitious programmes, allocated human and financial resources, and developed plans for biological preparedness and response. Advances in life sciences also offer new perspectives in many fields, including public health. But they also represent new challenges, with is a convergence between science and security.

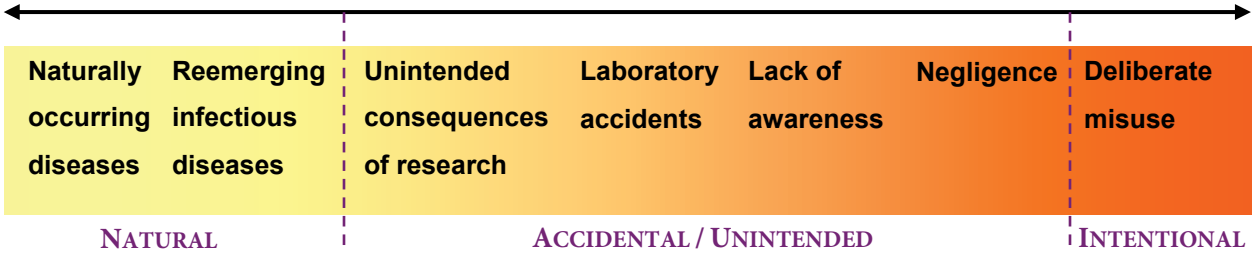
Reducing the risks can be achieved through a full range of options, such as adopting national legislation and regulations, strengthening the Biological and Toxins Weapons Convention and promoting UN Security Council Resolution 1540 (2004), engaging in outreach and cooperation activities, or providing guidance and guidelines, as well as raising public awareness. In this context, biosecurity and biosafety can contribute to reduce the full spectrum of biological risks, and can be easier to implement at local level and less controversial than other options.

The aim here is to analyze if and how biosecurity issues are addressed, through the identification and study of the main recent major policy statements, official papers and strategies, and actions and initiatives dedicated to biological threats (or including them). The term itself may not always be mentioned, so the context and the study of the measures are important. Biosecurity issues should be studied in the broader context of the fight against the proliferation of biological weapons and against bioterrorism. Other threats such as malevolence must not be excluded.

Background and Definitions

Biological Risks Spectrum

Before considering the means of protection and prevention, it is useful to consider the biological risk and threat assessment. The full spectrum of biological risks can be described as follows (Taylor, 2006):



Source: Terence Taylor, "Safeguarding advances in the life sciences," EMBO Reports 7 (2006).

The naturally occurring diseases and the (re)emerging infectious diseases obviously present the greatest risk. At the other end of the spectrum, the deliberate misuse of knowledge, agents or technologies, which could involve state actors as well as non-state actors or even individuals, cannot be excluded even if it must not be overestimated. In between are the events that can be qualified as accidental or unintended. If they remain scarce, this is nevertheless a source of preoccupation, with serious or even lethal accidents as reminders of the reality of the risks. They fuel the debate about biosecurity and biosafety.

Definitions

The major guidance documents cited regularly in official documents on such topics, in the European Union as well as in the United States, have been issued by the World Health Organization (WHO), the WHO Laboratory Biosafety Manual, Third Edition (2004) and the WHO Biorisk Management: Laboratory Biosecurity Guidance. This biorisk management approach encompasses biosafety, laboratory biosecurity as well as ethical responsibility.

The terms are defined as follows:

Laboratory biosafety: describes the containment principles, technologies and practices that are implemented to prevent the unintentional exposure to pathogens and toxins, or their accidental release.

Laboratory biosecurity: describes the protection, control and accountability for valuable biological materials within laboratories, in order to prevent their unauthorized access, loss, theft, misuse, diversion or intentional release.[55]

Finally, the 2008 expert's meeting of the Biological and Toxins Weapons Convention (BTWC) concluded that "biosecurity comprises measures that minimize the possibility of biological agents being deliberately used to cause harm. This distinguishes it from biosafety, which involves measures aimed at protecting people and the environment from the unintentional impact of biological agents, and includes workplace health and safety issues and the prevention of the accidental release of such agents."

In the United States, the Office of Science and Technology Policy within the Executive Office of the President has created a website dedicated to biosecurity and the relevant government policies, and definitions of the main terms are proposed, relevant with the WHO definitions. For "biosecurity," it refers specifically "to high-consequence biological agents and toxins, and critical relevant biological materials and information between laboratories." The use of "biosecurity" in the fifth Edition of the

Biosafety in Microbiological and Biomedical Laboratories (BMLB) from the Public Health Service (PHS), the Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH) is consistent with the definition provided by the WHO and the American Biological Safety Association (ABSA). The need for a biosecurity program based on risk assessment is underlined, and an example guidance of a biosecurity risk assessment and management program is provided, leading to the implementation of key elements, based on organisational threat/vulnerability assessment. Balancing biosafety and biosecurity, it considers that biosafety should take precedence over biosecurity concerns, if there is a lack of legal requirements for a biosecurity program. Regarding biosecurity specifically, prioritization of risks is a key element, as addressing every possible threat is not manageable.

In the European Union, contrary to biosafety, there are currently no common standards and definitions for biosecurity.[56] The Green Paper on Bio-Preparedness presented by the European Commission in 2007 mentions that biosecurity and biosafety can be understood in different ways, depending on the context. It is specified that concrete definitions are to be found in the 2006 WHO Laboratory Biosecurity Guidance. The European Center for Disease Prevention and Control (ECDC) also uses the definition proposed in the reference document. Furthermore, the CEN Workshop Agreement (CWA) on Laboratory biorisk management standard represents a voluntary standard applicable internationally, publicly available as reference document from the CEN Members National Standard Bodies and which does not have the force of regulation.[57] The adopted definitions for biosecurity and biosafety also derived from the 2006 WHO Laboratory Biosecurity Guidance, with "biological agents and toxins" replacing "valuable biological materials."

To conclude, while there is a lack of universal agreement about the definition, there is still usually a common basis in official documents. In many documents or statements, both terms are mentioned. However, sometimes they are employed indiscriminately, as the distinction does not appear evident, and it may be confusing. The use of *biosecurity* and/or *biosafety* may differ between countries, but it may also depend on the field of expertise and the context (for example, human health, animal health, agriculture, arms control, etc.) Depending on their background, biosecurity has a broader meaning for some experts and officials and encompasses all the measures which can improve security in the context of a biological threat, from biosurveillance to medical countermeasures.

Biosecurity and biosafety differ, but are nevertheless related. Both rely on risk assessment and management methodology, personal expertise and responsibility, control and accountability for research material including microorganisms and culture stocks, access control elements, material transfer documentation, training, emergency planning, and program management.[58] The distinction between biosecurity and biosafety may seem somewhat anecdotic, at the laboratory level, as some measures are common to both. However, on the one hand, good laboratory biosafety practices strengthen biosecurity systems, on the other hand, if there is a lack of a global approach identifying the potential consequences of each measures, the implementation of biosecurity and biosafety measures on the same site may prove conflicting, as the respective objectives differ. Biosecurity tends to rely on regulatory requirements, while biosafety relies more on best practices and guidance.

From Policy Statements to U.S./European Strategies

United States

Context in the United States and first specific regulations

There are a number of strategies, directives and orders which can be said to relate to biosecurity, some of them addressing the broader issue of terrorism and/or weapons of mass destruction, others more specifically addressing biosecurity even if the term itself is not mentioned. Two events have especially triggered the development of national strategies and policies.

Following the Oklahoma City bombing, in April 1995, Congress passed in October 1996 the Antiterrorism and Effective Death Penalty Act of 1996. The part on Biological Weapons Restrictions, with Enhanced penalties and control of biological agents, defines regulatory control of the biological agents, with the establishment of "a list of each biological agent that has the potential to pose a severe threat to public health and safety," specifying criteria for the inclusion on this list. 42 CFR 72.6 implemented the provisions of this act.[59]

In the aftermath of the 2001 terrorist attacks, the Congress passed the Uniting and strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), then the Public Health Security and Biopreparedness and Response Act of 2002, implemented by the Select Agent Regulations, which encompass 7 CFR Part 331, 9 CFR Part 121 and 42 CFR Part 73. "Biosecurity" is used only in relation with agriculture, while there is a part about "security" in the 42 CFR 73 which specifies that "an entity must develop and implement a security plan establishing policy and procedures that ensure the security of areas containing select agents and toxins." In sum, it is the goal of the U.S. government that biosecurity be enhanced to minimize the risk of misuse and the potential resulting threat to public health and national security, but without hindering the advances in the life sciences.

Presidential directives and national strategies

The key U.S. document relating to biosecurity is the National Strategy for Countering Biological Threats, released in 2009 and complementing other White House strategies.[60] It states that "a comprehensive and integrated approach is needed to prevent the full spectrum of biological threats as actions will vary in their effectiveness against specific threat." It is an all inclusive risk management approach. The Strategy identifies seven objectives, setting strategic guidance for federal entities in charge of the implementation.

Some parts clearly fall under biosecurity policies or practices (with the use of the expression "biological security" several times). The fourth objective indeed expresses the need to address the risk by promoting discussions and activities involving academia and the private sector, and by limiting ready access to known virulent high-risk pathogens and toxins, coupled with the use of adequate safety controls and practices, in order to optimize security. The intended efforts to achieve this goal include the optimization of domestic laws, regulations, policies and practices, the procurement of detailed guidance, as well as an improvement regarding the use of mechanisms to report theft, loss or release from laboratories to the relevant public health and law enforcement agencies. This part also

stresses the importance of international cooperation, with the promotion of international guidelines for safety and security of high-risk pathogens and toxins, the supporting of partner countries and regions to ensure the application of biological security and safety practices in a risk-based and sustainable manner, but although in order to identify collections of such pathogens and toxins, and where possible, consolidate them at national regional centres of excellence.

Furthermore, the WMD Prevention and Preparedness Act of 2010 also called Global Pathogen Surveillance Act of 2010 is at the moment in the first step of the legislative process (it may never go further). The first title of this Act is entitled "*Enhanced biosecurity*."

In addition, there are also a number of executive orders relating to biosecurity. For example, Executive Order 13486: Strengthening Laboratory Biosecurity in the United States (2009) created the Working Group on Strengthening the Biosecurity of the United States. It was given the mission to review existing laws, regulations, guidance and practices, at federal as well as non-federal facilities "that conduct research on, manage clinical or environmental laboratory operations involving or handle, store, or transport biological select agent and toxins," and then propose recommendations. The Working Group completed this task with the publication of a final report.[61] There is also Executive Order 13 527: Establishing Federal Capability for the Timely Provision of Medical Countermeasures Following a Biological Attack (2009), and Executive Order 13 546: Optimizing the Security of Biological Select Agents and Toxins in the United States (2010), presenting fundamental changes regarding how to secure biological select agents and toxins against misuse. The main improvements will be the potential reduction of the Select Agent list, coupled with the revision of Select Agent Regulations (SAR), rules and guidance. It also provides for the creation of a Federal Experts Security Advisory Panel for the Select Agent Program (SAP), and seeks to improve coordination of Federal oversight for BSAT security by the development and implementation of a dedicated plan, associated to a revision by the heads of departments and agencies of relevant policies and practices.

Main relevant entities in relation with biosecurity

The U.S. government has set up a number of structures to deal directly or indirectly with biosecurity. The National Science and Technology Council (NSTC), in the Office of science and Technology Policy, represents the principal means within the executive branch to coordinate science and technology, and one of the topics is biosecurity. A dedicated website has been designed, contributing to a better awareness.[62] It targets the public, academic researchers, scientific societies, biotechnology and pharmaceutical industries, as well as any other stakeholder communities in biological research.

The National Science Advisory Board for Biosecurity (NSABB) was established by the United States Government Policy on Biosecurity in Life Sciences Research, in order to provide advice and guidance to the federal departments and agencies about biosecurity in the life sciences, the efficient and effective oversight of dual use biological research. The Dual Use Research Program of the Office of Biotechnology Activities (OBA), which supports the NIH Office of Science Policy, convenes and manages the NSABB. NSABB has hosted international meetings on dual use research, and has produces a number of reports.

The Centers for Diseases Control (CDC) and the U.S. National Institutes of Health (NIH) have a key role in the field of biosafety and biosecurity, publishing biosafety guidelines. The CDC, WHO's Centre for Applied Biosafety Programmes and Training, provides formation and training. There is a specific online training on laboratory biosecurity.[63]

Relevant U.S. Actions and Initiatives at International Level

The U.S. Cooperative Threat Reduction (CTR) Program was established in 1992, and implemented by the Defense Threat Reduction Agency (DTRA). Following the Congressionally-mandated 2009 National Academy of Sciences report "Global Security Engagement: A New Model for Cooperative Threat Reduction," the DTRA has undertaken the Nunn-Lugar Global Cooperation (NLGC) initiative to assess how to implement its recommendations. The programme has sought to engage the former Soviet States and the new approach aims at expanding and strengthening it.

Some CTR programs deal with the enhancement of biosecurity and biosafety: the Biosecurity and Biosafety/Biological Weapons Threat Agent Detection (BS&S/TADR) is one of the four parts of the U.S. Department of Defense CTR Biological Threat Reduction Program; the Biosecurity Engagement Program (BEP) and Bio Industry Initiative (BII) both encompass this topic, and are part of the Global Threat Reduction Program, one of the three programs composing the Department of State Non-proliferation, Anti-terrorism, Demining, and Related Programs (NADR).

The United States is also participating state in the G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction, and contributes to the funding of ISTC (Moscow) and STCU (Kiev).

The CTR initiative also supports the implementation of international treaties and security instruments, such as the United Nations Security Council Resolution 1540 (2004). In this framework, American officials have been involved in activities contributing to the promotion of biosecurity and safety, such as the 2010 Africa Regional Workshop on Biosafety and Biosecurity.

European Union

Context

The response to CBRN threats at EU level was initiated with the Ghent European Council of 2001, in the wake of the terrorist attacks in the United States. The "Programme to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats" was adopted in 2002. After the attacks in 2004 in Madrid, the CBRN Programme was superseded by the Council and Commission's EU Solidarity Programme of 3 December 2004. Following the London attacks in 2005, it was included in the Strategy and Action Plan on Combating Terrorism.

EU strategy against the proliferation of weapons of mass destruction

The European Council adopted the EU Strategy against the proliferation of WMD on 12 December 2003, in parallel with the adoption of the European Security Strategy. Regarding biological weapons, it underlines that the threat posed by non-state actors and "the potential for the misuse of the dual-use technology and knowledge is increasing as a result of rapid developments in the life sciences." In

addition, there is a need to address all types of threats, from natural outbreaks to accidental or terrorist events at European level—taking into account the potential public health and security challenges resulting from the guarantee of free movements of people in the Schengen area, delimited by a single external border. The strategy is in favour of a "biological all-hazards approach,"[64] and one point of the strategy deals with the need to enhance "the security of proliferation-sensitive materials, equipment and expertise in the European Union against unauthorised access and risks of diversion," with the European Commission and national legislation and control over pathogenic microorganisms and toxins, and the need to improve awareness in industry.

This strategy was updated and reviewed, and in December 2008 the European Council adopted the "New lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems."

The EU actions: framework

With the Green Paper on Bio-Preparedness (2007), the Commission launched a process of consultation, seeking to generate discussions at European level about the means of reducing biological risks, in order to improve preparedness and response. It was a biological all-hazards approach, taking into consideration all potential risks, meaning terrorist attacks, other intentional releases, accidents or naturally occurring diseases.

With the 2009 EU CBRN Action Plan, the new policy aims at reducing the threat and damage from CBRN incidents to the citizens through the implementation of 133 different measures. It implies a spectrum broader than terrorism. A CBRN Advisory Group has been established to follow the implementation of these actions, and implementation periods are provided.

The Plan promotes a risk-management based process, with a prioritisation of security measures. A significant part of the goal and measures described in the part devoted to prevention falls under the scope of biosecurity. Preventive measures are deemed the main focus of activity, and "the efforts should be concentrated on a limited number of vulnerabilities, which could be exploited for malicious purposes, on the basis of robust risk-assessment process," while subsequent actions will include the security of CBRN materials and facilities, the security of transport, the control over CBRN materials, or developing a high-security culture staff.

Although some measures contribute to enhancing security, most of the existing European legislation addresses safety issues. Assessing potential legislative gaps is one of the objectives of the Action plan, and a study on "biological preparedness" which has been awarded includes a comprehensive overview of biosecurity and biosafety legislation.

It is important to remember that protecting the population against CBRN events remains the responsibility of each Member State, but European initiatives fall under the principle of EU solidarity.[65] The supportive role of the European Union regarding cooperation should be in accordance with the principles of subsidiarity and proportionality. Concerning the CBRN Action Plan, it is highlighted that "the new EU measures in this field should be coherent with and based on the existing national and international regulations and draw upon existing work in other relevant international organisations."

Main relevant EU initiatives and cooperative actions

At European level, the Commission has funded under the last two Framework Programs of Security Research several projects dealing, albeit not exclusively, with biosecurity and biosafety.[66]

The European Union contributes to the reinforcement of biosecurity and biosafety through various activities and initiatives, via different development and cooperation instruments. The Council has adopted a Joint Action in Support of the World Health Organization (WHO) in the area of laboratory bio-safety and bio-security.[67] Its goal is to promote actions to prevent biological risks, in an all-hazards approach, through regional outreach workshops, in-depth topic specific workshops on bio-risk reduction practices, and consultations with relevant competent authorities. The EU also provides assistance to third countries, through the Instrument for Stability or the Development Cooperation Instrument for example, regarding topics such as the promotion of a culture of biosafety and biosecurity, storage and transportation of dangerous microorganisms and toxins, safety and security for the handling, training, or legislative and regulatory assistance.

The European Union plays a role in the context of the BTWC. Before the sixth Review Conference, in 2006, it adopted a Common Position, defining the priorities related to the Convention. It especially specifies that the EU will promote the G8 Partnership programmes—which include some dedicated to the control and security of sensitive materials, facilities, and expertise—as well as common understanding and effective actions concerning national mechanisms for the security of pathogens microorganisms and toxins. EU member states also submitted to States Parties a Paper on Biosafety and Biosecurity.

The EU is also a contributor to the G8 Global Partnership and to the funding of ISTC (Moscow) and STCU (Kiev). Finally, the EU intends to establish regional CBRN Centres of Excellence, which would mobilize national, regional and international resources, and address all aspects of CBRN policy, biosecurity and biosafety included.

Biosecurity as a Transatlantic Issue

Studying biosecurity as a transnational issue is perfectly relevant. It is related to the nature of the associated threat, as well as to some measures and initiatives which have or could have a transatlantic dimension. Biosecurity can be regarded as a transatlantic issue because of the nature of the threat/risk. The risk of dissemination of highly infectious pathogens, including multi-resistant strains, can become a transatlantic issue with consequences for health management. Moreover, dealing with such pathogens may imply the need to address border control and travel restrictions issues. Transnational terrorist groups have shown an interest in weapons of mass destruction, including biological such. An attack on American soil could involve foreign nationals from the European Union, or the reverse. Furthermore, acquisition of biological agents, or of dual-use know-how or technologies, could just as well occur in another country.

But biosecurity is also a transatlantic issue from the angle of prevention and management. Exchange of information on such topics as threat assessment, terrorist alerts, students or researchers who have been deemed suspicious in a country; promotion of discussions and sharing of experience

about biosecurity and biosafety through various fora and dedicated workshops, involving different levels ranging from government representatives and experts to scientists. Finally, also pertinent in a transatlantic context is addressing the issue of standardization and regulation.

Assessment and Transatlantic Dimensions

Some key aspects can be associated with the need to discuss how to prevent biological risks, involving renewed or unprecedented challenges in terms of biosecurity and biosafety, and some of them interrelated:

First, several publicized incidents have fuelled the debate—especially vivid in the United States about the safety and security at laboratories, for example the power outages at CDC's high-containment laboratories in 2007 and 2008, and unreported infections or safety breaches are a cause of concern.[68] The 2001 anthrax attacks in the United States followed by thousands of hoaxes in the European Union have represented an incentive for the developments of biodefense programmes and the construction of laboratories, with the allocation of dedicated financial and human resources. But as usual it can be defined according to a benefits/risks approach. The efforts have indeed led to improved prevention and response capacities, with significant progresses, especially in the field of detection, diagnostic testing and medical countermeasures. But at the same time the risks of accidents or even misuse have increased, due to the higher number of people and infrastructures involved, and weaknesses in terms of safety and security culture and training are observed. Biosafety and biosecurity at high-containment laboratories and at biodefense facilities (whether BSL-4 or not) are especially under scrutiny. New biosafety-level-4 (BSL-4) laboratories are being built in the European Union. A similar expansion is observed in the United States, in response to the 2001 attacks and the need to develop medical countermeasures. However, if the number of BSL-4s labs is known, federal officers and experts are less sure about BSL-3 labs.[69,70] Even if laboratory accidents in high-containment laboratories are relatively rare, they usually occur because of human error or system failure. The identification by the FBI of a microbiologist at the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) as the perpetrator of the 2001 anthrax attacks highlighted the risk of misuse from insiders. Both biosafety and biosecurity are at stake, and compliance is a key aspect.

Second, the advances in the life sciences, with especially the expansion of biotechnologies, and synthetic biology and genomics,[71] mean new opportunities but also generate new challenges in terms of safety and security, with the risks of unintended consequences on health and environment, of accidental release. The potential consequences of ongoing diffusion of knowledge, technology and capabilities beyond the professional biotechnology community have to be assessed and discussed. If synthetic biology is a recent evolution by comparison with other scientific fields, the debate about biosafety and biosecurity is vivid and constructive, with initiatives launched at institutional, academic and/or industrial levels.[72] This evolution and the generated debate must be linked with the GMOs issue.

Third, actors from government, civil society and private sector are or should be involved. New actors and/or a higher number of them are involved, signifying people from various backgrounds with various levels of knowledge and awareness concerning these risks and the measures to be

implemented to prevent them. With synthetic biology, there is for example a convergence between several disciplines, and among them biology, chemistry, genetic engineering, or informatics. In this context, engaging some of the actors about biosecurity issues may prove challenging.

Fourth, the advances in life sciences, in association with the wide, easy and uncontrolled diffusion of information, have promoted the phenomenon of "biohackers"[73] and DIYbio ("do it yourself bio").[74]

Finally, concerning the pharmaceutical sector, the competition with generic manufacturers, the development of biotechnologies, the potential markets resulting from concerns about biodefense or emerging diseases, are responsible for an increased interest towards biological medicines. These medicines are produced by using living systems or organisms (by comparison with chemical compounds).

In summary, the European Union and the United States share common views. In the European Union as in the United States, bio-preparedness is deemed a priority and an "all-hazards" approach is favored, taking into account the full spectrum of biological risks, from natural outbreaks, to accidental contaminations and release, and misuse. Regarding biological weapons, preoccupations about the threat from non-state actors has been expressed in European and American strategies. Further, the EU and the United States apparently agree on the need for prioritization in terms of risks, and the need for definitions of biosecurity and biosafety that are consistent with the definitions from the WHO. Biosecurity and biosafety measures can be complementary but also sometimes prove to conflicting. Cost and complexity of implementing all the measures must not reduce compliance or affect research and legitimate activities. While both agree that a clear oversight of all the activities and facilities involving biosafety and biosecurity issues is essential, such oversight is likely difficult to achieve as, for example, governmental, academic or private laboratories or entities, the control of which may depend on different ministries or agencies. Reviews of existing biosecurity and biosafety policies and practices have been launched in the European Union and in the United States, and it has led to recommendations for improvements, the definition of goals and actions. The implementation has begun but it is for the moment too recent to analyze and conclude.

Recommendations

1. Adopting common definitions and terms of reference would improve communication and avoid misunderstanding.
2. Developing a common norm should remain an objective. A biosecurity regulatory framework must apply to all institutions and entities dealing with biological materials of concern. The scope must not be limited to biological agents and toxins causing harm to human health, but also address those which have an impact on livestock and crops.
3. Giving the extent of the recent policies and practices reviews in the United States and at the European level, sharing more analyses would be interesting. A better view of incidents related to biosecurity could also prove valuable.
4. A coordination of biosecurity programmes, requiring a clear oversight of all the outreach and cooperation initiatives and activities, would prove fruitful, preventing overlaps and enabling

synergic actions. Both the European Union and the United States have expressed an interest in promoting biosecurity and biosafety in the framework of the BTWC, for example through outreach activities. Undersecretary E. Tauscher has declared that for the administration the BTWC was the "*premier forum for dealing with biological threats*," "*for global outreach and coordination*." The United States and the European Union also provide funding to activities linked to the G8 Global partnership or the Resolution 1540.

5. Developing a culture of biosecurity is an important requirement, all the more so that exchange programmes are frequent for scientists and students, but remembering that all key stakeholders must be involved (from public health, law, intelligence,…). It raises the question of defining common guidelines, best practices, as well as and of the standardization and certification process (a laboratory could seek an accreditation to show it is implementing best practices, for example).

6. On a security level, discussions could also focus on how to give, when necessary, common guarantee if it is achievable, for example with a system of vetting and clearance. Strengthening security without hindering research and competitiveness is a key issue.

7. The CEN Workshop on Laboratory and Biosecurity involved among others representatives of the WHO and of the European and American Biological Safety Associations (EBSA, ABSA). Discussions focused on the certification process, best practices, and the situation concerning standardization, certification and the requirements for developments. The Biorisk Management Standard was developed through the CEN Process.

8. Constructive transatlantic initiatives and dialogues do not always involve institutional representatives, and must be encouraged. Industrials can contribute to the debate, and scientific communities and societies also have a key role. Through workshops and sharing of experience, they contribute to identify risks, propose improvements and develop guidelines. It is an important means for raising awareness and engaging scientists or professionals who does not apprehend security issues or even perceive security measures as hindering research and innovation.[75]

EU AND U.S. PANDEMICS PREPAREDNESS AND RESPONSE

Mark Rhinard, *Head of the Europe Program and Senior Research Fellow, UI,* and Erik Brattberg, *Research Assistant, UI*

Introduction

The scale of dangers posed by influenza pandemics, combined with a series of actual outbreaks, has led policymakers on both sides of the Atlantic to frame pandemics as a security threat. In the United States, the 2006 and 2010 national security strategies identify pandemics as a "catastrophic challenge" while the 2006 U.S. pandemic plan argues that pandemics should be viewed as a "national security issue."[76] The UK's National Security Strategy categorises an influenza pandemic as the "highest risk" civil emergency.[77] France's White Paper on Security and Defence lists pandemics as a pressing global security threat.[78] And the EU's review of its own European Security Strategy broadened the threat scope to include pandemic influenza.

Identifying an influenza pandemic as a security threat, however, is relatively easily done. More challenging is to act upon that designation, through implementing security strategies in practice. Preparing for the onset of a pandemic poses a host of troublesome governance issues for the EU and United States, not least in the areas of boosting domestic capacity at the operational level, improving coordination across policy jurisdictions, and enhancing international cooperation. As a prototypical example of a threat crossing the "internal/external nexus," an influenza pandemic arguably presents more governance challenges than a traditional security threat. This paper examines whether the EU and United States are turning words into action on the issue of pandemic threats. We focus on activities related to preparing for a pandemic. More specifically, we assess surveillance, early warning, and containment/control efforts.

Europe and the EU

Threat Perceptions

Despite the onset of SARS in 2002, which surprised officials worldwide with the unpredictable nature of its spread, the formulation of the EU's European Security Strategy (ESS) in 2003 made no reference to pandemics as a security threat. However, the review of the ESS in 2008, which produced an "implementation report" of the ESS, broadened the threat scope to include public health threats,

including pandemics, in the context of global development. This took place just after the 2005 H5N1 virus outbreak, which forced EU leaders to frequently gather in Brussels to assess cooperation. On one occasion, at a June 2005 meeting of heads of state and government, they emphasized the need to reached a "strong agreement that EU member states need to coordinate efforts in the face of a risk of a human pandemic" and agreed to "ensure strong coordination and information sharing" to tackle the uncertainties involved in a pandemic outbreak. They also urged the EU institutions, including the Commission, to ramp up coordination efforts.[79] This followed pressure from the European Commission to encourage member states to "coordinate at EU level their preparedness for a pandemic, and to work together if a pandemic occurs."[80]

When the 2009 H1N1 virus outbreak (or the "swine flu") hit Europe, health ministers again agreed to increase coordination. A press release from the Commission on its adoption of the strategy paper on pandemics on 15 September 2009 states that "in order to minimise the negative impact of the pandemic, the Commission highlights the importance of close coordination between EU member states in all related sectors affected by the pandemic."[81] At a meeting on 12 October 2009, health ministers called for, among other demands, national governments to ensure the availability of medicines throughout the EU and its neighbours.[82] Action at the EU level reflected similar strategic statements at national levels.

Expectations emerging out of EU rhetoric

European strategic rhetoric on the pandemic threat indicated a desire to increase EU cooperation on pandemic preparedness. Indeed, it was in the area of preparedness that national leaders identified the EU's most "value added" contribution. The boundary-spanning characteristics of pandemics were often cited: the importance of working collectively to identify and stop outbreaks that "know no borders" is a common refrain. Hence the perception that the EU institutions could play a constructive role in such activities as: monitoring national preparedness, coordinating and streamlining national responses during an outbreak, and ensuring compliance to commonly agreed rules. During implementation of strategic statements, we would expect to see increased communication and information sharing protocols, the sharing of "best practice" amongst national governments, and the expansion of Commission activities in this area.

Policies

Public health and disease control questions have historically been a national concern. However, the intensification of the single market, the increase in the movement of people and goods, and the onset of diseases such as SARS and pandemics influenzas, have exposed shortcomings of cooperation in Europe. This, in turn, led to a surge of EU initiatives and proposals in recent years.

The European Commission adopted its first influenza pandemic preparedness plan in March 2004.[83] This document outlines the respective roles of the Commission and the member states in preparing for a pandemic and discusses the key measures to be taken at certain phases of pandemic outbreaks. It also calls for closer cooperation between human and animal health authorities and experts in the area of influenza virus infections, including sharing of "best practice" in contingency planning.

In the response to the outbreak of the H5N1 virus, the Commission adopted in November 2005 a Communication that sets out the objectives for each inter-pandemic and pandemic influenza phase and the action to be taken to achieve them at both national and Community levels. The outbreak of the H5N1 virus also gave rise to a number of high-level EU emergency meetings on the state of preparedness around Europe. In response to the H1N1 virus, the Commission adopted a strategy paper on pandemics stating that the Commission is working on pandemics in five strategic areas: vaccine development, vaccination strategies, joint procurement of the vaccine, communication with the public, and support to non EU countries. In the Council Conclusions adopted on 12 October 2009 the Commission is asked to review the EU's influenza preparedness and response plan to update national preparedness plans and strengthen intersectoral aspects. The European Commission also plays a key role in facilitating the coordination at the EU level by supporting authorities in member states in their efforts to address pandemic diseases. This is done in particular through regular coordination with national health authorities meeting in the Health Security Committee (HSC). Research policy represents another area where the EU is taking action on pandemic preparedness.

These policy developments, although impressive from a relative perspective, still make up a rather small part of pandemic-related policy across the continent. National planning is still a primary concern. Most EU member states have developed their own pandemic influenza plans, although thoroughness, comprehensiveness, and applicability of those plans are still questioned in some quarters. The EU has encouraged reform of those plans (spurred by the subsequent outbreak of H1N1 flu) but differences remain.[84]

Capacities

What kind of operational capacities have emerged as the result of the prioritisation of pandemic influenza as a security threat? Here we examine four different (but interrelated) categories which are essential components to pandemic preparedness: surveillance, early alert, decisionmaking structures, and early response.

Surveillance

One area where EU governments have entrusted more power to the European level is surveillance. Towards that end, the ECDC was created in 2004 to "identify, assess, and communicate current and emerging threats to human health from communicable diseases."[85] The ECDC was also charged with mobilising and reinforcing synergies between the existing national centres for disease control. In the case of pandemic influenza, daily situation reports are prepared for the member states. The ECDC also provides ongoing support to member states and the Commission in terms of outbreaks and response to the crisis. In addition to the ECDC's monitoring role, another EU agency, the European Medical Evaluations Agency (EMEA), reviewed scientific advice on vaccinations and vaccines, continuously monitoring the safety of centrally authorised pandemic vaccines and antivirals. Concurrent to the efforts of ECDC and EMEA, the EU's European Food Safety Agency (EFSA) monitored both the H5N1 and H1N1 outbreaks in relation to animal health and food safety.[86] The Commission has also set up a number of tools to detect communicable diseases and to support member states to respond to these in a coordinated manner, such as the Medical Information System (MedISys), which provides monitoring and early detection of food and feed hazards.

Early alert

Another area of EU operational capacity-building is in the area of early warning and alert. This entails the activities required to notify governments of an impending, and sometimes difficult to detect, pathogen. As part of the Communicable Diseases Network (mentioned above), the Commission operates an Early Warning and Response System (EWRS). The EWRS networks national authorities and provides notifications and recommendations for control measures when an outbreak requiring coordination occurs. EWRS is a web-based system linking the Commission, the public health authorities in member states responsible for measures to control communicable diseases, and the ECDC. It is designed to provide immediate information on outbreaks with possible cross-border consequences to relevant EU actors. Since 2008, the system also allows its users to connect directly to the WHO.[87]

Decisionmaking structures

Decision structures specifically focused on the pandemics include the Health Security Committee (HSC). Established by the Council in 2001, the HSC is chaired by the European Commission and consists of officials of the EU Members States, officials of the Directorate General for Health and Consumers (DG Sanco) and other relevant Commission services and agencies (e.g. ECDC, EMEA) and holds meetings twice a year. During the initial stage of the H1N1 pandemic, the HSC had daily in audio-conference meetings during April and May.[88]

Another set of decision structures related to pandemic outbreaks is the Commission's Health Emergency Operations Facility (HEOF), created in April 2009. This structrure includes (especially during the alert phases of recent events) a 24/7 on-duty function to provide daily reports on the epidemiological details of a situation. It also coordinates management issues, such as measures to be implemented and information recommendations for the public.

Early response

Early response involves actions to stem the tide of an emerging influenza. The Commission has taken steps to boost a common approach to early response, not least through providing common case definitions and recommended response actions. Other examples include: an agreement on advice to persons planning to travel to or returning from affected areas; extension of the surveillance system to identify new cases in the EU; guidelines on case management and treatments and advice on medical countermeasures for health professionals; advice for the general public on personal protective measures agreed and made available to member states in all the official EU languages, regular statements by the HSC and the Early Warning and Response System (EWRS) contact points on school closures and travel advice; and, a statement on 'Vaccination strategies: target and priority groups' agreed by the HSC and the EWRS contact points.[89]

Of course, early response takes place (and must take place, considering the dynamics of a spreading pandemic) within a global framework. The WHO's Global Health Security Initiative (GHSI) group meets with the HSC when necessary, to consider common priorities and challenges.[90] On a more regular basis, the Commission's DG Sanco follows discussions taking place in the various WHO Committees and then adapts EU and national recommendations in line with these.

Strengths and Weaknesses

From a relative perspective, the EU's role in addressing pandemic influenza as a security threat has grown considerably following recent outbreaks. A newfound willingness to delegate authority towards cooperative institutions stems largely from the fact that pandemics cannot be handled by national governments alone. Nevertheless, a tension remains in the relationship between national and EU level responses to pandemics. While national governments tend to agree on the idea of cooperation, they disagree strongly on which policy tools should be used. In particular, legally binding measures were also viewed with scepticism by some member states. Yet the Commission frequently notes the lack of operational planning at local levels in Europe and calls for more active cooperation. Those same reports lament that "member states are protective of national prerogatives and cannot always agree on practical, collective measures."[91] One further problem is that public health crises and in particular expenditure for buying vaccines do not fall within the scope of the EU Solidarity Fund. The H1N1 pandemic flu outbreak demonstrated considerable difficulties in the procuring and sharing of vaccines in some EU countries. Thus, much work remains to be done in regard to getting national governments and EU institutions to work coherently and effectively in the fight against the spread of a major pandemic.

United States

Threat Perceptions

While health threats, including pandemics, were downplayed in the 2002 U.S. National Security Strategy (NSS), the 2006 version devoted more attention to pandemics as a security threat to the United States. The 2010 Quadrennial Homeland Security Review refers to pandemics as a major security threat, alongside other pressing threats such as terrorism, natural disasters, and organised crime. The review argues that pandemics "can result in massive loss of life and livelihood equal to or greater than many deliberate malicious attacks."[92]

In 2005, the Bush administration tasked the Homeland Security Council (HSC), an executive branch coordination council, with developing a new National Strategy for Pandemic Influenza. This strategy rests on three pillars: Preparedness and Communication, Surveillance and Detection, and Response and Containment. While the Strategy seeks to provide a framework for future U.S. government planning efforts that is consistent with the National Security Strategy and the National Strategy for Homeland Security, it also recognizes that preparing for and responding to a pandemic goes is not just a federal responsibility but also involves state and local governments and the private sector.

Expectations emerging out of U.S. rhetoric

The unprecedented move in the United States to view pandemic influenzas as a threat to national security prompts questions. What does such rhetoric imply? A text analysis would suggest a "whole of government" approach to tackling pandemics and their knock-on effects, in a long-term perspective. New policies are likely to be put in place to ensure preparedness at both the federal government level and at the state level. Different geographical regions of the United States may need to be "brought up

to standard" in identifying and reacting to an emerging pandemic. More coordination of state efforts by federal governments may be in order. The security strategies citing pandemic influenza also imply increased budgets and more resources devoted to pandemic preparedness across government. It is interesting to note here similarities between U.S. and EU perceived actions.

Policies

What kinds of policies have emerged from the strategic reorientation of pandemics as a security threat in the United States? Thus far, there has been no attempt to create a nation-wide strategy against the H1N1 flu. Attached to the original Strategy is the Implementation Plan for the National Strategy for Pandemic Influenza, which was released in May 2006. This document intended to support the broad framework and goals stipulated by the Strategy by outlining specific steps toward achieving the goals. As such, the Plan includes 324 action items. The majority of these also include associated time frames and measures of performance.[93] In addition to the National Strategy for Pandemic Influenza there is also the Pandemic Influenza Plan, developed by the Department of Health and Human Services (HHS) in November 2005. This plan includes an overview of the pandemic influenza threat; a description of the relationship of the plan to other federal documents, including the National Strategy for Pandemic Influenza; and outlines key roles and responsibilities as well as needs and opportunities during pandemic outbreaks. Finally, the U.S. government developed in 2009 the National Framework for H1N1 Influenza Preparedness and Response to serve as an integrated H1N1 strategy, including timelines for H1N1 preparedness and response readiness based on four pillars.

Capacities

What kind of operational capacities have emerged against the backdrop of U.S. strategic rhetoric on pandemics? Similar to the EU section above, we will examine here five different, yet often overlapping, categories which are essential components to pandemic preparedness: surveillance, early alert, shared standards, decisionmaking structures, and early response.

Surveillance

The Center for Disease Control and Prevention (CDC), headquartered in Atlanta, Georgia, conducts a multi-layered surveillance system for seasonal flu under the Department of Health and Human Services umbrella. These components include viral surveillance, physician surveillance for influenza-like illness, hospitalisation surveillance, summary of the geographic spread of the flu, death numbers from 122 cites, the number of laboratory-confirmed threats from flu among children. During the H1N1 flu pandemic, added surveillance components included reports by states on either laboratory-confirmed hospitalisations and deaths from flu, or syndromic cases.[94]

Early alert

To prepare against a domestic pandemic outbreak, the "the U.S. Government has provided resources to state and local health departments to increase the number of sentinel providers and improve laboratory detection at public health laboratories."[95] The government is reportedly also working closely with the industry to develop rapid diagnostic tests to quickly discriminate pandemic influenza from seasonal influenza or other illnesses. Federal funding for pandemic preparedness to state and local authorities is fragmented however. Because several departments and agencies have separate

grant programs, which comes with its own funding requirements and objectives, state and local health departments face hurdles when seeking to craft comprehensive preparedness plans. In addition to this problem, federal funding for pandemic preparedness has on the whole decreased over the past years.

Shared standards

A score of pandemic plans were crafted at various levels of the U.S. government, ranging from the local to state to federal level. By June 2008 all 50 states had developed influenza pandemic plans and conducted pandemic exercises. Congress provided in 2006 $5.62 billion in federal pandemic funds. Out of this sum, $600 million was specifically appropriated to state and local planning and exercises.[96] At the same time, it has been reported that deficiencies still existed in many of these pandemic plans as of January 2009.[97] Since then, work has continued. During FY 2009, $2 billion in emergency supplemental appropriations for the H1N1 pandemic was allocated, and an additional $5.8 billion made available upon presidential request. Work on shared standards is also taking place through the National Planning Scenarios of the National Preparedness Guidelines, which has pandemic influenza as one of its key scenarios. Furthermore, HHS has already taken steps to coordinate national planning for the Pandemic Influenza scenario by leading two interagency assessments of states' Pandemic Influenza plans.

Decisionmaking structures

Although the federal government has authority of planning and response for pandemics, effectively coordinating action in a multi-level government setting has proved a real challenge. During the H1N1 flu, DHS Director, Janet Napolitano, assumed the role of Principal Federal official, in charge of coordinating federal response efforts. On 24 October 2009, President Obama declared the pandemic to be a national emergency, thus allowing "a temporary waiver of certain standard Federal requirements . . . in order to enable U.S. health care facilities to implement emergency operations plans" and temporary waivers of certain requirements of the Medicare and Medicaid. During the H1N1 pandemic, the National Emergencies Act was used for the first time to enable waivers, allowing for patients with flu symptoms to access alternate facilities rather than hospital emergency rooms. However, no presidential declaration was made under the so-called "Stafford Act," so additional federal intervention was limited.[98] Another decisionmaking apparatus relevant to pandemic influenza is the National Response Framework (NRF). In principle, an influenza pandemic could trigger the NRF, especially if the appearance of the disease in the United States is in multiple communities crossing state lines. That would lead to an intense multi-party containment effort led by the federal government.

Early response

The National Strategy for Pandemic Influenza sets out goals with regard to vaccine stockpiling: the first is to stockpile enough H5N1 pre-pandemic vaccines to immediately vaccinate 20 million people; the second is to be able to inoculate the entire U.S. population within six months of a pandemic influenza outbreak. After the outbreak of the H1N1 flu, the United States quickly began preparing for H1N1 vaccinations, clearing vaccines for sale, and purchasing vaccines. Between May and September 2009, HHS had purchased over $2.25 billion worth of H1N1 vaccines. The federal government,

through the CDC, then distributed the vaccines to the states on a per capita basis, beginning in early October. However, massive delays were encountered in the vaccine supply, complicating the efforts of state and local officials and health care providers to vaccinate people.[99] This had partly to do with the limited U.S. vaccine production capabilities and the huge costs of vaccinating the entire population.[100]

Strengths and Weaknesses

In taking a strategic approach to pandemic preparation, the U.S. government raised the issue to the top of federal and state agendas. Identifying pandemics in the National Security Strategy, and stipulating action in the National Strategy for Pandemic Influenza, set out clear goals for raising the capacity of the United States to withstand a major pandemic. Those goals garnered praise from some quarters, for providing a "useful...guide for action and policy decisions" both within the federal government and concerning private industry.[101]

In other areas, however, U.S. rhetoric has not been coupled with action. Some argue that U.S. plans are not ambitious enough when it comes to setting out objectives for vaccine production and specifying how priorities for vaccination and distribution of anti-virals would be established. The U.S. Government Accountability Office (GAO) has repeatedly warned of shortcomings with the National Strategy for Pandemic Influenza and its Implementation Plan. In particular, the Plan does not establish priorities for the implementation of the 324 action items nor does it provide information on the financial resources required to implement the Plan.[102] GAO has also observed that the Plan "lacked a prescribed process for monitoring and reporting on progress" and lacking information on state and local governments and other non-federal entities.[103] Apparently, implementation of the Strategy and the Plan has also been uneven.

Transatlantic Developments

Common Policies and Strategies

Transatlantic policies on pandemic preparedness are fairly rare, since the WHO takes the lead in issuing policy decisions and advise during a pandemic. The EU and United States are amongst the more active members of the WHO, working together on a number of issues and conveying the message openly that preventive measures and preparedness plans need to be in place at home and abroad. For instance, both the EU and the United States take a leading role in promoting global pandemic preparedness. On 14 September 2005 President George W. Bush announced the creation of the 'International Partnership on Avian and Pandemic Influenza' (IPAPI), seeking to bring together "countries that share a set of core principles to generate and coordinate political momentum for addressing avian and pandemic influenza." The EU also takes a global role in pandemic preparedness through, for example, participating in regular meetings with senior health officials from across the world.

Existing Cooperation Mechanisms

Cooperation between the EU and United States takes place largely, but not entirely, within the WHO framework. Other mechanisms bring transatlantic officials together to tackle common problems. One such venue is the Global Health Security Initiative (GHSI), which includes the G7 members, Mexico

and the European Commission. It functions as an informal forum for sharing information on broader issues linked to health security, requiring exchange of information and dialogue. The senior officials' network, comprised of health ministers, is carried out by working groups and networks, one of which is on pandemic influenza. During the H1N1 pandemic flu, the GSHI network proved to be an effective platform for rapid communication and dialogue on approaches to vaccine production and vaccination strategies between all the members as well as on a bilateral level. Joint training and planning has also been carried out between the GSHI members. The Commission is currently set to organise a joint GHSI-HSC exercise in 2010 to share good practices, foster mutual learning, and develop contacts. The GHSI has also brought together the EU and some international partners, including the United States, in a project on early alerting and reporting. The Commission has previously also hosted a meeting of the GHSI in Brussels in September 2009.

Operational Aspects

For the preparation of strategies for the assessment and authorisation of vaccines the European Commission, the ECDC and the EMEA work in close contact with the WHO and other regulatory authorities worldwide. Furthermore, the Commission and the EMEA concluded bilateral confidentiality arrangements with regulatory agencies of three third countries (United States, Canada, Japan) for enhanced regulatory and scientific collaboration. These agreements have proved a useful mechanism for information exchange in the recent H1N1 pandemic. The ECDC has reportedly also been in close contact with the U.S. CDC during the H1N1 pandemic influenza to cooperate and coordinate policies.[104] For example, a video conference was held on 22 September 2009 to discuss the approaches to the flu. Since 2007, the CDC has also placed staff at the ECDC. With the acceleration the H1N1 pandemic, this exchange of experience has included ECDC staff seconded to the CDC. Through the WHO Collaborating Centre for Reference and Research on Influenza, the CDC influenza laboratory also cooperates with the National Institute for Medical Research, located in the UK, on exchanging viral samples, among other things. Moreover, during the H1N1 pandemic influenza outbreak, the EMEA, in the preparation of a scientific assessment of vaccines, exchanged views with registration authorities in third countries, including the United States.

Another cooperation mechanism put in place during the November 2009 EU-U.S. Summit in response to the H1N1 flu pandemic was a transatlantic task force on antibiotic resistance. The objective of the task force is to improve the pipeline of new antibiotics in support of existing cooperation between the ECDC and the CDC. Transatlantic cooperation on pandemics has also taken place through the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), a "24/7" coordination centre for disaster relief efforts among NATO member and its partner countries, located in NATO headquarters in Brussels.

Missing Transatlantic Links?

The case studies have illustrated that the EU and the U.S. perspectives on pandemic flu outbreaks are fairly well-aligned. They both share similar perspectives on pandemics as an issue transcending traditional, contentious security questions that normally divide the two blocs. Moreover, they both share the view of pandemics as a global phenomenon that requires global cooperation.

One difference between the two blocs is the rhetoric deployed in their respective strategic documents. The United States is more prone to frame pandemics as a "security threat." The EU, perhaps wary of divisive effects of "securitizing" new threats, mentions pandemics in security-relevant documents but shies away from over-using the word "threat." Both see the relation between preparing for pandemics and preparing for other large-scale public health emergencies, such as an anthrax attack. This realisation, it should be noted, has led to increasing references to an "all hazards" approach in many of the strategic documents.

The main institutional framework for transatlantic cooperation on pandemic influenza is the WHO. The EU and United States have no regular, institutionalised mechanisms for cooperation on a bilateral basis. The explanations behind this gap are two-fold. First, it is arguable that WHO cooperation is working sufficiently well to bring Europe and North American together, so as not to warrant new cooperation frameworks. Most research suggests that EU and U.S. cooperation works well through the WHO, and they are both leaders within that organisation.[105] Second, there are few EU institutions (specifically, agencies) with enough power or maturity to justify direct EU-U.S. links. For example, the ECDC, in its current form, is not comparable to the size or authority of the U.S. CDC. This makes relationships between the two agencies of secondary importance to U.S. relations with the WHO, or with individual EU member states. The Lisbon Treaty brought more authority to the supranational level in the area of public health, and EU agencies are constantly growing, but the national level remains the most potent partner for the United States on the question of pandemic preparedness.

It is in the area of common policies that the alignment between the EU and United States is difficult to detect, namely because there are few bilateral policy agreements. Most joint policymaking takes place through the WHO. Still, if we assess the compatibility of respective EU and U.S. policies, there appears to be good news to share. EU and U.S. policy approaches to preparing for a pandemic influenza are broadly similar (owing to the influence of the WHO, arguably, and the global nature of scientific advice). For example, both the 2009 EU Commission's Strategy Paper on Pandemic (H1N1) and the U.S. National Framework for 2009-H1N1 Influenza Preparedness and Response emphasise similar priorities: access to vaccines and public communication. Both the EU and the United States also actively support other countries in their efforts to prepare and respond to pandemics. Policy approaches have also been exchanged regularly at the GSHI meetings where both the EU and the U.S. Commission are participants.

We note potential "lessons learned" for both the EU and the United States, not least in how policy decisions are implemented and with what consistency and effectiveness. We explore this argument below.

Finally, we note that operational alignment in the transatlantic relationship appears to be working rather effectively. At the expert level, the EU and United States regularly share governmental experts and specialist scientists (between the ECDC/CDC and EMEA/FDA, for example). On the question of vaccine administration, both blocs faced similar problem with production and distribution. Critics on both sides of the Atlantic call for a more centralised control of vaccinations during pandemics. In Europe, this suggests a larger EU role, specifically for the ECDC. In the United States, this would be accompanied by clearer information to state and local public health authorities to smooth

comprehensive pandemic preparedness plans. Given the multinational character of many vaccine providers, these problems will need to solved in a transatlantic context, as we explore below.

One source of operational tension in the transatlantic relationship should be noted: conflicting travel warnings. Conflict emerged when EU health officials warned against travel to the United States, although the United States had used a similar risk assessment procedure in barring citizens from "non-essential travel" to Mexico. Both recommendations were made in contradiction to WHO recommendations against closing borders and restricting travel.

Conclusion and Recommendations

Enhancing EU-U.S. Shared Perspectives

This paper showed that EU and U.S. strategic perspectives on pandemic influenza are highly convergent. Both entities have included pandemics in their respective security strategies, and each has vowed to take extraordinary action to protect societies from a threat that easily crosses the internal/external frontier. In this respect, there is no immediate need to improve shared perspectives or strategic rhetoric between the EU and United States.

However, there may be a temptation on either side of the Atlantic to de-prioritise pandemic influenza as the threat appears to recede from view. Policymakers should guard against this temptation, since although a full-scale pandemic may be low probability, most experts agree it would be a high risk. Most, if not all, of society's resources would need to be directed toward managing a pandemic and those resources would need to be coordinated in an effective fashion. Moreover, management of a pandemic must be done in a way that limits "knock-on" or unintended "ripple" effects. Such challenges speak to a continued prioritisation of pandemics on both sides of the Atlantic.

Finally, policymakers and analysts curious about comparing the dynamics between internal security threats and external security threats would be wise to explore the question of pandemic influenza. A pandemic can be viewed as a "domestic health issue" as well as a "international security threat," and requires an effective mobilisation of national and international resources to effectively combat it. For policymakers interested in providing security in a globalised world, there is no better "stress test" than pandemic influenza.

Improving EU-U.S. Coordination Mechanisms

Our assessment of transatlantic pandemic cooperation illustrates that current cooperation mechanisms through the WTO and the GSHI are rather effective. This would suggest that any move towards building new cooperation mechanisms solely between the EU and United States be subject to scrutiny to demonstrate a clear "added value." However, special attention should be placed on the transatlantic relationship in the following ways.

First, the EU and United States should operate as a constructive leadership team within other international organisations. When cooperating effectively, the two blocs can move most initiatives in a consensual and speedy fashion. That cooperative relationship should be nurtured (through regular caucuses of EU and U.S. officials before and during WHO events, for example) and encouraged (through partnerships with officials from international organisations).

Second, bilateral cooperation mechanisms can be useful and effective on issue-specific questions. For example, the 2009 Transatlantic Task Force on Antibiotic Resistance seems to have played an important role in motivating both political attention and new medical research on a narrow (but serious) issue associated with pandemic preparedness. Another example is the existing network is the Transatlantic Biosecurity Network, which consists of a group of medical, public health, and national security experts from North America and Europe who have been meeting since early 2002.[106] EU and U.S. officials should not hesitate to form such expert working groups and task forces when specific needs arise.

Assessing EU-U.S. Policy Compatibility

This paper found few policy agreements directly between the EU and United States on pandemic influenza preparedness. Most policy agreements take place via the WHO. This is not an entirely satisfactory arrangement. On specific issues, transatlantic policy agreements could go a long way towards identifying potential problems and avoiding tension. One such issue is on the question of vaccine production and distribution. With most vaccine producers operating across international borders (particularly in Europe and the United States), a common policy would avoid unnecessary market competition, "beggar thy neighbour" behaviour, and an equitable distribution of vaccines in the event of a global emergency.

Not all policies will need to be shared between the EU and United States, which directs our attention to the compatibility of their respective policies. Here we encourage increased communication and the sharing of "best practices" to ensure that difficult lessons learned on either side of the Atlantic can be used for mutual benefit. One idea is to initiate a series of conferences (either one-off or as part of a task force format) to bring together EU and U.S. policymakers together with public health officials and scientific experts. Discussion would focus on respective experiences, and respective policy successes (and failures) during the recent swine flu outbreak.

Lastly, both the EU and United States suffer from similar problems. Policy implementation deficits (when centralised decisions are ignored or neglected by constituent political units) and uneven levels of capacity development (when different parts of a polity are not evenly prepared for a pandemic) affect both the EU and United States. Here, important lessons can be learned across the Atlantic to improve matters.

Enhancing EU-U.S. Operational Coordination

We should not neglect the importance of transatlantic cooperation "on the ground," amongst public health officials and epidemiological experts before and during a crisis. Our study found that operational coordination on pandemic influenza functions reasonably well in a transatlantic perspective. However, there is still room for improvement on several counts.

First, the EU and United States should assess existing mechanisms of communication and information exchange across the Atlantic. Those mechanisms should be assessed for their effectiveness and functionality during a pandemic outbreak. This points towards a much broader perspective: how well the EU and United States are coordinated across their respective governance systems. Although much criticism is often lodged at the EU, including its unclear mix of national governments, European institutions, and European agencies, we note a similar problem exists in the

United States, including jurisdictional overlaps and potential confusion between the Department of Health and Human Services and Department of Homeland Security. Both blocs should be encouraged to get their own "houses in order" and designate transatlantic communication and information sharing mechanisms appropriately.

Second, the EU and United States could enhance operational cooperation on health threats through joint exercises and trainings. One successful example is the January 2005 Atlantic Storm exercise, which featured an international bio-terrorism scenario and high level leaders carrying out a mock-response on both sides of the Atlantic.

Third, the EU and United States could increase operational cooperation on developing new vaccines and treatment guidelines. The fluid and regular exchange of experts has worked well in the past, and should be prioritised in the future.

NATURAL DISASTERS: STRATEGIC RHETORIC AND PRACTICAL ACTION IN THE EU, U.S., AND TRANSATLANTIC PARTNERSHIP

Rick "Ozzie" Nelson, *Director, Homeland Security and Counterterrorism Program, and Senior Fellow, International Security Program, CSIS*, and Ben Bodurian, *Research Assistant, CSIS*

Introduction

The human costs of natural disasters are well-known. The January 2010 Haiti earthquake has accounted for around 250,000 fatalities, drawing comparisons to the equally-tragic 2004 Indian Ocean tsunami, which killed more than 230,000 people. And natural disasters do not merely strike poor or developing countries; the 2010 Chilean earthquake killed more than 500 people, and more than 1,800 people died in Hurricane Katrina on America's Gulf Coast.

According to a 2007 Intergovernmental Panel on Climate Change report, future geologic changes are likely to lead to more extreme weather events, which may lead to more frequent natural disasters.[107] In addition, the growth of large cities located in fault zones is only likely to increase the human effects of major earthquakes. All of these factors come together at a time when the rise of globalization ensures that disasters like earthquakes, floods, and tornados affect individuals from a range of countries and backgrounds (hundreds of non-Haitians, including 104 Americans, died in the January earthquake; nearly 2,000 Europeans were killed during the 2004 tsunami). In short, large-scale natural disasters cannot simply be thought of as isolated or contained events, because they often result from global environmental phenomena, like climate change, and can wreak havoc in places far removed from the center of crisis.

How, then, have the EU and United States approached disaster preparation and response? What have been the key documents that articulate strategies and plans to deal with large-scale natural disasters? How successful have the EU and United States been in their efforts to implement these policies? And how effectively have both entities worked together to plan for and respond to natural disasters?

Strategic Rhetoric and Practical Action in the EU and United States

The European Union

In the past several years, there has been an important evolution in the treatment of natural disasters in EU security policy. Disaster preparation and relief have assumed greater importance in high-level official documents and public declarations. Accordingly, EU institutions have looked to take a stronger role in ensuring collective security on the continent.

The 2003 European Security Strategy (ESS), the EU's first major post-9/11 articulation of grand strategy, did not explicitly mention the role that natural disasters play in endangering public safety and destabilizing societies. The document did make a fleeting reference to climate change, which may increasingly spur natural disasters, but did so only to discuss its impact on resource competition.[108] Instead, threats like terrorism, weapons of mass destruction (WMD), and state failure dominated the 2003 ESS. Much of this had to do with time and context, since the ESS was published just over two years following the September 11 attacks. Indeed, two additional documents in this same time period—the EU Strategy Against Proliferation of Weapons of Mass Destruction,[109] adopted at the same time as the ESS, and the 2005 EU Counter-terrorism Strategy[110]—reinforced Europe's rhetorical focus on "hard" security threats like proliferation and extremist violence.

Instead of major strategy documents like the ESS, EU disaster policy in the early 2000s focused on more modest initiatives. The most important of these has been the Community Civil Protection Mechanism (CPM), established through the European Council Decision of October 23, 2001. The program helps to facilitate disaster relief among EU member states; one of its main features, the Monitoring and Information Centre (MIC), is a round-the-clock "communication hub" that provides updated information on major disasters inside and outside of Europe.[111] The CPM has been activated on numerous occasions, including during floods and forest fires in southern EU states, the Indian Ocean tsunami, and the Haitian and Chilean earthquakes. Through these incidents, it has tended to support, rather than lead, EU countries' relief efforts.

During the middle of the decade, natural disasters gained greater prominence in high-level official documents. The European Constitution, drafted in 2004, was set to include a "Solidarity Clause" committing member states to assist one another in the event of terrorist attacks and natural or man-made disasters. Though French and Dutch voters rejected the European Constitution, the Solidarity Clause survived largely unscathed in the Lisbon Treaty, which came into force in December 2009. Known as Article 222, the Solidarity Clause broadens EU conceptions of mutual assistance following natural disasters. It calls for the EU to "mobilise all the instruments at its disposal," including military means, in the event of a terrorist attack or disaster. Unlike the CPM, which promises merely to facilitate disaster relief among willing member states, the Solidarity Clause compels states to assist if a fellow government requests help.[112]

2010 brought yet more recognition of the importance of disaster preparation and relief in European grand strategy. The Internal Security Strategy (ISS), released in February, took pains to highlight the place of natural disasters among an array of threats. It called for the development of risk management guidelines and for an outline of the future threats that disasters may pose. In addition,

the ISS touted the success of the CPM, but called for a greater degree of cooperation between member states and the EU on civil protection. This proposal, like the Solidarity Clause, would seem to elevate EU institutions and make them co-equal partners with member states in coordinating relief efforts.

Over the last ten years, then, there has been an important shift in the way disaster preparation and relief feature in high-level EU documents. Early rhetoric tended to focus predominantly on topical threats like terrorism and WMD. Meanwhile, modest but important programs like the CPM allowed the EU to support member states' relief efforts. Over time, EU rhetorical narratives have come to increasingly recognize natural disasters as central threats to security on the continent. These official declarations now have given way to ambitious plans to enhance collective efforts and ensure a more significant role for the EU. What sort of practical action might emerge from this change in strategic rhetoric?

For the Solidarity Clause, the first step is developing the "implementation arrangements" that will clarify the terms and conditions of the admittedly broad Article 222. Among other considerations, there remain unanswered questions about the types of threats covered by the Clause, its scope, and its legal implications. EU officials will have to allay the concerns of member states worried about how obligatory assistance may restrict national sovereignty, or that especially-vulnerable countries may simply "free-ride" and take advantage of guaranteed support. The Solidarity Clause also must address the clear shortcomings of existing systems like the CPM. No event better illustrates these deficiencies than the summer 2007 forest fires, in which over 810,000 hectares of land were burned. In a span of 11 weeks, Bulgaria, Cyprus, Greece, Italy, Albania, and the Former Yugoslav Republic of Macedonia appealed to the CPM a combined 12 times. Member states offered support, primarily through "aerial fire fighting, fire-fighting equipment [sic], protective clothing, and expertise." But such assistance was limited since "fires were raging at the same time in several Member States and the risk of fires was high in other Member States," thus decreasing the number of European countries able to provide support.[113] And with no obligation for member states to provide support, there could be no guarantee that countries unaffected by the fires would offer assistance.

The Solidarity Clause looks to avoid such scenarios by obligating all EU member states to pledge support upon request by a fellow government. Making this stipulation workable will require that EU officials clearly spell out the expectations of member states prior to the occurrence of a disaster, possibly by specifying a pre-determined "threshold" for triggering the Clause. This threshold could apply to cross-border disasters that affect multiple states, like the 2007 forest fires, or could be based on the size and scope of given disasters. Above all, the key will be to spell out exactly what is expected of member states in order to clarify their expectations about the type of support they should be ready to provide and receive.

But even given a robust "implementation arrangements" process, the Solidarity Clause is unlikely to address all, or even most, of the important policy questions raised by natural disasters. Consider, for instance, the volcanic ash cloud during the spring of 2010. Unlike with floods or forest fires, European governments could do nothing to mitigate the ash cloud—they were forced to simply wait until the ash dissipated. The major lesson to emerge from that event was not about disaster relief, per se, but rather about the difficulty and costliness of trying to coordinate the policies and procedures of 27 different national airspaces in a time of confusion (the decision of whether to ground planes, after all, rests with member states, not the EU). In this sense, an important, if underappreciated, element of

natural disaster policy will be ensuring that the EU has political, legal, and commercial systems and processes in place that are impervious to various types of disruptions.

The United States

Policymakers in the United States also have increasingly highlighted the threat that natural disasters pose to national and global security. High-level strategic documents have moved to frame disaster preparation and response as part of an "all-hazards" and "whole-of-government" approach to security. This ambitious framework requires heightening coordination and cooperation between the myriad constituencies in charge of responding to and managing disasters and other threats.

The September 11 attacks spurred an important reconsideration of America's national security structures. Policymakers in the Bush administration readily acknowledged that a complex tangle of bureaucracies, many with overlapping or unclear mandates, had complicated efforts to prevent the attacks. For instance, the first ever National Strategy for Homeland Security (NSHS), released in July 2002, noted that at least five different plans framed the federal government's response to serious emergencies. As a remedy, the document called for the development of "inter-connected and complementary systems" to replace those that were redundant or contradictory.[114]

Most of these proposals revolved around counterterrorism. Accordingly, other sorts of threats to domestic security, like natural disasters, received less attention in the document. Still, the NSHS did state that the United States would work to develop a response framework that was "adaptable enough to deal with any terrorist attack…as well as all manner of natural disasters" while also involving state and local officials, in addition to those at the federal level, in preparedness and response initiatives.[115] These proposals signaled the government's willingness to expand the frame of reference for dealing with large-scale threats beyond the narrow constructs of terrorism.

Such high-level policies began to take shape in early 2003. The newly-established Department of Homeland Security (DHS) consolidated 22 government agencies into a single cabinet office. This reorganisation was especially important for disaster preparation and relief in that it placed FEMA, the Federal Emergency Management Agency, under DHS control. Soon after the establishment of DHS, President Bush signed Homeland Security Presidential Directive 5 (HSPD-5) directing the creation of a coordinated domestic incident management system; its two primary components were to be called the National Incident Management System (NIMS) and the National Response Plan (NRP). The former provided a "core set of concepts, principles, terminology, and technologies" to federal, state, and local officials in charge of disaster preparation and relief.[116] The latter, meanwhile, looked to integrate the government's "prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan."[117] Together, the two initiatives comprised an ambitious plan to unify an otherwise-sprawling, disparate set of federal, state, and local actors. And, as referenced by the language describing the NRP, HSPD-5 envisioned an emergency response framework that encompassed many different types of security threats.

These reforms proved insufficient to prepare for, and respond to, a large natural disaster like Hurricane Katrina, which made landfall in August 2005. A February 2006 White House report catalogued numerous shortcomings in the government's approach to that hurricane and to natural disasters more broadly, including gaps in national preparedness, communications, and logistics and

evacuations. The NRP came in for particular criticism; the report labeled the initiative "far too bureaucratic" to be of any use in response efforts.[118]

This and other critiques led to the Post-Katrina Emergency Management Reform Act of 2006. The legislation particularly targeted FEMA, which as a December 2006 Congressional Research Service (CRS) report noted, may have suffered following the move to DHS. Interestingly, the CRS report paraphrased some critics of the post-9/11 homeland security reforms as arguing that "an emphasis on terrorist-caused incidents within DHS dominated planning and allocations decisions and contributed to FEMA's diminished capabilities for all hazards."[119] The Post-Katrina Act restored some of FEMA's autonomy, classifying the agency as a "distinct entity" within DHS, like the Coast Guard and Secret Service. In addition, the bill looked to bolster FEMA's disaster response capabilities by creating new entities such as Urban Search and Rescue teams and the Metropolitan Medical Response Grant Program. Also, in recognition of the lack of federal-state-local cooperation during Katrina, the legislation mandated that ten regional offices operate within FEMA.[120] These entities include staff dedicated to operational planning and are particularly useful in improving coordination between federal, state, and local officials.[121]These post-Katrina reforms were reflected in the 2007 version of the National Strategy for Homeland Security, where natural disasters received far more attention than in the 2002 NSHS. The opening paragraph of the 2007 NSHS acknowledged that the United States was still "at war" with terrorists but took pains to note that other catastrophes, particularly natural disasters, also threatened the American people.[122] Beyond this rhetorical shift, the 2007 NSHS outlined revisions to presidential directives, like the NRP, that had failed during Hurricane Katrina.[123] In a January 2008 report describing the National Response Framework (NRF), the NRP's successor, DHS officials acknowledged that the NRP had struggled to integrate state and local governments and had failed to provide a "true operational *plan*," thus betraying its very title [their emphasis].[124]

The NRF, which took effect in March 2008, looked to improve on these shortcomings by expanding coordination between all levels of government, the private sector and nongovernmental organisations, and even families and individuals. A November 2008 CRS report suggested that the NRF performed well during Hurricanes Gustav and Ike and that federal-state-local cooperation had generally improved.[125] As the report quickly pointed out, though, Gustav and Ike were far less serious than Katrina, and so it was difficult to truly assess the NRF's competence. On a larger level, the report raised a number of challenges that the NRF faces in the coming years, including the need to further clarify federal, state, and local roles during disasters.[126] The Obama administration has grappled with this and related challenges since taking office. In February 2010, Secretary of Homeland Security Janet Napolitano released the country's first Quadrennial Homeland Security Review (QHSR), pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007. Early in the document, DHS officials referred to the "homeland security enterprise" to emphasize that actors beyond the federal level must play a vital role in ensuring domestic security.[127] In a follow-up document, the Bottom-Up Review, released in July 2010, DHS elaborated on the specific initiatives it has in place to further integrate non-federal entities into the country's disaster preparation and response framework.[128] Moving toward this type of "whole of government" approach to natural disasters will play an important role in deliberations over DHS's FY 2012-2016 future operating budget. And how

well DHS successfully integrates its non-federal constituencies will help determine, to an important degree, the success of future action to deal with disaster preparation and response.

Strategic Rhetoric and Practical Action in a Transatlantic Context

The EU and United States, as global leaders, play an essential role in disaster relief outside their own territories. Such assistance takes myriad forms and gives rise to frequent pledges of increased transatlantic cooperation. Thus presents a formidable challenge for EU and U.S. policymakers: enhancing coordination on disaster preparation and relief so that reality can match rhetoric.

Much of today's architecture for transatlantic and multinational disaster response has roots in the 1990s. In December 1991, the United Nations General Assembly passed Resolution 46/182, which established the Office for the Coordination of Humanitarian Affairs (OCHA). OCHA focuses broadly on emergency response and has played a key role in coordinating international relief efforts following natural disasters, especially in developing countries.[129] Four years after OCHA's founding, as part of discussions on the New Transatlantic Agenda, leaders in the EU and United States developed the Joint EU-U.S. Action Plan. The highly-rhetorical framework expressed broad support for peace, stability, human rights, and free markets. It also pledged to increase transatlantic coordination in humanitarian assistance and other emergency response efforts in the developing world.[130] In 1998, the Euro-Atlantic Partnership Council (EAPC), NATO's consultative body for members and partner countries, developed a new policy on "Enhanced Practical Cooperation in the Field of International Disaster Relief." It included two main components: a Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and a Euro-Atlantic Disaster Response Unit (EADRU). The former is an office at NATO headquarters that serves as the "focal point" for coordinating the relief efforts of NATO members and partners for disasters occurring in the Euro-Atlantic area. The latter is a "non-standing, multi-national mix of national civil and military elements" culled from EAPC countries and deployed in the event of a large-scale disaster.[131] The EADRCC touts its involvement in international disaster relief—its website notes that it has helped coordinate response efforts in at least 45 emergencies—and stresses that it plays a supporting role to OCHA during all of its missions.

To varying degrees, the EU and United States had stakes in all of these new creations. And, on some level, all of these initiatives reflected the post-Cold War thinking about how developing, fragile, or failed states could impact the advance of a peaceful, liberal, and free market-oriented global system. In addition to the intrinsic value of humanitarian assistance, one of the premises supporting the rhetoric on emergency preparedness was that instability following disasters and other emergencies could lead to civil or inter-state violence, transnational crime, or terrorism. This concern was especially prominent in the Joint EU-U.S. Action Plan, and helped animate that document's frequent paeans to transatlantic cooperation.

The September 11 attacks extended this line of thinking. Both the United States National Security Strategy (NSS) of 2002 and the 2003 European Security Strategy (ESS) stressed that cross-boundary threats required transatlantic solutions. The NSS stated that the United States could accomplish "little of lasting consequence" without support from allies like the EU.[132] The ESS described the EU-U.S. partnership as "irreplaceable."[133] While neither of these documents explicitly discussed bilateral

coordination on disaster relief, they reinforced EU and U.S. rhetorical commitments to joint security efforts.

The EU and United States would soon have to demonstrate their commitment to joint action in disaster relief. On December 24, 2004, an earthquake off the west coast of Sumatra, Indonesia caused a massive tsunami. The disaster affected 14 countries, killed an estimated 230,000 people, and triggered an intense outpouring of support from the international community. The EU Commission, EU member states, and the United States provided substantial manpower and financial assistance. A January 27, 2005, BBC News article noted that within one month of the disaster, member states like Britain (two RAF planes, a C-17, and a Tristar) and Germany (a military ship with two helicopters) had joined the United States (12,000 personnel, 21 ships, 14 cargo planes, and more than 90 helicopters) in providing military assets to distribute food and supplies.[134] By December 2005, the EU and its member states had pledged more than €2 billion in assistance.[135] Two years later, the U.S. Agency for International Development (USAID) pegged the American contribution at $841 million.[136] While the myriad sources of assistance make it difficult to estimate a total for overall levels of aid, EU and U.S. efforts accounted for a substantial percentage of the total volume of contributions.

The large and multi-faceted relief effort helped ensure that Indonesia, Sri Lanka, India, and other countries affected by the tsunami could have some chance of recovering. At the same time, though, the scale of the response made coordination especially difficult. A July 2006 OCHA report noted that the "roles, responsibilities and decisionmaking authority of participants were often not spelled out, leading to a sometimes unproductive mix of information sharing and decision making." Continuing, the authors remarked that there was "little evidence in the first months of either direction or management with respect to cross-sectoral integrated resource allocation."[137]

Incidentally, the UN-convened World Conference on Disaster Reduction came on the heels of the Indian Ocean earthquake and tsunami. Held January 18-22 in Kobe, Hyogo, Japan, the gathering was intended to measure progress on disaster policy in the intervening years since the Yokohama Conference of 1994. The convention adopted the Hyogo Framework for Action 2005-2015, which outlined five key priorities relating to risk management, resilience, and preparedness.[138] Both the EU[139] and United States[140] issued statements at the conference which expressed support for the development of a global tsunami warning system.

Soon enough, EU and U.S. rhetoric on enhanced coordination would again be put to the test when Hurricane Katrina made landfall in the Gulf Coast in August 2005. As its severity became more apparent, more than 150 countries and international organisations came forward to offer support to the relief efforts including NATO support through the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). Between September 12 and October 2, NATO pilots delivered nearly 189 tons of emergency supplies.[141] Still, international relief efforts faced hurdles. The White House's own February 2006 "Lessons Learned" report provided a frank assessment, noting that the United States was "not prepared to make the best use of foreign support" because of an inability to "prioritize and integrate such a large quantity of foreign assistance into the ongoing response."[142] Most recently, the EU, U.S., and other international partners came together to offer assistance when a massive earthquake struck Haiti near its capital, Port-au-Prince. 250,000 people are thought to have died. More than a year later, the recovery still lags. In the aftermath of the earthquake, the EU and United States both have offered substantial support to Haiti. In January 2010, the EU Commission set aside

€429 million for relief efforts.[143] And the U.S. commitment exceeded $1.1 billion for fiscal year 2010. In addition, the U.S. Coast Guard, Navy, and Air Force have played an active role in ensuring stability in the months following the disaster.[144] On the ground in Port-au-Prince, though, international coordination did not come easily. Despite the immeasurable benefits provided by rapid relief efforts, a July Inter-Agency Standing Committee Report noted that "the arrival in Haiti of a plethora of humanitarian actors with varying capacities, resources and agendas" led to a "coordination deficit" in the early stages of the response. The report chided the EU, United States, and other international entities for not "adequately engage[ing] with national organisations, civil society, and local authorities." Finally, the report echoed the July 2006 OCHA report on the tsunami by alleging that there was little coordination between the strategic and operational levels of the response.[145]

Such criticism provides the basis for a number of recommendations for EU-U.S. policy on disaster relief:

- Above all, effective coordination among all parties involved must be the *sine qua non* of any large-scale disaster relief effort. Response efforts for the Indian Ocean tsunami, Hurricane Katrina, and the Haiti earthquake, while remarkable for their size and scale, would have been more effective with better coordination among foreign governments, non-governmental organisations, and host nation officials.
- In conjunction with the UN, the EU and United States need to do more to identify the capacities, specialties, and limitations of various response stakeholders before disasters strike; this will help minimize redundancies and ensure that no vital needs go unaddressed. To the greatest extent possible, there needs to be a unity of effort.
- Finally, especially in cases where disasters occur in developing or poor countries, the EU and United States need to do a far better job of integrating local officials into the response effort. Recent lessons from Haiti show that local officials provide the essential language, cultural, and social know-how to connect Western experts with the people most in need of help. None of these measures will guarantee seamless response efforts. It will be near impossible to improve on current approaches, though, without enhancing across-the-board coordination among the full range of concerned stakeholders.

Notes

[1] European Union, A secure Europe in a better world, European Security Strategy, Brussels, 12 December 2003.

[2] European Union, *Report on the Implementation of the European Security Strategy: Providing Security in a Changing World*, Brussels, 11 December 2008.

[3] European Union Council, *Statement on tighter international security*, Brussels, 3 December 2008.

[4] European Union Council, *Internal Security Strategy for the European Union: "Towards a European Security Model*," 25 February 2010. See also the EC Communication, *The EU Internal Security Strategy in Action: five steps towards a more secure Europe* COM(2010) 673, 22 November 2010.

[5] Even if quite intuitive, an explicit definition of this term could not be found even in policy documents.

[6] Our attention will here focus on the first three aspects. For further information on the regulatory side, see, *inter alia*, European Commission, Proposal for a *Regulation of the European Parliament and of the Council establishing the European Electronic Communications Market Authority*, Brussels, COM(2007)699.

[7] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *A Strategy for a Secure Information Society—"Dialogue, partnership and empowerment*," Brussels, COM(2006)551, p. 3 It recalls the previous communication *Network and Information Security: Proposal for A European Policy Approach*, Brussels, COM(2001)298.
[8] European Commission, *Green Paper on a European Programme for Critical Infrastructures Protection*, 2005, Appendix I. The process of identifying European Critical Infrastructures launched with the Council Directive 2008/114 has focused so far on the energy and transport sectors. However, Information and Communication Technology (ICT) will be the next priority.
[9] Ibid.
[10] Europol, High Tech Crime Centre, *High tech crimes within the EU, Threat assessment 2007,* August 2007.
[11] European Commission, Communication from the Commission to the European Parliament, the Council and the Committee of the Regions *"Towards a general policy on the fight against cyber crime"* COM(2007)267.
[12] At the end of September 2010, EU Commissioners Cecilia Malmstrom (Home Affairs) and Neelie Kroes (Digital Agenda) presented two proposals for new directives on attacks against information systems and on ENISA. The former would introduce more severe criminal sanctions for the perpetrators of cyber-attacks and the producers of related and malicious software and compel member states to quickly respond to urgent requests for help in the case of cyber-attacks. See http://ec.europa.eu/commission_2010-2014/malmstrom/archive/directive_com2010_517.pdf, and see footnote 27.
[13] Since the main responsibility on (cyber)security issues lies within member states, the EU may intervene only in a subsidiary way, coordinating and harmonising national initiative.
[14] See the Action Plan of the European Commission, Communication on Critical Information Infrastructure Protection "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*," COM(2009)149 and the 2010 EC Communication on the ISS.
[15] Similar and other recommendations are included among the key actions of the "Trust and Security" pillar of the Digital Agenda for Europe, launched by the EU Commission in May 2010. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF, pp. 17-20.
[16] In 2008, 54,640 total cyber attacks against the U.S. DoD were registered, with a 60 percent increase in 2009. See http://www.scmagazineus.com/report-cyberattacks-against-the-us-rising-sharply/article/158236/.
[17] White House, *National Security Strategy*, May 2010, p. 27.
[18] White House, The National Strategy to Secure Cyberspace, February 2003.
[19] For Fiscal Year 2011, the Obama Administration requested about $3.6 billion for the CNCI.
[20] An essential reference document in the CIIP field is the Critical Infrastructure Information Act of 2002, http://www.dhs.gov/xlibrary/assets/CII_Act.pdf .
[21] For further details see http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.
[22] One of the most debated aspects of the first version concerned the President indefinite emergency authority to shut down private sector or government networks in the event of a cyber attack capable of causing massive damage or loss of life. This section was then amended requiring the president to get Congressional approval. See S. Fisher, *Cyber security Act of 2010 Passes Senate Committee,* June 2010, http://www.daniweb.com/news/story292578.html.
[23] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal L 077, 13/03/2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML. It is worth reminding that in 2008 ENISA's mandate was extended à l'identique until 2012.
[24] Namely, the Directorates-General Information Society and Home Affairs.

[25] The so-called operational activities include Computer Incident and Response handling, awareness raising, relations with EU member states and private bodies and various group activities. For details see the ENISA's 2010 Work Programme and Budget (Title 3), http://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-2010-budget.

[26] The new directive on ENISA proposed by the EU Commission would make it able, inter alia, to act as interface between all actors involved in cyber security; meet urgent requests within a rapid timeframe; assist member states and EU in developing an alert system to monitor the cyber security level in Europe; give EU technical advice to set a European CERT. Furthermore, ENISA would engage EU member states and private sector stakeholders in joint activities across Europe, such as cyber security exercises, public private partnerships for network resilience, economic analyses and risk assessment and awareness campaigns. See EU Commission *Proposal for a regulation of the European Parliament and of the Council concerning the ENISA* COM(2010) 521 final.

[27] "A more recent term is Computer Security and Incident Response Team (CSIRT). Besides . . . incident response, they usually provide security services for their customers, like alerts and warnings, advisories and security training." See http://www.enisa.europa.eu/act/cert/background/cert-factsheet.

[28] See http://www.first.org/about.

[29] For further details, see http://www.itpro.co.uk/626884/enisa-calls-for-an-eu-security-response-team. According to the EC 2010 Communication on the ISS, a EU CERT should be established by 2012.

[30] For further details on Cyber Europe 2010, see ENISA, *Q&As on the first pan-European Cyber Security Exercise*, at http://www.enisa.europa.eu/media/news-items/faqs-cyber-europe-2010-final.

[31] For further details see ENISA, *Interim findings of Cyber Europe 2010*, at http://www.enisa.europa.eu/media/press-releases/cyber-europe-2010-a-successful-2019cyber-stress-test2019-for-europe.

[32] See A. Moscaritolo, White House office grants DHS cyber security oversight, July 2010, available at http://www.scmagazineus.com/white-house-office-grants-dhs-cybersecurity-oversight/article/174442/.

[33] See http://www.us-cert.gov/aboutus.html.

[34] See http://www.dhs.gov/files/training/gc_1204738275985.shtm.

[35] For further details, *Cyber security Progress after President Obama's address*, July 2010, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010.

[36] Howard Schmidt, an Air Force and FBI veteran and a former Bush administration adviser and Microsoft executive.

[37] Group of Personalities, *Research for a Secure Europe*, Report of the GoP in the field of Security research, 2004.

[38] ESRAB, *Meeting the Security Challenge: the European Security Research Agenda*, 2006.

[39] ESRIF, Final report, December 2009, at http://www.esrif.eu/documents/esrif_final_report.pdf.

[40] *Area: 10.2.5 Cyber crime*. Topic SEC-2011.2.5-1 Cyber attacks against critical infrastructures. See ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k-wp-201101_en.pdf. Furthermore, see the EC DG Justice, Freedom and Security's Call for proposals, CIPS Action Grants 2010 within the Prevention, Preparedness and Consequence Management of terrorism and other security-related risks Programme.

[41] See http://www.whitehouse.gov/the-press-office/us-eu-joint-declaration-and-annexes.

[42] See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597.

[43] For further details on the U.S.-EU Energy Council and on its functioning, see http://www.whitehouse.gov/the-press-office/us-eu-joint-declaration-and-annexes, Annex 2. Members of the Cyber security Council could be on the U.S. side the Cybersecurity Coordinator, the Secretaries of State, of Homeland Security and of Defence; on the EU side, the High Representative for Foreign Affairs and Security Policy, the President of the European Council, the Commissioners for Home Affairs and for Digital Agenda.

[44] The 2010 NATO Strategic Concept includes cyber attacks among the threats to the international security environment. The Alliance therefore commits itself to develop further its ability to prevent, detect, defend against and recover from them (see http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf). Experts claim for a stronger cooperation between the EU and NATO. See Security & Defence Agenda, *Cyber Security: A Transatlantic Perspective*, Brussels, 22 March 2010 and House of Lords, European Union Committee, *Protecting Europe against large-scale cyber-attacks*, Report with evidence, London, March 2010.
[45] Please see footnote 14.
[46] See former Commissioner Reding's proposal
http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/199.
[47] Here, transatlantic cooperation could be undermined by issues on information exchange and transfer of sensitive technology and know-how especially in the defence field.
[48] EU-U.S. expert meeting on CIP in March 2010 (the next one is expected in early 2011)
http://useu.usmission.gov/useu_expertmeeting_030410.html or past EU-U.S. Summits on Cyber Trust,
ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/dublin-workshop-conclusions_en.pdf and
ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/20070426-27-joint-eu-us-cyber-summit-illinois_en.pdf.
[49] According to Europol, the U.S. sources preponderance is influencing the EU perspectives. See
http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf.
[50] On the U.S. side, the strategic and policy documents such as simple acts contain more precise definitions and there is a clearer division of competences between DoD and DHS in the management of cyber-related issues despite the possible overlaps and conflicts across the Agencies.
[51] For the Parties to the Convention, see http://www.coe.int/t/dc/files/themes/cybercrime/
WorldMapCybercrime_E.pdf.
[52] It includes the Internet Crime Reporting Online System (ICROS), the Analysis Work File Cyborg, that is actively working to fight criminal groups operating on the internet, and the Internet & Forensic Expert Forum (IFOREX) providing technical data and training for cyber crime law enforcement. See 2899th JUSTICE and HOME AFFAIRS Council meeting Luxembourg, 24 October 2008.
[53] See 2010 EC Communication on ISS, footnote 4.
[54] This is a typical question regarding asymmetric threats. See Security and Defence Agenda, *Cyber security: a transatlantic perspective*, 22 March 2010.
[55] The OECD writings are also considered as a reference on this topic. The glossary of terms provided by the dedicated website about biosecurity gives the following definitions: Biosafety: the safe handling practices, procedures and proper use of containment facilities to prevent accidental harm caused by living organisms either directly or indirectly to individuals within laboratories or to the environment. Biosecurity: measures to protect against the malicious use of pathogens, parts of them, or their toxins in direct or indirect acts against humans, livestock or *crops*.
[56] It is important to remind that there are various official languages in the European Union, which may sometimes add to the confusion. For example, "biosecurity" is translated "biosûreté" into French, and "biosafety" means "biosécurité."
[57] European Committee for Standardization.
[58] BMBL, 5th Edition, revised December 2009.
[59] Code of Federal Regulations. Title 42.
[60] While these documents are important in the global framework since biosecurity is not directly or indirectly mentioned or is not central, they will not be studied.
[61] See http://www.phe.gov/Preparedness/legal/boards/biosecurity/Documents/biosecreportfinal102309.pdf.
[62] See http://www.whitehouse.gov/administration/eop/ostp/nstc/biosecurity.
[63] See http://www.cdc.gov/biosafety/biosecurity_training/index.html.

[64] I. Bénoliel, "European Commission's Green Paper on Bio-Preparedness," in *Crop Biosecurity,* NATO Science for Peace and Security Study, ed. M. Gullino et al. (Dordrecht: Springer, 2008), p 136.
[65] The so-called Solidarity Clause of the Lisbon Treaty states that the European Union and its member states "*shall act jointly in a spirit of solidarity if a member state is the target of a terrorist attack or the victim of a natural or manmade disaster.*"
[66] For example, SYNBIOSAFE (FP6-NEST), CORPS (FP6-POLICIES), VALUE ISOBARS and SYNTH-ETHICS (FP7-SIS).
[67] Joint Action 2008/307/CFSP.
[68] T. Kimman et al.Ev-based biosafety: a review of the principles and effectiveness of microbiological containment measures," *Clinical Microbiology Reviews* 21(3) (2009): 403–25.
[69] D. Butler, "European biosafety labs set to grow," *Nature* 462 (2009:146–7.
There are currently 6 BSL-4 labs in the European Union, and at least 8 more are under construction or under discussion. The number of BSL-4 labs in the United States should reach 13 (from 7 today).
[70] GAO, *High-Containment Laboratories: National Strategy for Oversight Is Needed* (September 2009).
[71] Definition proposed by the Royal Society of London: "Synthetic biology is an emerging area of research that can broadly be described as the design and construction of novel artificial biological pathways, organisms or devices, or the redesign of existing natural biological systems."
[72] H. Bügl et al., "DNA synthesis and biological security," Nat Biotechnol. 25(6)(2007): 627–9, International Consortium for Polynucleotide Synthesis.
[73] Term derived from "biology" and "hacker" to describe someone who experiments on his own with DNA and other aspects related to genetics, usually not in a laboratory.
[74] DIYbio is an organisation that aims to help make biology a worthwhile pursuit for citizen scientists, amateur biologists, and DIY biological engineers who value openness and safety. They will require mechanisms for amateurs to increase their knowledge and skills, access to a community of experts, the development of a code of ethics, responsible oversight, and leadership on issues that are unique to doing biology outside of traditional professional settings." See http://diybio.org.
[75] Examples of relevant groups or activities include Biosecurity Working Group of InterAcademy Panel on International Issues (IAP), which is a global network of over 100 science academies worldwide; the International Federation of Biosafety Associations (IFBA), which supports and promotes biosafety on a national and international level, through collaboration among national and regional biosafety organisations worldwide, including the EBSA and ABSA; the International Society for Biosafety Research; the *International Consortium for Polynucleotide Synthesis* (ICPS) and the *Industry Association of Synthetic Biology* (IASB), consortia gathering biotechnology industrial companies which have been created in order to contribute to the improvement of biosecurity and biosafety. One aspect of the debate is about regulation versus auto-governance.
[76] The reference to "catastrophic challenge" is taken from the 2006 U.S. National Security Strategy, p. 43. The 2010 U.S. National Security Strategy argues that containing an epidemic "has never been so important" (p. 48). The subsequent reference is taken from the Implementation Plan for the National Strategy for Pandemic Influenza (Washington, D.C.: Homeland Security Council, 2006), p. 18.
[77] Available at http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.
[78] Available at http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf.
[79] Press Release, Council of Ministers, Brussels, 20-21 October 2005, available at http://www.eu2005.gov.uk/servlet/Front/.
[80] A. McLauchlin (2005), "EU Braced for Crisis as Flu Pandemic Threatens," *European Voice* (Brussels, 28 July 2005).
[81] Press Release "Commission adopts EU strategy on Pandemic (H1N1) 2009."

[82] "Council Conclusions on Pandemic (H1N1) 2009—a strategic approach," available online at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/lsa/110500.pdf.
[83] "Commission Working Document on Community Influenza Pandemic Preparedness and Response Planning," COM(2004)201 final, 26 March 2004.
[84] R. Martin (2009), "The role of law in pandemic influenza preparedness in Europe," *Public Health*123: 247–254.
[85] Parliament and Council (2004). European Parliament and Council Regulation establishing a European centre for disease prevention and control. No 851/2004 (Brussels, 21 April 2004).
[86] EU Commission–Public Health/Pandemic Influenza (H1N1) website: http://ec.europa.eu/health/communicable_diseases/diseases/influenza/h1n1/index_en.htm#fragment4.
[87] Zandén Kjellén, "Rapid Alerts for Crisis at the EU Level" in Stefan Olsson, *Crisis management in the European Union: Cooperation in the Face of Emergencies* (Swedish Defence Research Agency, 2009), pp. 68–69.
[88] Council memo (MEMO/09/363) Background on the Health Security Committee and the Early Warning and Response System authorities, available online at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/363&format=HTML&aged=0&language=EN.
[89] Commission, Brussels, 15.9.2009, "COM(2009) 481 final."
[90] "Commission Staff Working Documents: Health Security in the European Union and Internationally" SEC(2009) 1622 final, 23 November 2009.
[91] European Centre for Disease Prevention and Control (2007), *Technical Report: Pandemic Influenza Preparedness in the EU, Status Report as of Autumn 2006* (Stockholm, Sweden, European Centre for Disease Prevention and Control), 36.
[92] Department of Homeland Security, "Quadrennial Homeland Security Review," 2010, p. 7.
[93] GAO Report, Committee on Homeland Security, House of Representatives, Influenza Pandemic, November 2009, p. 1.
[94] Sarah A. Lister and C. Stephen Redhead, *The 2009 Influenza pandemic: An Overview* (Washington, D.C.: Congressional Research Service, 16 November 2009), p. 12.
[95] National Strategy for Pandemic Influenza Implementation Plan One Year Summary.
[96] GAO Report: Influenza Pandemic: Gaps in Pandemic Planning and Preparedness Need to Be Addressed, July 2009. Available online at http://www.gao.gov/new.items/d09909t.pdf.
[97] See http://www.flu.gov/professional/states/state_assessment.pdf.
[98] Lister and Redhead, *The 2009 Influenza Pandemic*.
[99] CNN, "CDC: Production of H1N1 flu vaccine lagging," 17 October 2009, available online at http://edition.cnn.com/2009/HEALTH/10/16/h1n1.vaccine.delay/index.html.
[100] Center for Biosecurity at UPMC, "Pandemic Flu Preparedness: Lessons from the Frontlines" (2009), available online at http://healthyamericans.org/report/64/pandemic-flu-frontlines.
[101] Comments from the Center for Biosecurity of UMPC on the National Strategy for Pandemic Influenza: Implementation Plan (2006), *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 4: 3.
[102] GAO Testimony Before the Committee on Homeland Security, House of Representatives, July 29, 2009.
[103] GAO Report, Committee on Homeland Security, House of Representatives, *Influenza Pandemic,* November 2009, p. 2.
[104] Bengt Sundelius, in Daniel S. Hamilton, "Shoulder to Shoulder: Forging a Strategic U.S.-EU Partnership (Washington D.C.: Center for Transatlantic Relations, Johns Hopkins University, 2010), p. 146.
[105] It should be noted that some EU leaders have expressed concern about WHO's influenza planning and that the EU is not a full member of WHO.
[106] These members provided insight on key issues that the transatlantic community would face in the event of a bioterrorist attack, and they were consulted in the development of the Atlantic Storm exercise.

[107] IPCC, "2007: Summary for Policymakers," p. 17, in *Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change,* ed. M.L. Parry et al. (Cambridge, UK: Cambridge University Press, 2007), 7–22.
[108] "A Secure Europe in a Better World: The European Security Strategy," Brussels, December 12, 2003, p. 3, http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.
[109] "Fight against the proliferation of weapons of mass destruction–EU strategy against proliferation of weapons of mass destruction," Brussels, December 10, 2003, http://www.consilium.europa.eu/uedocs/cmsUpload/st15708.en03.pdf.
[110] "The European Union Counter-Terrorism Strategy," Brussels, November 30, 2005, http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf.
[111] "The Community mechanism for civil protection," European Civil Protection, European Commission, http://ec.europa.eu/echo/civil_protection/civil/prote/mechanism.htm.
[112] "Article 222," The Lisbon Treaty, http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-5-external-action-by-the-union/title-7-solidarity-clause/510-article-222.html.
[113] "Annex: Forest Fires," in Communication from the Commission to the European Parliament and Council on Reinforcing the Union's Disaster Response Capacity, European Commission, Brussels, March 5, 2008, p. 12, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0130:FIN:EN:PDF.
[114] National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, p. vii, http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf.
[115] Ibid, p. 42.
[116] The White House, "Homeland Security Presidential Directive/HSPD-5," Washington, D.C., February 23, 2003, p. 3, http://training.fema.gov/EMIWeb/IS/ICSResource/assets/HSPD-5.pdf.
[117] Ibid.
[118] The White House, Homeland Security Council, "The Federal Response to Hurricane Katrina: Lessons Learned," Washington, D.C., February 2006, p. 52, http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf.
[119] Keith Bea et al., "Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions," CRS Report for Congress, December 15, 2006, p. 6, http://www.fas.org/sgp/crs/homesec/RL33729.pdf.
[120] Ibid, pp. 7, 10, 12.
[121] U.S. Department of Homeland Security, "FEMA Strategic Plan: Fiscal Years 2008-2013," Washington, D.C., January 2008, p. 13, http://www.fema.gov/pdf/about/fy08_fema_sp_bookmarked.pdf.
[122] The White House, Homeland Security Council, "National Strategy for Homeland Security," October 5, 2007, p. 1, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.
[123] Ibid., p. 31.
[124] U.S. Department of Homeland Security, "National Response Framework," Washington, D.C., January 2008, p. 2, http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.
[125] CRS Report for Congress, "The National Response Framework: Overview and Possible Issues for Congress," November 20, 2008, p. 8, http://www.fas.org/sgp/crs/homesec/RL34758.pdf.
[126] Ibid. Lindsay writes: "State officials in Texas said it was the local government's responsibility to set up distribution points for supplies. However, the local government claimed it was unaware of this responsibility."
[127] U.S. Department of Homeland Security, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," Washington, D.C., February 2010, p. iii, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.
[128] U.S. Department of Homeland Security, "Bottom-Up Review Report," Washington, D.C., July 2010, http://www.dhs.gov/xlibrary/assets/bur_bottom_up_review.pdf.

[129] United Nations Office for the Coordination of Humanitarian Affairs, "About Us," http://ochaonline.un.org/tabid/5838/language/en-U.S./Default.aspx.
[130] European Union, Delegation of the European Commission to the USA, "Joint EU/U.S. Action Plan," http://www.eurunion.org/partner/actplan.htm.
[131] Euro-Atlantic Disaster Response Coordination Centre, "Enhanced Practical Cooperation in the Field of International Disaster Relief," Fact Sheet, http://www.nato.int/eadrcc/fact.htm.
[132] The White House, "The National Security Strategy of the United States of America," Washington, D.C., September 2002, p. 25, http://www.globalsecurity.org/military/library/policy/national/nss-020920.pdf.
[133] 2003 European Security Strategy, p. 13, http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.
[134] "Tsunami aid: Who's giving what," BBC News, January 27, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4145259.stm.
[135] "The EU's contribution to the international response to the 2004 Asian Tsunami: Achievements, next steps and lessons learned," Discussion Paper, High-Level Meeting, Brussels, December 20, 2005, p. 3, http://ec.europa.eu/world/tsunami/docs/051215_paper_final11.pdf.
[136] *U.S. Agency for International Development, "Tsunami Reconstruction, Three Years Later," Fact Sheet, December 22, 2007*, http://www.usaid.gov/locations/asia/documents/tsunami/Final_Tsunami_3rd_Anniversary_Fact_Sheet.pdf.
[137] Jon Bennett et al., "Coordination of international humanitarian assistance in tsunami-affected countries," Tsunami Evaluation Coalition (TEC), Evaluation and Studies Unit, United Nations Office for the Coordination of Humanitarian Affairs, New York, July 2006, p. 156, http://www.alnap.org/pool/files/synthrep%281%29.pdf.

[138] World Conference on Disaster Reduction, "Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters," Kobe, Hyogo, Japan, January 18-22, 2005, http://www.unisdr.org/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf.
[139] "Statement on Behalf of the European Community," World Conference on Disaster Reduction, Special Session on the Indian Ocean Disaster, Kobe, January 20, 2005, http://www.unisdr.org/wcdr/intergover/indian-ocean/european-community.pdf.
[140] "Kobe Plenary Statement," U.S. Embassy Tokyo, http://www.unisdr.org/wcdr/intergover/member-states/usa.pdf.
[141] "Support to the U.S. in response to hurricane Katrina," EADRCC – Operations, Euro-Atlantic Disaster Response Coordination Centre, http://www.nato.int/eadrcc/2005/katrina/index.htm.
[142] "The Federal Response to Hurricane Katrina," p. 62, http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf.
[143] "EU earmarks over €429 million for Haiti," *Business Day*, January 18, 2010, http://www.businessday.co.za/articles/Content.aspx?id=91461.
[144] USAID, Bureau for Democracy, Conflict, and Humanitarian Assistance, "Haiti–Earthquake," Fact Sheet, July 16, 2010, http://www.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/countries/haiti/template/fs_sr/fy2010/haiti_eq_fs63_07-16-2010.pdf.
[145] "Response to the Humanitarian Crisis in Haiti," IASC, July 16, 2010, http://www.interaction.org/sites/default/files/Additional%20Resources-%20IASC-%20Response%20to%20the%20Humanitarian%20Crisis%20in%20Haiti%5B1%5D.pdf.

ISSUE 3

INDUSTRY TOWARD SECURITY

INTRODUCTION

Nicolò Sartori, *Junior Researcher, IAI*

Since the end of the Cold War, the collapse of the Soviet Union and the advent of structural modifications within the international system, the security perceptions and strategies across the Western world have witnessed radical change and development. Nowhere else is this more evidenced than by defense spending trends over the last half century.

As concerns for large-scale conventional warfare, nuclear attack and the spread of communism fell by the wayside, so too did the age of bi-polarity. With the rise of U.S. leadership, the international community also bore witness to the enhancement of the European Union and other international organizations. Reflective of this downturn in global military conflict, the 1990s defense budgets in both the United States and in the EU countries, experienced sharp reductions and cuts, while national defense industrial bases underwent extreme reorganization and consolidation.

Today, the economic, political and technological landscape of the 21st century has ushered in new security concerns and progressively influenced the politics of modern-day warfare. The terrorist attacks of September 11, 2001, on the World Trade Center illustrates the level of danger new-age technologies and warfare techniques pose to both civilian and military personnel. It also clearly depicts the central role national security has to play in ensuring the safety and well-being of citizens.

As a result of the 9/11 attack, defense budgets of the major transatlantic players once again began to experience growth, and for many, this budgetary increase continues to rise. . The funding for military efforts in Afghanistan and Iraq and crisis management operations by the United States, EU and/or NATO frameworks account for the majority of this expenditure.

Defined as multifaceted, interrelated and increasingly transnational, modern-day threats have shaped a new approach to national security policy and agenda setting. Risks associated with technological development, the rise and empowerment of non-state actors and the possibility of domestic attack must all be taken into account. As a result, activities such as counterterrorism and the fight against organized crime, border control, critical infrastructure protection and preparedness and recovery in times of crisis, now represent fundamental aspects of national security policy.

The emphasis placed on these new challenges has established security as a viable and pertinent market and represents an expansion of a traditionally defense-oriented industry. Although defense-related issues continue to constitute significant portions of governments' budgets, the United States and the EU are actively seeking to build a comprehensive approach to the security

sector by way of legislation and regulations, collaboration with the commercial sector to build industrial and commercial strategies as well as by expansion of the public-private dialogue and partnership programs.

This paper seeks to provide not only a clearer definition of the security market, but will describe the strategies, policies and procedures adopted by both the EU and the United States in efforts to establish an efficient security market and a thriving security industrial base. Additionally, the political, economic and technological drivers and constraints with the potential to influence the development of a competitive transatlantic security industrial sector will be discussed and possible policy recommendations for EU and the United States will be proposed.

The first section, by Hélène Masson and Lucia Marta of the Fondation pour la Recherche Stratégique (FRS), provides a complete picture of the current security market from both the demand and supply sides. The analysis focuses on the main industrial actors and procurement agencies operating in the security sector and pays particular attention to the transatlantic dimension of the market. A high level of fragmentation, both in terms of customer base and industry, has been established as the characterizing feature of the security markets in the EU and the United States.

In the second part of the paper Jan Joel Andersson and Erik Brattberg of the Swedish Institute of International Affairs (UI) focus on the rise of the public-private dialogue. Specifically, this section seeks to determine whether the partnerships between governmental agencies and the private sector reflect an adequate level of collaboration capable of fostering a fruitful exchange of ideas between stakeholders. As UI illustrates, the diversity of buyers' profiles and the unstable/volatile nature of demand within the security market continues to pose significant challenges for the industry.

The third section by David Berteau, Guy Ben-Ari and Priscilla Hermann of the Center for International and Strategic Studies (CSIS), and Sandra Mezzadri of the Istituto Affari Internazionali (IAI), analyses the regulatory environments for security in the United States and the EU. Their investigation identifies different kinds of regulatory shortcomings in both the United States and the EU and highlights a series of common regulatory weaknesses, such as the unclear distinction between the security vs. defense industries, barriers to the security market and insufficient public-private dialogue, all of which areas that can benefit from common transatlantic development.

The final section of the paper written by Valerio Briani and Nicolò Sartori of the Istituto Affari Internazionali (IAI), analyses the different economics characteristics of the defense and the security industrial sectors and their effect on transatlantic cooperation. In addition, IAI discusses the two very different approaches adopted by the United States and the EU in terms of industrial security policy. With the help of collaborating international partners, this section also highlights the differences between the EU's European-centric or multinational-focused industrial policy and the institutionally centered U.S. approach.

This paper concludes with a set of policy recommendations, applicable both to the EU and the United States, aimed at improving the industry's engagement in the governance of the security sector, the enhancement of the regulatory environment and the avoidance of protectionist practices.

THE SECURITY MARKET IN THE EU AND THE UNITED STATES: FEATURES AND TRENDS

Hélène Masson, *Senior Research Fellow, FRS,* and
Lucia Marta, *Researcher, FRS*

Introduction

This section aims to provide a general overview of the structure and dynamics of the security market in Europe and in the United States as well as assesses the opportunities for cooperation at the transatlantic level. Taking a look at the demand-side of the market, this paper will discuss the main actors and security functions identified at the institutional level as well as provide estimations of governmental funding for R&D and the procurement of security solutions and systems. On the supply-side, this paper describes the competitive structure of the security market and its dominant characteristics as well as market segmentation and the strategic orientations of the most prominent competitors.

Security Market: Demand Side

In Europe

Fragmentation in the European security procurement environment

While the defense market is mature and well-structured at the national level, the security market is relatively new and undeveloped. The juxtaposition of these two sectors reveals two fundamental differences with regard to the procurement of security solutions.

First, in the security sector more than one customer can procure security systems. Customers at the national level can be public (several ministries, agencies and institutions) or private (banks, but also owners or managers of critical infrastructures). Moreover, public customers can be found at the central, regional or local level.

Consequences of such fragmentation include the following:

- The security demand is varied and, therefore, many relatively small/medium contracts are issued (when compared to the defense sector) ;
- Security requirements are not harmonized, except for those solutions for which public regulation (in terms of requirements, standards, etc.) exists;

- The size of the security market is hard to ascertain, unlike the defense market

Second, unlike the United States, the demand-side has not established a "European Homeland Security Agency." As a result, procurement of security equipment does not occur at the EU level, yet at the national level.[1]

Besides the fragmentation of European security procurement across all 27 member states, demand for security is also highly split across national lines. With security-related activities occurring primarily at the national and subsequent regional and local levels, the EU requires a high degree of coordination, which currently is insufficient. For example, in France the budget allocated by the Ministry of Interior for the national police and gendarmerie in 2010 concerning investments in new technologies was around 192.6M€, but it does not include the procurement of security solutions related to border control (included in the Coast Guard budget) or airports and ports security solutions, which are under the responsibility of private companies. Official statistics, in this respect, do not exist. Therefore, a complete overview of the budgets allocated for investments in technological solutions is very hard to assess, even at the national level.

We can identify a few examples of countries trying to reduce fragmentation and centralize procurement activities, at least in the communications and biometrics industries. Notably, the acquisition of a single radio system for Federal and Lander first responders in Germany and the National Resilience Extranet System providing national responders with access to the same web-based information system in the UK.

When looking at some security contracts awarded by the main European countries, we can observe the following features:

- They are quite small compared to the defense sector, in terms of costs;
- They have been completed in the past few years, and apparently no new expensive contracts have been recently issued in all the security segments, although some of them, communications and biometrics in particular, are the center of public attention;
- They are often linked to specific events for example, in the UK, the Home Office manages the project "Olympic Safe and Security," which costs around 600M£. Similarly, if a natural disaster or a terroristic attack occurs in Europe, the security market is able to quickly react.

To conclude, European procurement remains in the hands of single member states, the market is fragmented among different players (public and private, national and local) and demand appears to be experiencing a slowdown across the market, except for in a few key sectors and following specific events.

The European Union: a crucial player in the field of security R&D

While the EU cannot be considered a security procurer, it, nevertheless, plays a very important role in coordinating the security research agenda across 27 EU member states and Associated countries.

The ESRAB report,[2] in particular, is the first and only comprehensive European effort to highlight security needs in terms of capabilities and technologies for European security and indicates the necessary R&D track. The ESRAB report adopted a capability-related approach, moving in a linear fashion from threats to missions, to functions, to capabilities and lastly to technologies. Identified technologies are meant to address the needs of the following four security

missions: border security; protection against terrorism and organized crime; critical infrastructure protection; and recovery following times of crisis.

Following the efforts put in place by the Commission (GoP, PASR, ESRAB), the Seventh Framework Program on research includes, for the first time, a budget line dedicated to security, which is inserted in the Cooperation Program. It covers the period 2007–2013 and allocates 1,4B€ for the Security theme (around 4 percent of the FP's cooperation program), which accounts for an approximate 200M€ per year. This figure is somehow misleading however, as there are security-related projects within other themes, like Information and Communication Technologies, Transports and Space. Although, the overall European funding for security research is hard to calculate, the specifically allocated 1.4B€ is an important figure contributing to the development and expansion of the security market.[3]

Beyond the 7FP, other agencies at European level are developing security programs with the potential for future procurement. European agencies like EUROPOL, EUROJUST, FRONTEX, EDA are catalysts for demand harmonization in R&D sector and the future procurement of security systems. Equally, they are often involved in missions requiring collaboration with the United States and thus have led to the establishment of operational and technical transatlantic capabilities.[4]

At the national level, security R&D appears weak compared to those made by the EU. In Germany, the Federal Ministry of Education and Research allocated around 123M€ for the period 2007–2011 for civil security research. In France, the Délégation Générale pour l'Armement (within the MoD), alongside the Agence National pour la Recherche conducts a "concepts, systems and tools for global security" program with12.7M€ in funding for 2009. In the UK, the Home Office Scientific Development Branch supports the Home Office's mission, which is an investment of approximately 65M€ per year.

The significant level of R&D funding for security at the EU level, rather than at the national level, is creating the good basis for future common procurement. Whether resources for procurement will be available, however, remains unknown. Many experts question the growth of the security market in Europe and the capacity of national institutions to benefit from the established R&D programs.

Estimation of the European security market size and trends

Some estimations of the size of the European security market are made available by research centers and consultancies.

The European Commission[5] and ECORYS[6] have stated that the EU security industry had an estimated value ranging from 26 to 36B€ in 2008. This figure represents a large range, confirming the difficulty in acquiring a precise idea of the market size. Moreover, it includes "low level" security systems, like video surveillance and fire detection systems.

According to ECORYS, the following sectors account for the major market share:

- Physical security protections, from 10 to 15B€;
- Border security as well as counterterrorism intelligence, 4.5B€ at least; critical infrastructure protection from 2.5 to 3.5B€;
- Aviation and maritime security sectors from 1.5 to 2.5B€.

Moreover, according to ECORYS, the public sector is the main purchaser of security equipment and services accounting for approximately 80 percent of the market, which places global public spending between 13 and 17B€.

Demand at the European and the national level exist as security concerns are, and will continue to be, high on the political agenda. The public sector will continue to stimulate demand from the private sector through the establishment of security procedures, particularly with regard to aviation security and critical infrastructures protection. Moreover, European agencies are working on the definition of new common and interoperable solutions. Nevertheless, the current economic slowdown and public budget cuts, besides the growing costs of technological solutions which require long term investments, do not guarantee adequate investments for the procurement of security solutions. It is very hard to assess how fast and for how long the security market will grow. At the moment, the level of growth is not being sustained or increasing as quickly as expected in the past years.

In the United States

The Department of Homeland Security and other actors in the security procurement

In the United States, demand in the security market is mainly led by the government (federal, state and local level). Also private companies play a role, but this is limited when compared to the public spending.

The Department of Homeland Security (DHS) brings together, under one agency, activities that were previously spread across the federal government, centralizing the competences in the security domain and improving coordination and effectiveness. Agencies that are now part of DHS include the Coast Guard, the Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA) and activities previously performed by the Immigration and Naturalization Service (INS) and Customs and Border Protection (CBP).

It is worth noting that most of the DHS acquisition budget is spent on services rather than on products (for a more detailed view on DHS procurement see section 3 in this paper). Moreover, not all the resources allocated to DHS are spent on core homeland security activities: part of it (the CBO estimates about 35 percent of the total budget in 2004)[7] financed non-homeland security functions that were performed by their original agencies (for example, Coast Guards task in marine safety and navigation support).

At the same time, other federal agencies perform tasks related to homeland security although their budget is not part of DHS, the CBO estimates that in 2004 about 17M$ were allocated for non-DHS homeland security activities. For example, DoD spending for systems and operations was approximately 10B$ for FY 2006. Additionally, more than 2B$ per year is spent on Improvised Explosive Devises (IED) along with substantial investments in counter Weapons of Mass Destruction (WMD) technologies.[8]

Also in the United States, demand appears fragmented as DHS and other federal agencies are involved in security R&D and procurement. Indeed, DHS has fewer large programs than DoD and pushes a significant share of the acquisition money to states and local authorities through a variety of relatively small grant programs.

As in Europe, developments and shifts in policy as well as the occurrence of either natural and or terrorist-related events can lead rapidly to new priorities and budget allocation. The security

market is therefore maturing comparing to 10 years ago, and is certainly more mature than the EU market, but still volatile and dynamic.

U.S. R&D in the security sector

The Quadrennial Homeland Security Review identifies the threats and hazards that challenge the U.S. interests from a homeland security perspective such as, the dangers of weapons of mass destruction; Al Qaeda and global violent extremism; risks posed by wide-scale cyber-attacks, intrusions, disruptions, and exploitations; pandemics, major accidents and natural hazards; illicit trafficking and related transnational crime; smaller-scale terrorism.

Those new threats, combined with traditional responsibilities in terms of security, represent the core homeland security missions, for which a set of objectives and capabilities are identified. As in the EU, DHS calls for compatible architecture and standards among the different end-users.

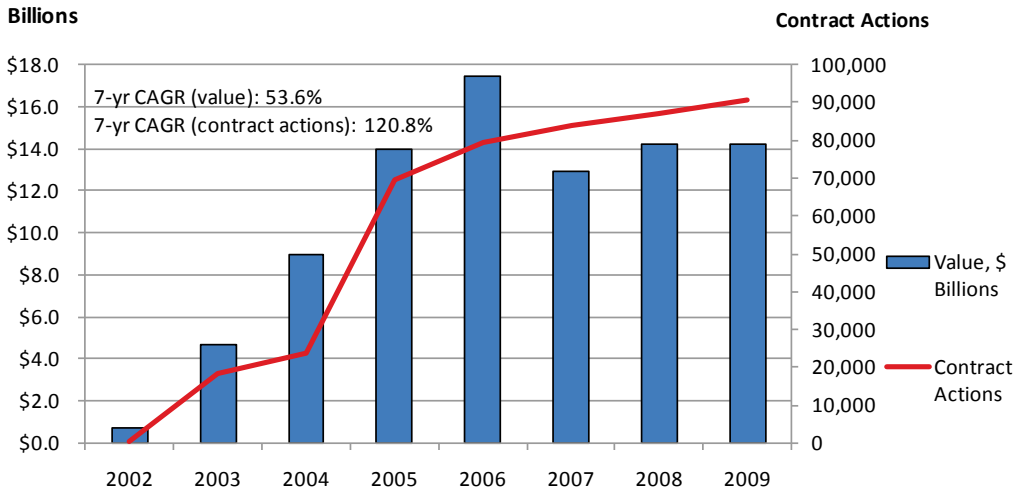
R&D in early stages is funded mainly through the Homeland Security Advanced Research Projects Agency (HSARPA), part of the Science and Technology (S&T) directorate of DHS, and the Defense Advanced Research Projects Agency (DARPA), which is dedicated to defense and has at its disposal a more significant budget (54B€ in defense R&D in 2008). HSARPA "*performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and* universities."[9]

The budget request for the Science & Technology directorate is about 1.02B$ for FY2011 (less than 2 percent of the total DHS budget, but certainly larger when compared to the EU plus national R&D resources). The R&D funding is allocated among the S&T directorate's divisions, 6 of them correspond to the 6 areas HSARPA primarily focuses its activities on border and maritime security with 44.2M$ in FY2010 funds; 206.8M$ for chemical and biological programs and 120.8M$ for research on explosives.[10]

Estimation of the U.S. security market size

From a historical perspective, federal funding for homeland security activities has constantly increased since 2002 with a light inflection in 2009. The total budget request for DHS in the FY 2011 budget is about 56.3B$,[11] confirming an increasing trend (+2 percent of discretionary funding compared to FY 2010 levels). DHS resources are distributed among its components and agencies, for example, 20 percent to the Customs and Border Protection; 18 percent to the Coast Guard; 14 percent to the Transportation Security Administration. Each of these bodies allocates part of the budget for procurement, although the FY2011 budget document does not specify the amount.

The following graphic illustrates DHS acquisitions by value and contract actions for the period 2002–2009. Despite the exclusion of the resources coming from other federal agencies, state and local authorities and the private sector, this graph shows the trend wherein more contracts are issued for less value. The large increase in 2006 reflects activity in the security market following Hurricane Katrina.



Source: Federal Procurement Data System, CSIS analysis.

CIVITAS Group, in 2006, published a study that estimates the total size of all federal government expenditure for homeland security (including expenses by other Departments and agencies) to more than 18.2B$ as of 2006.[12] Moreover, they estimate that the state and local government spending on homeland security, which is accessible to the private sector at approximately 3.5B$ for the same year, 2.7B$ of which comes from a variety of federal grant programs.

Additionally, CIVITAS Group found that the private sector and quasi-governmental authorities spent about 9.3B$ in 2006 on homeland security-related products and services.

Governmental reports and consultancies seem to agree that the increase in DHS spending, particularly the spending that will be captured by industrials and service providers, will only rise in the years to come. The Homeland Security Research Center report reveals that, over the next five years, the homeland security and homeland defense market, from the federal, local and nongovernmental levels, including the private sector, will grow at a CAGR of at least 5 percent from 69B$ in FY2010 to 85B$ in FY2014 with increased funding in some key market sectors such as cyber-security, bio-defense, information technology, C3I, perimeter and border security.[13]

Such analysis is, however, questioned by experts[14] who consider that the economic slowdown and the federal budget deficit will have a relevant impact on the budget for security procurement.

Finally, with regard to the distribution of the homeland security and homeland defense budgets among customers, the report highlights the leading role played by state and local security authorities, with a share of 23.7 percent. The Department of Defense (DoD) follows with 22.5 percent and DHS takes the third position with 18.3 percent. This trend seems to create a certain paradox, as the procurement of security solutions remains somewhat decentralized. Despite the creation of DHS, the trend of increased funding to state and local grant programs started in 2001, ranging from 0 to 3.4B$ in only 4 years.

Despite the existence of a more structured security market in the United States, the demand-side nevertheless, suffers from fragmentation, making the assessment of the overall security market's size difficult to ascertain. Resources allocated for R&D and procurement are more

relevant than in Europe, making the United States the dominant world market in the security field.

EU-U.S. Security Market: The Supply Side

First Picture

A wide range of submarkets

The security market is not easy to define because it is an aggregation of market niches. It encompasses a wide range of product and services, from "traditional" security products such as physical access controls, CCTV, anti-intrusion and anti-fire detection/alarm, electronic surveillance tools, physical security measures and security guarding, passenger-screening or cargo-screening systems, biometrics ID systems, video surveillance systems, RFID, cyber-security systems, CBRN detection equipment. On both sides of the Atlantic, the current security solutions address the following key submarkets: aviation security, mass transit security, maritime security, critical infrastructure protection, telecommunications, data management, cyber-security, border security, counter-terrorism intelligence, disaster response and recovery.[15]

Submarkets	*Leading Technologies*
Aviation security	Screening Systems (Millimetre Wave Systems, Terahertz Systems, Backscatter X-Ray Systems)
Mass transit (public transport) security	Biometrics ID Systems
Maritime security (Cargo and port security)	RFID-Based Systems
Critical infrastructure protection (Electricity, Oil, Gas, Water Infrastructures; CBRN Detection Systems)	Cybersecurity Systems
Telecommunications, data management and cybersecurity	Counter-Terrorism Intelligence (Video surveillance systems, Databases)
Border security	CBRN Detection Systems
Counter-terrorism intelligence	
Disaster response and recovery	

Source: Homeland Security Research Corporation, Jane's Information Group, and Security Industry Association; synthesized by authors Masson and Marta.

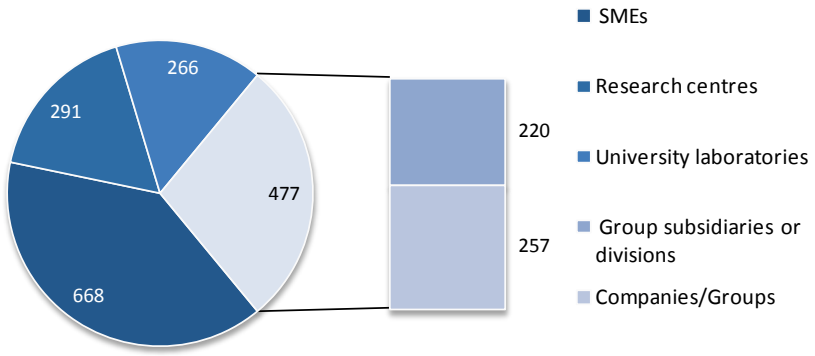
Competitor profiles

Regarding the suppliers profile, we can distinguish different types of competitors:

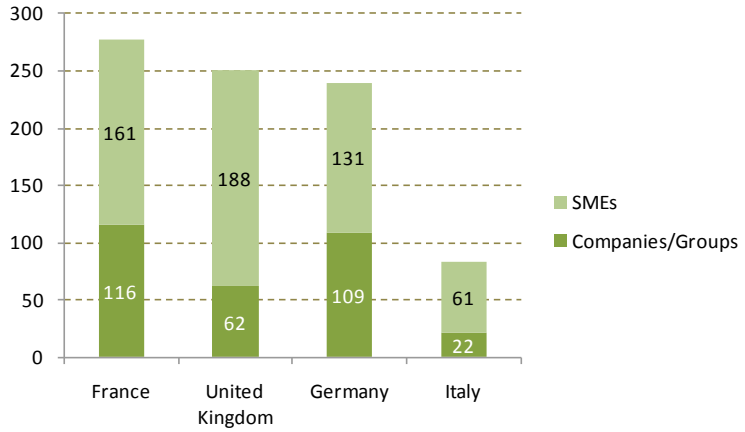
- **Suppliers of "traditional" security products.**[16] The traditional private security industry is represented by well-structured trade associations, such as the British Security Industry Association (BSIA), or the Security Industry Association (SIA) in the United States representing electronic and physical security product manufacturers, distributors, integrators, and service providers.
- **Defense industry.** A number of defense business segments can address the capability requirements within security markets. According to Gert Runde, ASD Director Security and Defense: "*Both future and current security solutions can derive important advantages from a spin-in of technologies that were developed by the European defense industry.*"[17] In this context, big defense companies realign their position for further growth in new and adjacent markets, drawing on their know-how and experience in the defense, electronics and aerospace markets.

- **ICT companies** (i.e. Sun Microsystems, Oracle, IBM, HP, Cisco, MacAfee). ICT companies that previously paid little attention to government contracts, look for business opportunities in the security market, seeking to respond to the growing needs within IT sector as expressed by the public administration, both in Europe and the United States.
- **Specialized Providers** (Mid-sized companies). As noted by Civitas Group "*the growing homeland security market has encouraged the creation of many companies focused solely on this sector,"* mainly in the United States.
- **A very large number of small innovative companies.** Start-up innovators,[18] developers and providers of new security technologies, are addressing the security market, on both sides of the Atlantic. The *European Security Directory 2009* underlines that European SMEs are very active in the security field. Trade and industry bodies with "security capabilities/technologies," definitions based on the ESRAB report, and excluding security guardian companies, represent around 668 SMEs. Also represented are 477 companies/groups (including 220 group subsidiaries or divisions with specific security technological or industrial capabilities and 257 Companies/Groups), and 557 research centers and university laboratories.[19]

European Security Industry

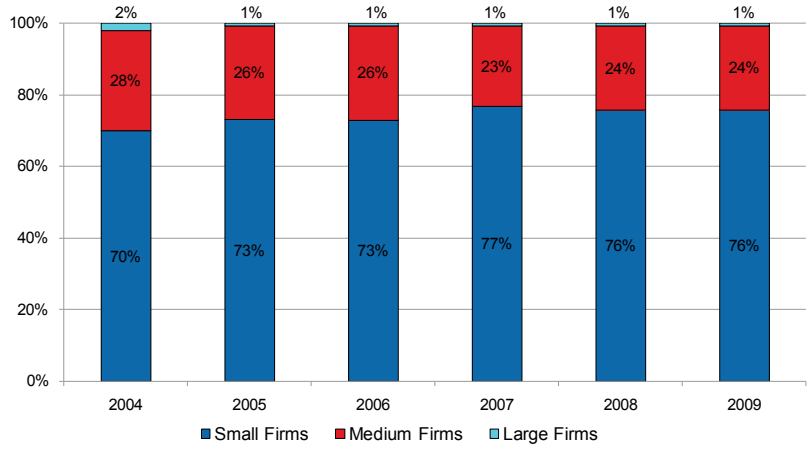


European Security Sector (companies, SMEs)



Source: ESD partner STI Database, 2009.

An in-depth analysis of the distribution, by number of contractors, of the DHS market to Small, Medium and Large firms for the period 2004–2009, made by the CSIS, stresses that more than 70 percent of DHS contractors are small firms.



Source: Federal Procurement Data System, CSIS analysis 2010.

Market Leaders

In the United States

All sources of information[20] converge on the fact that the big winners of the homeland security market, the top U.S. security companies, are mostly and generally all leading military contractors: Boeing, Lockheed Martin, General Dynamics, L-3 Com, Northrop Grumman, General Electric, Raytheon, Honeywell, Unisys, SAIC, to list the most prominent competitors.

DHS Top 20 firms, 2004–2009 (in constant 2009 dollars)

1	Integrated Coast Guard Systems	$3,979,163,159
2	IBM	$2,802,631,148
3	Unisys	$2,285,665,607
4	Fluor Enterprises	$2,019,273,571
5	Computer Sciences Corporation	$1,721,588,994
6	Boeing	$1,634,017,353
7	L3 Communications	$1,479,312,139
8	General Dynamics	$1,452,117,679
9	Accenture	$1,414,790,101
10	Lockheed Martin	$1,175,138,257
11	SAIC	$974,475,308
12	Circle B Enterprises	$974,220,637
13	Shaw Environmental	$864,384,513
14	Northrop Grumman	$784,353,608
15	Gulf Stream Coach	$572,313,392
16	Morpho Detection	$551,803,327
17	Cooperative Personnel Services	$517,828,533
18	Bechtel	$500,014,658
19	Nationwide Infrastructure Support Technical Assistance Consultants	$486,384,667
20	CH2M Hill	$465,347,424
	Total (2004-2009)	**$26,654,824,075**

Source: Federal Procurement Data System, CSIS, 2010.

The homeland security contractors list includes mid-sized companies, and above all, major system integrators, which act as managers of large-scale homeland security programs:

- SBInet program (Boeing)
- Bio Watch Gen-3 program (Northrop Grumman)
- U.S. Coast Guard Deepwater (Integrated Coast Guard Systems, a joint venture between Lockheed Martin and Northrop Grumman)
- FBI's Integrated Automated Fingerprint Identification System (Lockheed Martin)
- Integrated Wireless Network (IWN) program (General Dynamics)
- Transportation Security administration Advanced Screening Technology programs (Unisys)
- Customs and Border Protection Agency Land Ports of Entry program (IBM)
- U.S.-VISIT Border Management program (Accenture)
- EAGLE IT Program (among the leading contractors are CACI, Booz Allen Hamilton, Lockheed Martin, SAIC, Northrop Grumman, General Dynamics, and BAE Systems)

Indeed, in five years, the top U.S. defense contractors have moved to consolidate their portfolio of products and services, and strengthened their market position by implementing the following strategic orientations:

- creation of "homeland security" new branch/division and/or subsidiaries
- strengthening the homeland security business by applying technologies and systems integration expertise developed in the defense market.

- acquisition of SMEs (small niche providers) with valuable technology, intellectual property and/or target market channels focused on intelligence and homeland security.

Major system integrators all have very similar and large portfolios with activities ranging from defense, intelligence and homeland security. Generally, they have built up strong positions through a number of acquisitions of smaller competitors and investments in homeland security, expanding their capabilities in information systems security/cyber-security, intelligence, critical infrastructure protection, and in a number of different specialty areas (i.e. detection).

Companies	Date / Firms acquired	Domains
Boeing	2008 / Digital Receiver Technology (DRT)	digital signal processing products
	2008 / Ravenwing	Cybersecurity solutions
	2008 /Kestrel Enterprises	Data management, development and systems integration, program management, training
	2009 / eXMeritus	Hardware and security software
	2010 / Argon	C4ISR and combat systems
	2010 / Narus	Cybersecurity solutions
Raytheon	2009 / BBN Technologies	IT, sensor systems, and cybersecurity
Lockheed Martin	2006/ SAVI Technology	RFID Equipment and solutions
	2007 / Management Systems Designers	IT and scientific solutions
	2008 / Eagle Group International	Logistics, IT, training and healthcare services
	2009 / Gyrocam Systems	Gyrostabilized optical surveillance systems
	2009 / Universal Systems & Technology	Interactive training and simulation, technical solutions
SAIC	2010 / CloudShield Technologies	Cybersecurity and management solutions
	2009 / Spectrum San Diego	Ultra-low-dose X-ray scanning systems
General Dynamics	2009 / Axsys Technologies	High-performance electro-optical and infrared (EO/IR) sensors and systems and multi-axis stabilized cameras
L-3 Com	2002 / Perkin Elmer	X-ray screening business
	2006 / CyTerra Corporation	Advanced through-wall radar and explosive detection sensors for checkpoints
	2006 / SafeView	Non-invasive scanning systems
	2006 / TRL Electronics (UK)	Secure Radio and Satellite Communications for Defense and Homeland Security Applications (Electronic Counter Measures and cryptographic areas)
Northrop Grumman	2007 / Essex Corporation	Signal processing services and products, advanced optoelectronic imaging
	2007 / Xinetics	active optics such as deformable and hybrid mirrors, advanced wavefront control systems for real-time control of active optical systems
	2008 / 3001 International	Geospatial data production and analysis

Source: Authors.

European companies look overseas

The large European defense groups represent today's major competitors in the European security market. But, with a very fragmented and R&D-focused European market, these companies look, first and foremost, overseas for more profitable growth.

As shown by the UI's paper, *Challenges to Agenda-Setting Priorities: Toward Effective Public-Private Partnerships for Security in the EU and United States*, at EU level they have had an indubitable influence upon the shaping of the EU security-research agenda and various strategies and research projects. At the national level, the UK, French and German markets account for the largest share of public spending, but fragmentation exists with regard to the many smaller programs, focused more on R&D than on procurement. Unsure of the European market demand and requirements, the industrial players are *de facto* and very active in pursuing business opportunities in the U.S. market, Middle East, North Africa and Asia.

Like their U.S. counterparts, European firms have acquired small and mid-sized companies in order to expand their portfolio of technologies and innovative forward-looking security solutions, opening new lines of business and entering new overseas markets. U.S. acquisitions include both defense companies doing homeland security work and stand-alone homeland security companies.[21] In addition, European firms have developed a number of commercial and technology partnerships with U.S. providers.

Companies	Date / Firms acquired	Domains
EADS	2005 / Nokia's Professional Mobile Radio (PMR) activities	Secure telecommunication
	2006 / french company Sofrelog	Vessel Traffic Service (VTS) systems and Coastal Surveillance Systems (CSS)
	2008 / US PlantCML	Emergency response solutions and services
	2010 / EADS DS and Atlas Elektronik (AE) have decided to consolidate their position in the maritime safety and security market by merging their subsidiaries Sofrelog and Atlas Maritime Security, a spin-off of AE, to form "Sofrelog Atlas Maritime Security" (SA Maritime Security)	
Thales	2007 / rail signalling and security systems businesses acquired from Alcatel-Lucent	
	2008 / british company n-Cipher	Encryption firm (Internet and communications system security market)
Safran	2008 / Dutch company Sdu-Identification	Secure identification documents, including electronic and biometric passports, ID cards and driver licenses
	2009 / US Motorola's biometrics business	Printrak trademark. Automated fingerprint identification systems (AFIS)
	2009 / 81% of US GE Homeland Protection	Systems to detect dangerous or illicit materials (X-ray tomography detection systems). Much of the technology is designed for use in airport screening
Finmeccanica	2007 / british VEGA Consulting Services Ltd (VEGA)	Project management as well as advanced solutions for simulation and training
	2008 / US DRS Technologies	VTMS, port security, law enforcement, border control; subcontractor to Boeing on SBInet
BAE Systems	2008/british DETICA	Technologies for analytical decision support, real-time situational awareness and control, secure computing and communications (anti-terrorism and anti-fraud applications)
	2000-2009 / more than ten US acquisitions in IT, defence electronics and land armament sectors	

Source: Authors.

At present, European big players hold several key technological leaderships in the security market.

- EADS: PMR networks, Maritime security & coastal surveillance, integrated security systems

  In 2003, the creation of the Defence & Security Division (today CASSIDIAN) underlined EADS' ambition to expand in the defense and security market. The acquisition in 2005 of Nokia's Professional Mobile Radio (PMR) activities has firmly established EADS as a global player in the secure telecommunication industry as well as defined it as the largest European PMR supplier. Furthermore, thanks to the acquisition of the French SME Sofrelog, EADS has consolidated its world market position in Vessel Traffic Services Systems and Coastal Surveillance Systems, accounting for, as the world leader, more than 40 percent share of the market, ahead of Kongsberg (27 percent), and HITT (10 percent). The 650 M€ contract concluded between Romania and EADS in August 2004 represents the first important opportunity for EADS to showcase its capabilities in large-scale system integration in the border security domain. The project involves information and communication systems, equipment for checkpoints at airports and land borders, coastal surveillance systems and operation centers. The maritime component contributed to a win in July 2009 of the large

Saudi Arabian national border surveillance program, which includes coverage of the Red Sea and part of the Arabian Gulf, beating competitors Raytheon and Thales. This award came after a number of contracts issued in the United Kingdom, Romania and Qatar and a subcontract for surveillance on the Saudi northern border. EADS is also pursuing homeland security opportunities in the United States. In order to sell its PMR solutions in the U.S. market and expand its industrial footprint. While solidifying its position in security systems and solutions, EADS also purchased PlantCML, a U.S. leading provider of emergency response solutions and services.

- Thales: a dual-technology strategy

  Thales' security activities combine the group's former security and services divisions with the rail signaling and security systems businesses acquired from Alcatel-Lucent in January 2007. Following the operation, and in line with the company's dual-technology strategy, Thales adjusted its positioning and objectives for the civil security market, drawing on the group's mission, critical systems know-how and experience in the defense and aerospace markets. Thales' key technologies for the civil security market encompass secure information and communication systems (encryption), process supervision and control for critical infrastructure, sophisticated sensor systems (radars, infrared cameras, intrusion detection), biometric ID cards, electronic passports, command centers for the police and fire services, trusted e-government platforms, simulation and synthetic environments. In 2009, more than 20 percent of Thales' revenues came from its security systems, which totaleded an approximate 2.9 B€ in 2009 (consolidated revenues 12.8 B€). The United Kingdom is the company's second largest country of operation after France and the leading European homeland security market. In this context, the acquisition in 2008 of the British company n-Cipher has further rounded out Thales' information security portfolio in addition to its information security services (internet and communications system security market).

- SAFRAN Group: a world leadership in biometric and detection technologies

  Security activities reported 904 M€ in revenue in 2009 (9 percent of total revenue), divided in 3 major segments: secure identification (66 percent), smart cards (26 percent) and detection (8 percent). As part of the Defense Security branch,[22] Sagem Sécurité is a world leader in biometric technologies for fingerprint, iris and face recognition and a major player in smart cards, identity management solutions, access management and transaction security. This business is positioned to become a major growth driver for Safran, and within a few years should generate 20 percent of the group's consolidated sales. Security business logged a 38 percent increase in sales and a 60 percent jump in earnings in the period 2005–2009. Since the acquisition of Motorola's biometrics business, Sagem Sécurité market share represents around 60 percent of the world AFIS market, ahead of Cogent and NEC. Moreover, with the purchase of 81 percent of the Homeland Protection division of General Electric, the group, already the world leader in biometrics, is now number one worldwide in imaging systems that detect dangerous or illicit substances in luggage. Thanks to these two noteworthy acquisitions in the United States, Safran is building a real transatlantic biometrics and detection business.[23]

- Finmeccanica: expansion in the UK and U.S. homeland security markets

  The aerospace and defense Italian conglomerate, Finmeccanica, is positioned in both civilian and military safety-critical systems markets and delivers integrated solutions for non-military domains such as Critical National Infrastructure (CNI) protection, territory control and civil

protection, maritime and border security and major event management and security. Within the field of Defense & Security Electronics, Finmeccanica operates through several subsidiaries, mainly based in Italy and in the United Kingdom (SELEX Galileo, SELEX Communications, SELEX Sistemi Integrati, Selex Services Managements, Elsag Datamat, and Agusta Westland). If Finmeccanica had consolidated its position in the UK security market, by launching a takeover bid for the British VEGA Consulting Services Ltd, the group has taken its U.S. footprint to a new level with the acquisition of the U.S. military contractor DRS Technologies for 4 B$ in May of 2008. DRS has a prominent position in the U.S. security market (VTMS, port security, law enforcement, border control; subcontractor to Boeing on SBInet). Thanks to the DRS portfolio, Finmeccanica is now considering possible bids on border control projects in in the Middle East, North Africa and Central Asia).

- BAE Systems: focus on information-based intelligence capabilities

  BAE Systems has established good positions in homeland security in both the UK and the U.S. security markets. Among the key European industrial players active in the U.S. security market, the group has established one of the most extensive market positions as the prime contractor or team member on a number of global contracts.[24] Alongside its established defense-related activities, BAE Systems has a growing position in national security with a focus on information-based intelligence capabilities (information technology, cyber-security, mission support and services), as well as seeks to capitalize on its leadership position in electronic warfare and infrared technologies. As a trusted provider of the U.S. DoD, BAE Systems has made a number of acquisitions related to defense, some of which are also related to homeland security. For instance, Armor Holdings, a U.S. maker of military and heavy vehicles (acquisition made in 2007) provides state and local police forces with mobility and protection systems (tactical vests, armor, helmets). BAE Systems are also engaged in extensive work in information technology for DHS. For instance, DHS has selected BAE Systems to develop a prototype for a system designed to protect commercial aircraft from heat-seeking, shoulder-fired missiles (JETEYE aircraft missile defense system). As a result of DHS grants, several municipalities have acquired their First InterComm first-responder interoperable communications system.

  In the United Kingdom, BAE Systems has acquired Detica (2008), which is comprised of British civil IT contracts with the police, local government, banking, telecoms, transport, and health sectors. Furthermore, the group develops a number of partnerships with innovative UK SMEs in areas such as cyber-security, biometrics and intelligent surveillance systems (i.e. with the face-recognition British specialist Omniperception on developing a gait and facial behavior recognition to be integrated into street corner CCTVs).[25]

  Other European based mid-sized companies have gained stronger positions in the worldwide market, such as Konigsberg Maritime (tracking and tracing of goods for maritime transport submarket), or Smiths Detection in the air cargo security submarket (screening systems and equipment for x-ray screening and trace detection of explosives).[26]

  More generally, and as underlined by Ecorys Report, although Europeans hold technological leadership with regard to several products and services in the global security market, with the exception of the major players and a few mid-sized companies, the supply chain remains fragile.

U.S. industry, reluctant to pursue projects in Europe?

U.S. companies are already active in the international market, but their domestic market remains the most attractive and important. In Europe, the large number of competitors and the fragmentation of demand seem to have hindered competition from the United States. But U.S. defense groups like Raytheon, Northrop Grumman and L-3 Communications, which are well positioned in the British defense market, are counting on border security and IT projects to drive revenue growth overseas and to obtain entry into the civil security and surveillance market.

Raytheon is not only the most active company, but is the market leader due to its success in the UK market. In 2007, the group was selected as the prime contractor, by the UK Home Office, to develop and implement the nation's e-Borders project, an advanced border control and security program. In December 2009, the Board of Directors of the European Organization for Security (EOS, a trade association) unanimously accepted Raytheon Systems Ltd as a new EOS Member, the U.K. affiliate of Raytheon Company. Northrop Grumman is a principal member of the BT team and was selected in December 2009 by the UK Technology Strategy Board to develop a cyber-test range for the research and testing of cyber security threats on large-scale networks. L-3 Communications also entered this market by acquiring TRL Electronics, a UK Leader in Secure Radio and Satellite Communications for Defense and Homeland Security Applications.

Conclusion/Recommendations

Despite the absence of a transatlantic political dialogue to identify common threats and common security missions, EU and U.S. official documents have revealed an impressive commonality of high level missions in the field of homeland security.

EU (ESRAB)	US (QHSR)
Border security	Securing and managing our borders
Protection against terrorism and organized crime	Preventing terrorism and enhancing security
Critical infrastructure protection	Safeguarding and securing our cyber space
Restoring security in case of crisis	Ensuring resilience to disasters
	Securing and administering our immigration law

Source: Authors.

Some differences exist in the approach toward key mission areas and their priorities, however, the capability and technology needs of both actors remain inherently similar.

Such similarity, thus, creates the necessary basis for transatlantic industrial cooperation within the security domain. Already special attention to certain industries is noticeable across the EU and the United States, particularly in biometrics, IT and secured communications. The European industry participation in the U.S. security market and the interest showed by some U.S. firms toward the EU confirms present-day transatlantic interaction and a more open market, when compared to the defense sector.

In order to foster cooperation, interoperability of solutions and common standards for next generation of security solutions is essential. Such a need is felt in the EU as interoperability is needed across the 27 member states as well as in the United States (across federal, state and local lines). The enlargement of transatlantic interoperability and standardization will also be crucial.

This dimension, which is transversal to all missions, has already been introduced at the transatlantic level in some security frameworks (i.e. FRONTEX, EDA). European high-level groups recognize the importance of this dimension recommending cooperation, especially with regards to standards and market access to third countries in the security FP projects. The launch of EU-U.S. R&D projects focused on the development of common technological building blocks could be the right starting point.

However, the economic slowdown on both sides of the Atlantic does not seem to offer the best window of opportunity for public investments, and industries seem to look to new emerging markets. The EC should support security procurement through European agencies in order to exploit R&D results financed with European resources.

In order to enhance the visibility of EU and U.S. security industries and SMEs as well as to assess the feasibility of industrial and technological cooperation in the security domain, the EU and the United States could co-organize an annual transatlantic security forum. Key institutions, stakeholders and end-users at the technical and operational level, rather than high political level, should participate and discuss the opportunities for partnership and contribute to information sharing, market trends analysis, channels for sales, key requirements, customer preferences and discuss the operating constraints and regulatory environment of the security market.

CHALLENGES TO AGENDA-SETTING PRIORITIES: TOWARD EFFECTIVE PUBLIC-PRIVATE PARTNERSHIPS FOR SECURITY IN THE EU AND UNITED STATES

Erik Brattberg, *Research Assistant, UI,* and Jan Joel Andersson, *Head of Security and Defence Programme and Senior Research Fellow, UI*

Introduction

This paper examines the relationship between governments and the evolving security industry in developing capacity to implement security strategies in the United States and in Europe,[27] respectively. We are interested in exploring if, and how, the security industry provides governments with the tools for carrying out strategies, and whether it does so in close cooperation with governments via institutionalized relationships. Our paper will explore that relationship, using the "traditional" defense industry relationship as an implicit comparison, to arrive at problem areas and issues for improvement. Our analysis is based on the premise that the relationship between government and industry is mutually dependent and supportive, rather than antagonistic or with industry as the only *demandeur* in the relations (as is the case in other policy sectors). Our main argument is that the industry-government relationship in the security domain is still evolving, hence sharply contrasting the defense industry, which has long-since evolved its capacity. The security sector, on the other hand, is still in the process of developing an efficient, effective and productive relationship with government so as to set the agenda. Our conclusion is that an effective and mutually supportive relationship between government and industry is crucial for the implementation of security strategies. As a result, this paper presents several recommendations for further strengthening cooperation between government and industry on both sides of the Atlantic.

This paper proceeds as follows: first we provide a brief overview of the traditional defense industry-government relationship in Europe and the United States. Then we account for the new security industry-government relationship on both sides of the Atlantic. Based on this discussion, we then draw some implicit conclusions about the changing nature of the industry-government relationship, point out some key similarities and differences between the EU and the United States, and some key challenges. Finally, we provide key recommendations for addressing these challenges.

The Traditional Defense Government-Industry Relationship

Europe

After a series of national and international mergers, beginning in the 1960s, the European defense industry has, as of 2010, reduced to only a handful of actors and countries. At the highest level, global companies such as BAE systems, EADS, Thales, and Finmeccanica are all among the top ten arms producers in the world. Rapid advance in technology development have made distinctions between aerospace, land armaments and naval systems less relevant. Today, BAE Systems produces the full range of armaments from artillery and fighter aircraft to nuclear attack submarines. Similarly, EADS produces military aircraft, electronic systems and missiles in several European countries. The exception to this trend of European and international concentration is the armored vehicle industry that largely remains fragmented across many programs and countries.

Behind this group of major arms producers, there are smaller, but still important European defense industry companies, such as the world's leading British engine maker Rolls Royce, major French naval producer DCNS, Swedish aerospace company SAAB and German armored vehicle specialist Rhinemetall. Moreover, there are several traditional defense industry companies in Europe owned by U.S. companies. Today, classic names such as Steyr-Daimler-Puch Spezialfahrzeug GmbH (STEYR-SSF) of Austria, MOWAG GmbH of Switzerland, and Santa Bárbara Sistemas of Spain are all part of General Dynamics European Land Systems (GDELS), a business unit of U.S. defense giant General Dynamics.[28]

The traditional defense industry is organized into national defense industry associations. These organizations are in turn organized in the Aerospace and Defense Industries Association of Europe (ASD). Today, ASD members include 28 National Trade Associations in 20 countries across Europe, representing over 2000 aeronautics, space and defense companies. Together these companies employ a total of approximately 676,000 employees and a turnover of over 137 billion € in 2008.[29] The ASD is the result of a merger in 2004 of AECMA, EDIG and EUROSPACE to reflect the integrated nature of civilian and military technologies and between aerospace and defense. The simultaneous creation of the European Defense Agency (EDA) in 2004 meant that both the European defense industry and the EU, for the first time, had a unified contact point for discussion and exchange of views.

The EDA's mission is to support the EU member states and the Council in their efforts to improve European defense capabilities. The EDA's functions and tasks are to develop defense capabilities, promote Defense Research and Technology (R&T), promote armaments co-operation and to create a competitive European Defense Equipment Market and a strengthened European Defense, Technological and Industrial Base (EDTIB). By promoting coherence, these functions aim to improve Europe's defense performance. The argument is that a more integrated approach to capability development will contribute to better-defined future requirements in which collaborations - in armaments or R&D or the operational domain - can be built. More collaboration will not only provide opportunities for industrial restructuring but also promote larger demand and an expanding market.[30] The EDA is the central actor for EU discussions on the defense industry. The central role played by the EDA is underlined by the fact that the Agency's "shareholders" are not only the member states participating in the Agency but that the key stakeholders also include the Council and the Commission as well as third parties such as OCCAR

(Organisation Conjointe de Coopération en matière d'Armement), the LoI (Letter of Intent) group and NATO.[31]

United States

The traditional U.S. defense industry is the largest and most sophisticated in the world. Six of the seven largest defense companies and 16 of the world's 20 largest defense companies are American. Similar to the development in Europe, the U.S. defense industry has undergone a series of major mergers. Today, the traditional U.S. defense industry is dominated by a dozen companies led by Lockheed Martin, Boeing, Northrop Grumman, General Dynamics and Raytheon. Each of these companies has numerous production sites spread around the country and post arms sales ranging between $20–$30 billion per year.[32] With nearly 3.5 million people employed in a defense-related industry, the traditional U.S. defense industry carries significant political clout at the local, state and federal level.

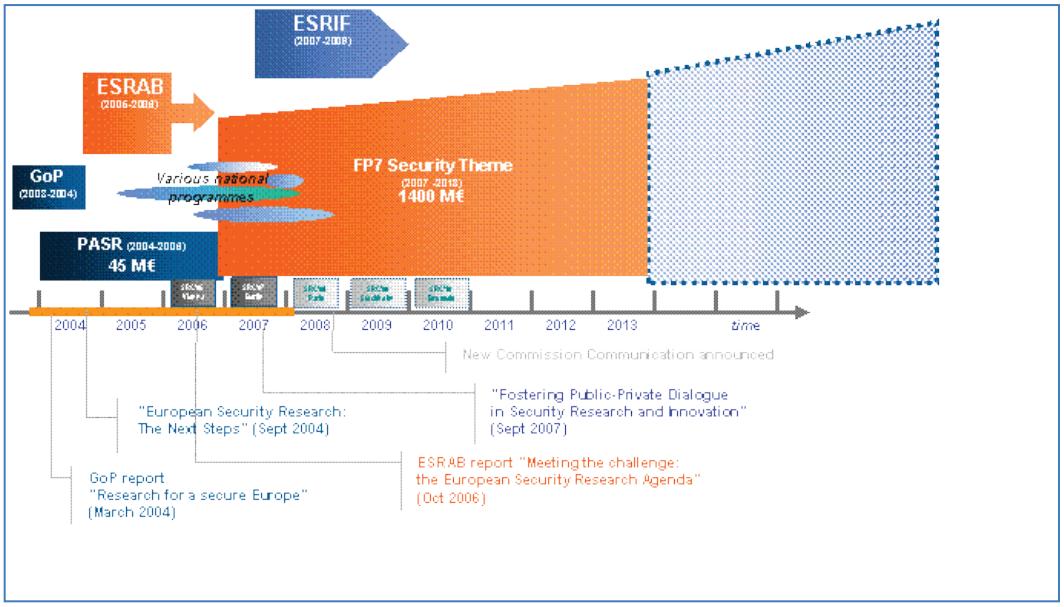
The relationship between the U.S. government, the U.S. military and the defense industry has long been very strong. For decades, a network of contracts and flows of money and resources between the defense industry, the Pentagon, the Congress and the Executive Branch have made relations between industry and government very close. The long tradition of government officials and retired military officers taking up positions in the private industry and the tendency of government to recruit procurement managers and policy specialists from industry, also lead to shared understandings and multiple access points to influence government policies. Such policies include approval for research, development, production, use, and support for military training, weapons, equipment, and facilities within the national defense and security policy.

The New Security Industry-Government Relationship

In this section we will discuss the changing security industry-government relationship in Europe and the United States. For both sides of the Atlantic, we will (i) focus on the expansion of the security agenda and (ii) describe the security industry.

The Widening of the European Security Agenda

While most security funding in the European Union remains available at the national level, the need to develop a European Security Research Program grew out of the awareness that Europe risked exclusion from the growing market of scientific research and technological innovation related to new security measures. To help remedy this situation, the EU started a process of consultation and coordination to fund security research and help the structuring of the market in the security sector. This process started with the *Group of Personalities* in 2004 and was followed by the *Preparatory Action for Security Research* (2004 to 2006), the *European Security Research Advisory Board* (ESRAB from 2005 to 2006), the *European Security Research and Innovation Forum* (ESRIF from 2007 to today) and the *FP7 Security Theme* (2007-2013), summarized in the figure below. The next section will begin by taking a closer look at the development of the EU security research program starting with PASR to the FP7 security theme.



Source: See http://ec.europa.eu/enterprise/policies/security/industrial-policy/research-agenda/index_en.htm.

Group of personalities in the field of security research (2002-2004)

In order to develop longer-term public-private cooperation on European security research, the European Commission, in 2003, set up the "Group of Personalities" (GoP), composed of high-level industrialists, Members of the European Parliament (MEPs), and representatives of international organizations and research institutes, whose purpose was to lend their expertise in establishing a strategy for a secure Europe and to spearhead the process of enhancing the European industrial potential in the field of security research.[33] The GoP presented to the Commission a report entitled "Research for a Secure Europe," advocating the combination of national, intergovernmental and community research across the civil-military continuum and the development of a ESRP, with respect to civil liberties and ethical principles. Twelve recommendations were put forward and the guarantee that a minimum of €1 billion per year in funding would be allocated for research in the security field, in addition to existing funding. The GoP also recommended the establishment of a European Security Research Advisory Board "to draw strategic lines of action and to prepare the research agenda of a European Security Research Program as well as to advise on the principles and mechanism of its implementation. In September, 2004 the Commission published the communication "Security Research: The Next Steps" endorsing GoP's recommendations.[34]

Simultaneously, the Commission launched the Preparatory Action for Security Research (PASR), toward the end of the 6th Framework Program for research (FP6), aiming at harmonizing security research activities in Europe, coordinating existing capabilities and competences and preparing the groundwork for the introduction of the security theme in the next Framework Program. Between 2004 and 2005, three proposals led to the funding of 39 R&D projects totaling 45M€. The main thematic areas of research included: crisis prevention and crisis management systems; space surveillance; critical infrastructure protection; and protection against terrorism.[35]

PASR also served as the predecessor to the Commission's full security research program, the FP7 (see below).

European Security Research Advisory Board (ESRAB) (2005–2006)

The European Security Research Advisory Board (ESRAB) was established in April 2005 as an attempt to bring together, at European level, the market's demand and supply sides in order to jointly define commonly agreed upon strategic guidelines for European security research. It was tasked to ensure consultation and cooperation among all stakeholders in order to outline a comprehensive European security research agenda as well as to establish a network between end-users and stakeholders to identify technological capabilities. Additionally, it sought to provide advice on the strategic and operational aspects of the future program and on its implementation.[36] Consisting of some 50 high-level specialists and strategists, including public authorities (including MEPs and Commission's officers), think thanks and research institutes, research and technology suppliers and industry representatives, ESRAB's final report, entitled "Meeting the challenge: the European Security Research Agenda," was released in September of 2006. This report offers a strategic framework to structure the research content covering both technological and non-technological aspects, identifying and prioritizing only those areas which offer high potential to deliver European added-value. Among other things, the report recommends that European security research compliment national security research programs, and where these already exist, align themselves to EU programs.[37] The ESRAB report identifies three areas of cross cutting interest for security research: integration, connectivity and interoperability; capabilities and technologies; and demonstration programs (e.g. capability development, system development, and systems of systems demonstration).

European Security Research and Innovation Forum (ESRIF) (2007-2008)

In line with the final GoP report , the European Security Research and Innovation Forum (ESRIF) was established in September of 2007 to serve as an informal and voluntary group of experts representative of both the demand and the supply sides of the security sector and various societal organizations. To date, ESRIF has 64 formal members.[38] In addition, more than 600 individuals have registered as contributors to ESRIF's 11 working groups, providing a broad basis for the forum. ESRIF was established to develop a mid and long-term (up to 20 years) European Security Research and Innovation Agenda (ESRIA) linking security research with security policy making, through public-private dialogue by 2009.[39] Accomplishing this objective, ESRIF brought together industry, public and private end-users, research establishments, universities and non-governmental organizations from 32 countries. ESRIF's final report contained a set of key messages addressing the necessity of a future European security and relevant research, the need to reduce the fragmentation of the security market as well as the need to enhance the currently insufficient degree of interoperability and standardization.

FP7 "security theme"

To promote security research in Europe, the Commission has launched two, seven-year Framework Programs in the security domain, totaling €2.135 billion in funding over the 2007–2013 period. The first is the FP7, which was launched by DG Research in 2007 and will last through 2013.[40] Under the FP7, the European Commission has made €1.4 billion specifically available for the security research theme (out of a total budget of €50 billion). This is the first time

that DG Research has funded research in the security area, including "security of citizens," "critical infrastructure," "surveillance," "border security," and "crisis response." This figure is somewhat misleading, however; security-related projects within other themes can also be identified, such as "information and communication technologies," "transports," and "space." Additionally, under the FP7 framework is the Joint Research Centre (JRC), a research-based policy support organization to the Commission providing the scientific advice and technical know-how to support a wide range of EU policies touching five policy themes. The FP7 will provide the JRC with €1.8 billion for research across four priority areas. At least two of these themes—"security and freedom" and "Europe as a world partner"—relate to security.[41] The second is the EU Framework Program on "Security and Safeguarding Liberties" with a budget of €745 million provided by the DG for Home Affairs.

The New Security Industry in Europe

This section will focus on the participation of industry in shaping the EU's security research agenda. The GoP included 25 members, among them four members from Europe's four largest aerospace and defense companies (EADS, BAE Systems, Thales, Finmeccanica) and four representatives from the ICT sector (Ericsson, Indra, Siemens and Diehl). In this context, Didier Bigo and Julien Jeandesboz conclude that "major defense and security companies have played a key role in the definition of the orientation and priorities of the EU's research and development policy for security-related technical systems."[42] In ESRAB, out of a total of 50 personalities, 28 percent were industry representatives (bio, manufacturing and ICT), 36 percent from EU member states (ministries of Defense and Interior and police forces) and 28 percent from research institutes and academia. Since September 2007, EADS, Thales, Safran (Sagem), Finmeccanica, SAAB and Smiths Group are all members of the voluntary strategy group ESRIF, serving as rapporteurs of four Working Groups in charge of drafting building blocks for the security research agenda.

Beginning with the GoP, through to the PASR, to the ESRAB and ESRIF today, the biggest European defense companies have had an indubitable influence upon shaping the EU security-research agenda, strategy and research projects. Their inputs are noticeable in writing the three EU security research strategy reports. Furthermore, European defense companies have also benefited considerably from the EU security research programs. Of 39 security research projects (PASR 2004-2006) and 45 FP7 projects (first call), 21(54 percent) and 7 (15,5 percent), respectively, were led by European defense groups. Thales is the most active industrial player, participating in 23 projects, coordinating 8, followed by Finmeccanica, EADS, Safran/Sagem DS, BAE Systems, Diehl, SAAB, Dassault Aviation and Indra. Thales, EADS and Sagem DS are the most recurrent.

The industry has also sought to influence EU security policies through participation in the European Organization for Security (EOS), an association of European private-sector security actors founded in 2007. The organization's primary goal is to support the development of a European security market by promoting innovation and implementation of European civil security capabilities. EOS recently produced a report entitled "Priorities for a Future European Security Framework," which contains a number of recommendations over a five-year period (2010–2014) on how to implement a structured European security framework.[43] These suggest:

- developing a comprehensive, coherent and sustainable EU model for security;

- strengthening the Public-Private Security Dialogue in support the development of security policies;
- creating, under the umbrella of an EU Security Program, relevant EU sectorial programs (such as Borders Control, Civil Protection, Protection of Resilience and Critical Infrastructures and Services, Security of Transport, Cyber Security);
- creating conditions for the development of a harmonized EU Security Market by establishing legal frameworks and societal/privacy aspects linked to security.

The creation of EOS was encouraged by the European Commission, which hopes to see the security industry become a more organized "counter-part" to help consolidate the European security market and considers EOS to be a viable alternative to the Aerospace and Defense Industries Associate of Europe (ASD).[44]

With regard to ASD, its key priorities include future security research programs "that are fully geared to operational objectives, technology developments and to strategies for innovation implementation." It also seeks to establish an appropriate and robust defense industry, proper market policies at EU level and a harmonized European Security Environment.[45] With regard to the latter priority, ASD notes that the current European security market is characterized by many purchasing authorities that coexist and act in limited coordination. Furthermore, ASD perceives the EU security market as "highly fragmented and unstructured." ASD, therefore, seeks to increase competiveness and reduce market fragmentation through the development of a comprehensive and sustainable European industrial security policy as well as a structured public-private dialogue between the demand and supply sides.[46]

The Rise of Homeland Security in the United States

The 9/11, 2001 terrorist attacks highlighted the vulnerability of the United States to a "new" range of transnational threats and brought impetus for a homeland security overhaul. This process culminated with the establishment of the Department of Homeland Security (DHS) in late 2002. By consolidating many of the essential departments and agencies previously charged with providing for homeland security activities in the United States, DHS became responsible for identifying and developing plans for protecting critical infrastructure; conducting intelligence gathering and analysis; exercising the mechanisms to enhance emergency preparedness; coordinating and sharing information with other executive branch agencies, local and state actors and with non-federal entities.

But DHS has also come to play a key role in supporting homeland security research. For this task it has formed the Directorate of Science and Technology (S&T) to help organize scientific, engineering and technological resources for the various homeland security missions.[47] S&T partners include federal state and local agencies as well as laboratories, universities and the private sector. The Basic Research Focus Areas of the S&T Directorate were generated from six divisions of the Research Leads in the Directorate with input from the research community and vetted through the S&T Directorate's Research Council. These focus areas represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs and help guide the direction of the S&T research portfolio to provide long-term science and technology advancements for the benefit of homeland security. These six focus areas are: Explosives Division Focus Areas (EXD), Chemical and Biological Division Focus Areas (CBD), Command, Control, and Interoperability Focus Areas (CID), Infrastructure and Geophysical Division Focus Areas

(IGD), Human Factors Division Focus Areas (HFD), and Borders and Maritime Division Focus Areas (BMD).[48]

The prioritized research needs initially focused on the area of counterterrorism. Currently, DHS spending on homeland security R&D is $1.1 billion, a 9.2 percent increase from the 2008 fiscal year.[49] The largest sector of the DHS R&D portfolio is Domestic Nuclear Detection Office (DNDO). DNDO was removed from the S&T Directorate in 2006 and is now an independent entity devoted to radiological and nuclear counter-measures. The second biggest area is the chemical and biological countermeasures portfolio which is located within S&T. Furthermore, DHS research, excluding development funding, is heavily oriented around the life sciences and engineering. The research portfolio as a whole is currently expected to continue growing, as research becomes a larger part of DHS R&D and development funding declines.[50]

Besides the Department of Homeland Security, several other federal agencies are involved in R&D efforts pertaining to the area of homeland security. Prior to the establishment of DHS, homeland security-related R&D was spread out across various federal agencies, but since its creation, much of this funding has been channeled specifically to DHS. However, some homeland security R&D funding remains with other federal agencies, including the Departments of Health and Human Services, Defense, Agriculture, and Energy and the Environmental Protection Agency.

The Homeland Security Industry in the United States

The reorientation of the U.S. security environment following the 9/11 attacks paved the way for an explosion of government spending in the homeland security area. According to HSToday, an industrial magazine, the homeland security industry "has grown at an extremely fast and disorganized pace."[51] In the early period following 9/11, the U.S. homeland security market tended to be dominated by smaller firms already specialized in homeland security technologies. But the growth and consolidation of the market soon attracted larger companies with extensive experience in government contracting to join the field, including traditional defense companies such as Halliburton, Lockheed Martin, Raytheon, and Northrop Grumman.[52] According to Lockheed Martin's Senior Vice President, Art Johnson, larger companies have benefited because they have already established government contacts with the various agencies before they were merged into the DHS.

According to directory maintained by HSToday, the homeland security field now consists of some 300 companies,[53] while the *Washington Post* has listed almost 2,000 companies working on programs related to counterterrorism, homeland security and intelligence in the United States.[54] The initial focus of the homeland security market was airport security. The industry has since then expanded to include a wide range of different companies, including chemical, biological and radiological detection; border, rail, seaport; industrial and nuclear plant security; integrated technology and surveillance, etc. Even though most government contracts go to larger companies, smaller companies benefit as they serve as sub-contractors to these companies. During the FY 2005, roughly a third of all government contracts went to smaller companies. Increasingly, however, U.S. government spending on homeland security is also going to so-called second-generation anti-terrorism products. Concurrently, homeland security spending has departed from the initial focus on terrorism and is exceedingly "all-hazards" oriented. In the aftermath of Hurricane Katrina a number of engineering and construction companies became major

contractors to FEMA, which in FY 2006 accounted for roughly a third of the DHS procurement budget.

Unlike the traditional defense market in the United States, a significant challenge to security companies is customer fragmentation. Success in the homeland security market depends on the ability to sell to multiple customers of varying size: federal governments, state and local governments (counties and cities) and the private sector. While DHS plays a key role in homeland security, it is far from dominating the demand side of the market. The combined FY 2010 for state and local markets totaled $16.5 billion, whereas the DHS homeland security market totaled $13 billion. However, DHS still plays a major role in shaping the industry. The creation of DHS has contributed significantly to the growth in the number of homeland security providers (both in terms of products and services), new companies and new divisions of existing companies. Less than 1 percent of federal contracts in 2000, DHS outsourcing has quadrupled as a portion of federal contracting from 2003 to 2009.[55] Contrary to the confusion of its earliest days, DHS seems to have stabilized its policies and operations, with consistency programs and long term commitments of funding for acquisitions.[56] For instance, we can note a notable expansion of the involvement of DHS in long-term programs, particularly in electronic identification, cyber-security and critical infrastructure.

The growth of the homeland security market has attracted traditionally non-security oriented companies to enter the market and has encouraged the creation of many companies focused solely on this sector. According to Civitas Group, the dual-use nature of many of the homeland security sector's applicable core technologies and its close alignment with the defense, intelligence, information technology and, in some cases, biotech markets, has also allowed established technology companies to diversify across a number of growing markets. It has also provided the opportunity for security-focused companies to diversify into adjacent sectors. This dynamic is contributing to the development of a market increasingly defined by a number of large companies at the top, a large and vibrant pool of small, innovative companies at the bottom, and a select few in the middle. Moreover, IT and software technology companies (e.g., Sun Microsystems, Oracle, IBM, HP Enterprise Company, HP, Cisco, MacAfee) that previously paid little attention to government contracts, now look for business opportunities in the homeland security market in the context of growing needs in IT Security expressed by the federal government/agencies and declining commercial spending.

The growing importance of services (from IT integration, engineering consulting, and management support to construction, guard services, and facility management), areas where DHS spends the most money, represents another trend, which has become more and more noticeable. This trend explains the growing involvement of service providers.[57] In five years, the top U.S. defense contractors have moved to consolidate their portfolio of products and services and strengthened their market position by implementing the following strategic orientations: creation of "homeland security" new branch/division and/or subsidiaries; strengthening the homeland security business by applying technologies and systems integration expertise developed in defense business; and acquisition of SMEs with valuable technology, intellectual property and/or target market channels focused on intelligence and homeland security. Large defense companies retained their competitiveness on the homeland security market because they also had existing ties to various agencies that were wrapped into DHS when it was created. They anticipated a reduction in defense budgets and a shift in customer priorities, and then realigned their position to allow for growth in new and adjacent markets, while continuing to serve existing defense customers.

Moreover, as noted by Civitas, the end-user demand for integrated solutions is a dominant characteristic of this market, a characteristic that tends to favor large systems integrators who can provide both the hardware and the necessary IT backbone for such systems.

Public-private relations in the U.S. security sector

In the United States, the security industrial base has not established separate formal mechanisms to interact with the public authorities in charge of developing homeland security requirements and acquisition policies. DHS acquisition policy is governed by the Federal Acquisition Regulation (FAR), which governs all government acquisition (the Department of Defense has the Defense Federal Acquisition Regulation Supplement - DFARS). No prominent industry associations exist that are dedicated solely to homeland security. There are formal committees under DHS that include industry members, but their interactions are controlled and must be conducted under the Federal Advisory Committee Act. Lobbying activities are closely regulated and lobbying by a specific company on a specific acquisition program cannot be undertaken with the responsible government entity while the acquisition is being considered.

However, defense companies, many of which also undertake work for DHS, use the existing national security trade associations and advocacy groups to also represent their interests in the homeland security domain. As a result, behavioral patterns and practices characterizing the defense sector seep into the security domain, despite the lack of a strong separate trade association or robust formal processes to influence the security agenda-setting as exist in Europe through ESRAB, ESRIF and so on.

What emerges from this analysis is a U.S. situation substantially different from the European one. In Europe, given the lack of a public authority dealing with security policies and procurement, companies commit themselves to joint efforts to institutionalize public-private partnerships in the security domain. In the United States, DHS centralizes the majority of federal decision-making and procurement policies and the FAR regulate all federal acquisitions. Companies, by themselves or through associations and lobbyists, attempt to influence government acquisition within a well-defined legal framework. Defense companies are better positioned to do so via the trade associations in place to represent them vis-a-vis the Department of Defense.

Conclusions

Whereas the Cold War environment was based on clear external threats from state actors which required traditional defense capabilities, the new security environment is characterized by new forms of both actor-based and structural threats, making security capacities harder to define. The changing threat environment and the different defense capabilities needed to handle new threats have paved the way for "new" security industries in Europe and the United States. In both the EU and the United States, it is possible to contrast the emerging security industry-government relationships from the traditional defense-government relationships in two major ways.

First, the type of companies is different. Whereas the old defense industry was dominated by a handful of large companies with the capacity to produce large-scale weapons, the new security industry consists mostly of mostly smaller companies with niche specialties. It appears as though the traditional large defense companies have not been adequately prepared for the new security

environment. Even though many larger companies are now entering the security market, a rapidly growing number of smaller companies with niche specialties in areas such as border security have already sprung up, particularly in the U.S. DHS seems to favor using existing civilian technology for homeland security application rather than developing new technology from scratch. In the EU, however, many smaller companies find the FP7 applications overly bureaucratic and the administrative burden too high.

Second, the type of government relationships is also different. Before, the large defense companies could enjoy "cozy" and heavily institutionalized relations with national governments, today this is much more difficult due to market fragmentation, on the one hand, and the lack of organization of the industry, on the other. At the same time, it appears that big traditional defense players have been able to leverage existing government contacts to some degree in both the EU and the United States. Of note is the fact that the EU has made specific efforts to cultivate and institutionalize relationships with the security industry and supranational governance in Europe, which is by definition a major contrast with the defense-government relationship of earlier years.

What then are the specific challenges pertaining to the new security industry developing in the EU and the United States and how are they best addressed? First, end-users are highly diverse. With several government buyers at both the national, regional and local level and with non-profit and private sector buyers, the market perceives a lack of predictability. The industry accordingly needs predictable funding and regular procurement requests as well as a predictable market for products. Furthermore, the industry needs clearer funding agendas and needs assessment by governments. Furthermore, public-private partnerships in the field of security research is of utmost importance in order to increase the security of infrastructures, to fight organized crime and terrorism, to help restore security in times of crisis and to improve surveillance and border control. Governments cannot pursue security for its citizens without being closely aligned with the security industry at both the policy formation and implementation stages. A characteristic of the security area is that much of the critical infrastructure remains in private hands. Industry actors must hence be involved in formulating requirements that prepare for future threats and aid in the countering of such threats. Finally, there is a need for greater integration of industry in agenda-setting. Here, the EU has arguably made more progress than the United States, incorporating industry in high-level working groups to assist the Commission in identifying industry expertise and capacity, etc. Conversely, there has been a lack of involvement within industry in defining the needs of the homeland security market in the United States—in clear contrast to involvement in the defense sector.

THE REGULATORY AND ACQUISITION ENVIRONMENT FOR SECURITY IN THE EU AND THE UNITED STATES

David Berteau, *Senior Adviser and Director, Defense-Industrial Initiatives Group, CSIS;* Guy Ben-Ari, *Fellow and Deputy Director, Defense-Industrial Initiatives Group, CSIS;* Priscilla Hermann, *Research Assistant, CSIS;* Sandra Mezzadri, *Associate Fellow, IAI*

This paper provides an assessment of the regulatory environments for security and homeland security in the United States and the EU through July 2010. This evaluation is an important element in the analysis of security strategies, as it defines the field of action for industry on both sides of the Atlantic and has a heavy impact on the development and fielding of security-related capabilities. The pieces of legislation discussed in this report are by no means comprehensive, yet allow for an understanding of current market conditions and provide the basis for comparative analysis.

Security Market Regulatory Environment in Europe

Introduction

The main features of the regulatory environment for the security market in the EU are complexity and fragmentation. There is nothing like a single regulatory framework for the security market, but a multitude of different rules and regulations with different purposes for different areas. The reasons for this are the characteristics of today's security environment, the specificities of security markets and the current state of European integration.

First, it is generally recognized that the main security threats today are not large-scale military conflicts, but regional crises, natural disasters and threats from non-governmental actors, in particular terrorism and organized crime. The latter often operates globally, in transnational networks, blurring the dividing line between internal and external security. Facing such threats, governments in the EU and around the world have redefined their security and defense concepts and started to develop a comprehensive approach, combining a broad variety of policies, instruments and actions. Consequently, the areas in which security relevant rules and regulations exist are as numerous as diverse.

Second, security markets are specific and highly regulated markets. In this respect, they have some similarities, but also important differences with defense markets. Whereas the demand-side in defense markets is exclusively public and centralized at the national level, the demand-side in security markets is public and decentralized (regional, national, local), but also private. This is the

case in particular for operators of critical infrastructures. At the same time, the latter's demand for security (in particular against high-end security threats) is often driven by rules and regulations set by public authorities. In other words, public actors shape the security market as both customers and regulators, making the regulatory environment inevitably even more complex.

Third, in the EU, national and European laws co-exist. Although regulation of the security market occurs primarily at the member state level, the EU is actively promoting legislative harmonization and coordination. The Lisbon Treaty's renaming of the European Security and Defense Policy (ESDP) as the *Common* Security and Defense Policy is one such example. Security-related areas which fall under the direct competency of the Commission include, but are not limited to, research, transport, public procurement rules and standards. In addition to the legislative constraints caused by member state regulation, the Commission faces internal difficulties. The numerous Directorates General and Agencies simultaneously responsible for security activities contribute to the decentralized nature of this market sector and compound the level of bureaucratic complexity. Implications for the security market include poor product and service coordination and schedule delays.

Due to this complex regulatory environment, developing a comprehensive overview of the European security market is difficult. Assessing, in an exhaustive manner, legislation across all 27 member states and analyzing the implications for industry far exceed the size and scope of this report. Our objective is, therefore, to provide insight into the current regulatory framework of the EU focusing on three primary areas: the legislative environment for high-end security activities across the key mission areas, the Protect mission area and the recent developments in public procurement.

To begin, we will look at the EU's general policy and strategic framework for high-end security activities, regrouping the multitude of rules and regulations along four capability areas related to EU actions on counter-terrorism: prevent, protect, pursue and respond. Secondly, we will take a closer look at the Protect capability area which covers security sectors of major interest to industry, such as infrastructure security. These sectors are also the most regulated at EU level. We will also identify the challenges ahead and the limits of the current EU legislation.

Finally, we will analyze the new Defense Procurement Directive 2009/81/EC—which constitutes the only piece of legislation in the EU that applies to defense and security-related activities.

Main Features of the EU Security Regulations

EU legislative environment

EU legislation regulating the security market is quite recent. It is primarily "threat"-driven and seeks to respond to particular areas of weakness rather than provide long-term risk management and planning. It is also limited in scale and scope, with only a few binding legislative acts. The way and degree to which these EU legislative acts affect national law differs depending on the instrument used. Directives of the Council and the Parliament, for example, harmonize and coordinate national legislation; regulations of the Council and the Parliament, by contrast, become directly part of national law and leave no room for interpretation. Different types of implementing acts do not set new law but modify and update existing EU-law.

EU-wide security initiatives

As there is no single security regulatory framework for the security market at the EU level, it is necessary to look at the main EU security policy and strategy documents to identify the future objectives for this sector. There are a number of key documents which set the framework for EU policies and actions and guide the launch of regulations in the security market, particularly in the "high-end" sector:

- the EU security Strategies: the 2003 Security Strategy[58] complemented in 2010 by the Internal Security Strategy[59]
- the Counter-terrorism Strategy, with the latest update in 2010[60]
- The Stockholm Program adopted in 2009 and the related Action Plan of April 2010.

These policy documents show that in the years following 2001 terrorism was indeed the main driver for measures in the field of security threats. The London and Madrid attacks helped to keep terrorism high on the political agenda as the principle security mission, which guided and shaped the others. An Action Plan to Combat Terrorism was adopted in 2001 and was complemented in December 2005 by a Counter-terrorism Strategy. The EU Security Strategy of 2003, which guides the EU's Security and Defense Policy, was also strongly influenced by the terrorist attacks.

Over the last five years, however, we can observe a shift in security priorities at the EU level. Counterterrorism remains a major area of action; however, the Internal Security Strategy of 2010 and, more important, the Stockholm Program of December 2009 show that the EU's Security framework has broadened considerably with a stronger emphasis on citizens' direct interests, needs and perceptions. The Stockholm Program, subsequent to the Hague Program (2004–2009), is a comprehensive plan of EU justice and security policies for 2010–2014. The Commission has recently turned these political objectives into an action plan for 2010–2014 focusing on measures in the area of Justice, Fundamental Rights and Citizenship (such as improvement of data protection in the EU) and in Home Affairs (such as strengthening cooperation in civil protection as well as in disaster and border management).

More generally, security regulations and initiatives across the EU are systematically categorized across four capability areas: prevent and anticipate threats, protect citizens and infrastructures, pursue and investigate criminals, and respond by managing the consequences of a disaster.

The measures and initiatives initiated under the "Protect" pillar have the most effect on the security market as they require high value investments in infrastructure protection and border security and often produce new security standards.

Protection

The area "Protect" can be classified in 3 main priorities:

1. Protection of citizens: with measures such as securing EU passports through the introduction of biometrics;
2. Protection of borders (sea and land): with the establishment of the Visa Information System (VIS) , the second generation Schengen Information System (SIS II); and the development of risk analysis of the EU's external border via the establishment of Frontex;

3. Protection of infrastructure (aviation, maritime and rail): with the implementation of agreed common standards on civil aviation, port and maritime security; the development of a European program for critical infrastructure protection; and the promotion of EU and Community level research activity.

The following section will address the regulatory frameworks for critical infrastructure protection. These mission areas are critical for European security and will, to a large degree, dictate the future regulatory environment for security across all 27 member states.

Legislation

- The terrorist attacks in Madrid and London highlighted the risk of terrorist attacks against European infrastructure. The EU responded in adopting a framework (EPCIP) for the protection of critical infrastructure that would develop a common level of protection in Europe. The objective was to make sure that each member state would provide adequate and equal levels of protection concerning their critical infrastructure and that the rules of competition within the internal market would not be distorted.
- More specifically, the Commission adopted in October 2004 a Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism."[61] This Communication provides, in particular, a very broad definition of critical infrastructures covering a wide range of sectors: energy installations and networks, communications and information technology; finance (banking, securities and investment); health care; food; water (dams, storage, treatment and networks); transport (airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems); production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials); government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).
- In 2006, the Commission adopted a policy package on EPCIP composed of a Communication (COM (2In006)786 final) and a Directive (COM (2006) 787 final. The Communication deals with general policy in connection with EPCIP, whereas, the Directive focuses on the designation of critical infrastructure of a European dimension (European Critical Infrastructure or "ECI").
- In 2008, a Council Directive (2008/114/EC) was adopted on the identification and designation of ECI and the assessment to improve their protection in the field of energy and transport.

The conclusion to be drawn from this legislative framework is that member states and the owners/operators are ultimately responsible for protecting ECI. Identification of ECI is established via a Commission developed procedure has developed a. However, the European Union has also adopted a number of legislative measures setting minimum standards for infrastructure protection in the framework of its different EU policies. This is notably the case in aviation and maritime transport.

Aviation Security

Security has been a matter of concern for civil aviation for several decades. However, in spite of its economic importance and cross-border dimension, aviation security has, up until more recently, been addressed on essentially a national level. Following the terrorist attacks of 9/11, the Commission made a legislative proposal to bring aviation security under the EU's regulatory umbrella. The EU adopted its first common regulations in the air transport security domain in the

aftermath of the 9/11 attacks and international cooperation on security issues considerably increased.

Legislation

- The first common regulations adopted in 2002, following international standards on aviation security, provided the basis for harmonization of aviation security rules across the European Union with binding effect.[62] In relatively short period of time, several acts of implementing legislation were added.[63] That regulatory framework has been fully completed and replaced by a new framework, in full effect since 29 April 2010, as laid down by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March, 2008 on common rules in the field of civil aviation security.
- The EU regulation (300/2008) lays down measures for the implementation and technical adaptation of common basic standards regarding aviation security to be incorporated into national civil aviation security programs. The regulation provides standards for airport planning requirements, aircraft security, staff training and most importantly screening. Member states and/or airports are given a list of screening and controlling methods and technologies for passengers, baggage, cargo and courier from which they must choose the necessary elements in order to perform their aviation security tasks in an effective and efficient manner (using a basic hand search, walk through metal detection equipment, conventional x-ray equipment, high definition x-ray and bio-sensory technologies such as sniffers, trace detectors and explosive detection dogs). The regulation also provides a set of guidelines for equipment used in support of aviation security. For instance it defines requirements (security, operation requirements) for metal detection equipment.[64] It also provides standards and testing procedures for x-ray equipment (performance requirements and operational requirements).[65]
- Member states are free to set more stringent security measures in case of increased risk, provided they are relevant, non-discriminatory and proportional to the risk addressed.

Public Procurement

In August 2009, Directive 2009/81/EC on the procurement of defense and sensitive security supplies, works and services entered into force. Member states have two years to transpose this directive into their national legislation. Directive 2009/81/EC aims mainly at bringing the bulk of defense procurement into the internal market, thereby opening up national markets to EU-wide competition and establishing the basis for a European Defense Equipment Market.

The procurement rules laid down in Directive 2009/81/EC do not only apply to defense, but also to the security market. This directive is thus the only piece of EU legislation which covers the whole spectrum of military and non-military security, including contracts awarded by private operators of critical infrastructures in the water, energy and transport sectors. In the field of defense, its scope is (at least indirectly) defined by military lists. In the field of security, by contrast, its scope is defined in a very generic way: The directive applies to "sensitive procurements" and defines the latter as *"equipment, works and services for security purposes, involving, requiring and/or containing classified information."* This very generic approach makes it possible to apply the directive across the entire spectrum of security areas. In this context, recital 11 specifies that *"in the specific field of non-military security, this Directive should apply to procurements which have features similar to those of defense procurements and are equally sensitive.*

This can be the case in particular in areas where military and non-military forces cooperate to fulfill the same missions and/or where the purpose of the procurement is to protect the security of the Union and/or the Member States, on their own territory or beyond it, against serious threats from non-military and/or non-governmental actors. This may involve, for example, border protection, police activities and crisis management missions."

To what degree the directive will open national security markets to EU-wide competition is hard to predict for various reasons. As clearly shown by the FRS paper, *The Security Market in the EU and the United States: Features and Trends*, there are hardly any figures on the size of these markets, let alone their openness. In other words: there is no reliable baseline for an impact assessment.[66] In addition, up until now, member states have exempted their sensitive security procurements via an exclusion clause of the General Public Procurement Directive 2004/18/EC, which states that this directive *"shall not apply to public contracts when they are declared to be secret, when their performance must be accompanied by special security measures . . . or when the protection of the essential interests of that Member State so requires"* (Article 14). The question for the future is twofold:

- How many contracts, which have been exempted up until now from directive 2004/18/EC, will be in the future awarded according to the rules of the new directive 2009/81/EC and,
- What is the financial value of these contracts in comparison to defense procurement, where are production volumes and orders normally much larger than in security?

The new directive contains a number of provisions specifically adapted to the special features of security procurement. For security customers, protection and privacy of classified information and reliability of suppliers are particularly important; the directive allows making such requirements in different forms (in particular, as selection criteria and/or contract execution conditions). These safeguards are expected to limit the cases where contracting authorities "have" to derogate in order to protect their essential security interests to only exceptional cases.

At the same time, however, the directive itself contains a number of exclusions which are particularly relevant for security. According to Article 13, the directive shall not apply to *"contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security"* (13a), nor to *"contracts for the purpose of intelligence activities"* (13b). The first exclusion is an almost literal repetition of Article 346 (1)(a) TFEU and therefore in principle redundant, since the directives applies by definition only subject to Article 346 (1)(a). The second exclusion is at the same time limited (intelligence) and generic (activities). In this context, recital 27 specifies that *"some contracts are so sensitive that it would be inappropriate to apply this Directive, despite its specificity. That is the case for procurements provided by intelligence services, or procurements for all types of intelligence activities, including counter-intelligence activities, as defined by Member states. It is also the case for other particularly sensitive purchases which require an extremely high level of confidentiality, such as, for example, certain purchases intended for border protection or combating terrorism or organized crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces."* This list of cases potentially covered by the exclusion indicates that Article 13 (a) and (b) are apparently tailor-made to security (rather than defense) concerns. The directive thus takes into account that non-military security procurements can often be even more sensitive than military procurements

and accepts that in these cases transparent procurement procedures and transnational competition may not be appropriate.

In principle, the existence of common procurement rules in the security area should lead to greater market openness for European companies. However, due to numerous exceptions and the margin of maneuver, it is doubtful that the market will become considerably more transparent and open. The situation may be different for private operators of critical infrastructures who already face competition in their own markets and may, therefore, be ready to choose the economically most advantageous security solution, no matter whether it comes from a national or non-national supplier.

Conclusions

Currently, the European Union does not have a single regulatory framework for the security market as a whole, but each of its segments has a specific regulatory framework. To a certain degree, such fragmentation is normal and inevitable, since each sector has its own specificities, which must be taken into account in the rules and regulations governing the sector (see, for example, aviation versus maritime transport). The problem in Europe, however, is that fragmentation at sector level coincides with fragmentation at the national level. In some cases, EU legislation can overcome or at least alleviate this fragmentation, but definitely not all the time, and attempts to harmonize national rules at the EU-level still faces resistance from member states who are reluctant to delegate national sovereignty to Brussels.

At the same time, the European regulatory framework for security is characterized by important gaps. According to stakeholders, the most important loopholes concern:

- The lack of a proper liability protection system for both equipment suppliers and users, which creates considerable legal uncertainty in case of equipment- or system-failure.
- The absence of standards or differences between national and sector specific standards, which tends to reduce market transparency and efficiency.
- The lack of an EU security label based on agreed validation and certification procedures.
- The lack of an EU risk assessment methodology.
- The absence of an EU Security Industrial Policy.

Such legislative gaps ultimately reduce market transparency, openness and legal clarity. Additionally, these gaps have the potential to discourage investment in technology development and innovation and create a non-competitive business environment, particularly for the security industry.

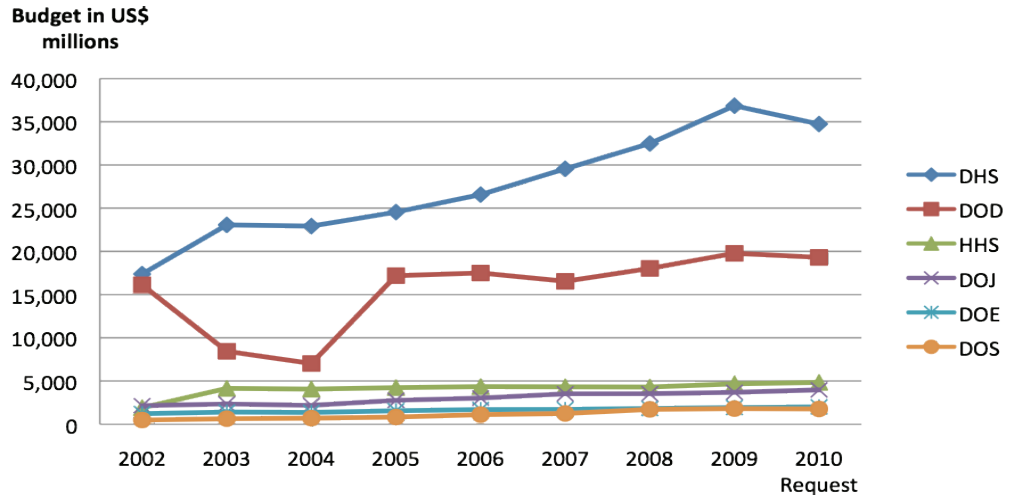
The Homeland Security Regulatory Environment in the United States

In the United States, homeland security activities are funded and undertaken by a number of federal agencies. The lead agency is the Department of Homeland Security (DHS) which was established on November 25, 2002 by combining the activities of 22 federal agencies and more than 2,000 Congressional appropriations accounts.[67] DHS today accounts for approximately 52

percent of the U.S. homeland security budget. The second largest contributor is the Department of Defense, which has accounted for roughly 29 percent of the federal homeland security budget during the period of 2002-2010.

below presents the breakdown of homeland security budget across various federal agencies for the past 9 years.

Federal Homeland Security Funding by Agency, 2002–2010



Source: Congressional Research Service (2010), Homeland Security Department: FY2010 Appropriations, p. 103.

Although regulation and funding occurs primarily at the national level, homeland security activities are also regulated and funded at the state and local levels. However, this study will focus on the activities undertaken by the Department of Homeland Security at the national level across four primary mission areas: counterterrorism; infrastructure protection; border security; and preparedness, response and recovery.

DHS-Wide Developments Affecting the Industrial Base:

Legislation passed by Congress and acquisition guidelines and regulations prescribed by DHS are the two key elements that affect the homeland security industrial base.

Legislation

In recent years, DHS has not experienced much Department-wide legislative activity.[68] However, there are three notable developments addressed below:

The Support Anti-terrorism by Fostering Effective Technologies (SAEFTY) Act of 2002 is designed to provide critical incentives for the development and deployment of qualified anti-terrorism technologies by providing liability protections for manufacturers. Its primary objective

is to minimize risk and encourage the commercialization of new technologies, services and software programs.[69]

The Procedures for Handling Protected Critical Infrastructure Information is classified as a "final rule," which came into effect on September 1, 2006. It provides a list of procedures that oversee the receipt, validation, handling and storage of critical infrastructure information (CII) voluntarily submitted to the Department and is applicable to all federal agencies, U.S. government contractors, and state and local entities with access to CII.[70]

Recently signed into law is the Department of Homeland Security Appropriations Act of 2010, which provides a gross budget authority of $51.9 billion in DHS funding for FY2010.[71]

Acquisition guidance

In efforts to enhance the acquisition and procurement processes, the Department has drafted and released several Department-wide acquisition guidance publications, notably:

The Homeland Security Acquisition Regulation (HSAR), which supplements and implements the Federal Acquisition Regulation (FAR) in the homeland security context and provides guidance for procedural uniformity for Department-wide acquisitions. It is applicable for all acquisition activities except for those within the Transportation Security Authority (TSA).

The Homeland Security Acquisition Manual (HSAM) is a supplementary document to both the FAR and the HSAR. Although non-regulatory, the HSAM also seeks to establish uniform DHS acquisition procedures for services and supplies.[72]

The Major Systems Acquisition Manual (MSAM) reflects the Department's efforts to provide guidance for the implementation of the DHS Acquisition Review Process. Designed as a tool for program managers, primary objectives include reducing the acquisition time cycle to productive time periods, using a systems engineering approach for major acquisition projects, estimating realistic total ownership costs and using flexible acquisition processes. It also seeks to align the Coast Guard major acquisition processes with Department policy and procedure.[73]

The Acquisition and Program Management Division, established in 2007, is assisted by the Cost Analysis Division in the implementation of the Acquisition Directive 102-01. The directive establishes the framework and the tools for all acquisition procedures, regulations, and statutes and is also responsible for defining the Acquisition Life Cycles Framework (ALF), the Acquisition Review Process (ARP) and the Acquisition Review Board (ARB).

Governance and oversight

DHS accountability has faced scrutiny as current acquisition policies lack the management and oversight needed to curtail rising costs and schedule delays. As the GAO report concludes, although the Department continues to develop its acquisition oversight capabilities and has begun implementation of its interim acquisition management directive, there still exist great inefficiencies across the acquisition framework. Ultimately, the Acquisition Review Board (ARB), an entity charged with providing program decision memorandums with action items to improve performance, has reviewed only 24 of the major acquisition programs in FY2008-FY2009 and many of its proposed review action items have not been implemented in a systemic and timely manner.

Although there have been significant developments in this regard, rising budgetary expenditures and insufficient staffing levels continue to render a comprehensive review of acquisition programs difficult. In FY2009 acquisition spending increased by 66 percent and reached $14.2 billion from $8.5 billion in FY2004.[74] Although a tracking system has been installed to oversee the key information regarding all acquisitions by the acquisition oversight office, the lack of a department-wide requirements oversight body ultimately affects the Department's success in meeting both current and future critical mission needs.[75]

Key Mission Areas

Counterterrorism

Dubbed the "founding purpose" of the Department, counterterrorism activities strive to prevent terrorist-driven violence on the United States by land, by sea and/or by air.

Legislation

- HSPD–4: National Strategy to Combat Weapons of Mass Destruction established in 2002 encourages the use of new technologies, strengthens intelligence collection and analysis and emphasizes the importance of strategic partnerships with alliances in order to combat and reduce the proliferation of WMD.[76]
- HSPD–11: Comprehensive Terrorist-Related Screening Procedures created in 2004 builds upon HSPD 6 and clarifies the terrorist-related screening procedures used by DHS. It calls for coordinated procedures that "detect, identify, track, and interdict people, cargo, and other entities."[77]

Infrastructure Protection

Protecting the nation's critical infrastructure and key resources (CIKR) is a core element of the DHS mission, and the Office of Infrastructure Protection (IP) is charged with this responsibility. Critical infrastructure is defined as "the physical or virtual assets, systems, and networks, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."[78] Key resources are the "publicly or privately controlled resources essential to the minimal operations of the economy and government," including agriculture and food, commercial facilities, energy, banking and finance, critical manufacturing, information technology, transportation systems and the defense industrial base.[79]

Legislation

- The Critical Infrastructure Information (CII Act) Act of 2002 defines critical infrastructure information as the "information not customarily in the public domain and related to the security of critical infrastructure or protected systems." This act seeks to increase infrastructure information sharing between the operators of CI and the government agencies charged with infrastructure protection activities.[80]
- Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization and Protection was released in 2003 for the purpose of developing a framework that "identifies, prioritizes, and protects" the CIKR from terrorist attack. It defines the roles

and responsibilities of the Secretary, Sector-Specific Agencies, state and local entities, other departments and agencies, as well as the private sector.[81]

- Homeland Security Cyber and Physical Infrastructure Protection Act, introduced in January of 2011, is still in the legislative process. If ratified, it will enhance domestic preparedness and collective response to terrorist activities by establishing an Office of Cyber-security and Communications, which will comprise a United States Computer Emergency Readiness Team and a Cyber-security Compliance Division, a division to be created by this act. Additionally, this act would call upon the Cyber-security Compliance Division to establish cyber-security requirements for civilian non-mililtary and non-intelligence community federal systems.[82]

Preparedness, Response and Recovery

Enhancing the nation's preparedness, response and recovery in the event of a natural disaster, emergency, or terrorist attack is the third core DHS mission area and one that relies most upon collaboration with the state and local levels.

Legislation

- HSPD-8 National Preparedness of 2003 and the accompanying Annex 1 is a directive designed to enhance the current "preparedness" of the U.S. government's ability to secure against and or directly respond to terrorist attacks, natural disasters and sudden emergencies. The fundamental principal of this directive defines the "all-hazards preparedness" goal which seeks to develop "readiness priorities" and couples the potential and or existing threats with the resources capable of detecting, deterring, and recovering from any national emergencies. Annex 1 provides planning guidance in accordance with the Homeland Management System in the National Strategy for Homeland Security of 2007.[83]
- The National Response Framework (NRF) of 2008, a Federal Emergency Management Agency (FEMA) initiative, replaces the previous National Response Plan. It provides the framework and guiding principles for the national response architecture and outlines the five principles of the response doctrine to better coordinate nation-wide initiatives.[84]
- The FEMA Strategic Plan for 2008-2013 is comprised of 9 core competences and 2 strategies which will build upon existing federal, state, and local preparedness capabilities and incorporate new integrated, interoperable and coordinated response assistance activities.[85]
- Disaster Recovery Improvement Act, introduced January of 2011 is still in the legislative process however, if passed seeks to amend the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Specifically, it aims to improve overall disaster relief by expediting the time needed and costs incurred of recovery projects.[86]

Border Security

Securing the nation's borders involves protecting against the illegal smuggling of people and goods. Security measures must exist at all points of entry and prepare for, protect against, and mitigate all existing and potential threats by way of land, air and sea while fostering lawful immigration for visitors and residents alike. The four primary federal agencies within the Department responsible for border security activities are: the Customs and Border Protection (CBP), Bureau of Immigrations and Customs Enforcement (ICE), the United States Coast Guard (USCG), and the Transportation Security Administration (TSA).

Legislation

Border Security

- Established in 2003, the United States Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT) conducts verification procedures on non-U.S. citizens entering the United States The U.S.-VISIT Final Rule, released in August 2004, expands to include aliens travelling with non-immigrant visas, individuals travelling under the Visa Waver Program, and to lawful permanent residents at chosen land ports of entry.[87]
- The Secure Fence Act of 2006 authorizes the funding for operational border security capabilities along U.S. land and maritime borders. Specifically, Section 102 requires the Department to construct, along an approximate 700-mile segment, security infrastructure along the Southwest border.[88]
- The REAL ID Final Rule released in 2008, acting in accordance with the REAL ID Act of 2005, establishes minimal standards for state-issued driver's licenses and identification cards to standardize state procedures and regulations.[89]
- The Emergency Border Security Supplemental Appropriations Act of 2010 allocates $600 million for emergency funding for Southwest Border operations, $394 million of which to the Department of Homeland Security.[90] This bill is, however, offset by a $100 million reduction in SBInet funding and $552 million in revenue increases, resulting in a net impact of roughly $52 million.[91]
- The Interim final rule regarding the implementation of the Electronic System for Travel Authorization (ESTA) Program released in August of 2010 amends the previous DHS regulation requiring travel fees by individuals from Visa Waver Program countries. Specifically, it confirms that travellers with approved program authorization are exempt from paying ESTA fees if only updating an ESTA application. Travellers, however, with new passports must pay the fee.[92]
- Border Security, Cooperation, and Act Now Drug War Prevention Act, introduced January of 2011, if ratified will authorize up to 500 additional U.S. Border Patrol, DEA and ATF agents along the Southwest border shared with Mexico. It will also increase the resources needed to protect the border from illegal immigration, drug trafficking and the smuggling of illegal goods by increasing the number of motor vehicles, radio communication systems and global positioning systems as well as by providing higher-quality body-armor.[93]
- Border Enforcement Security Task Force, introduced in February of 2011, if passed will enhance border security by fostering greater collaboration between the federal, state and local governments and aid in the process of information sharing. Task forces will be established in designated areas facing cross-border violence.[94]

Aviation and Transportation Security

- HSPD-11 Comprehensive Terrorist-Related Screening Procedures Directive, released in 2004, establishes wide-ranging screening procedures for cargo, people, and other entities suspected and or engaged in terrorist-related activities.
- NSPD-47/HSPD-16, released in 2006, further establish a strategic vision and comprehensive plan for increased border security at all airports and call for the establishment of a National Strategy for Aviation Security.

- Passed June 4, 2009, the Transportation Security Administration Authorization Act appropriates $7,604,561,000 for FY2010 and $8,060,835,000 for FY2011 to enhance the management and operational functioning of current transportation security.[95]
- Secure Airport Terminal Act of 2011, introduced in February of 2011, will, if ratified, increase the use of security cameras all airport screening facilities, at both areas of entry and exit. It also requires all camera's be used, maintained and tested in addition to other implemented technologies.[96]

Port and Maritime Security

- The Maritime Port Security Transportation (MSTA) Act of 2002 works to prevent loss of life, transportation infrastructure disruption or destruction, economic instability and environmental damage. It provides a strategic framework regulating maritime commerce and the security of domestic sea ports.
- NSPD 41/HSPD13, released in 2004, provide policy guidelines for the U.S. maritime domain and call for the development of a National Strategy for Maritime Security. Released in 2005, the National Strategy for Maritime Security is designed to coordinate and implement all existing Department-level strategies and procedures and security programs at the State, local, and private sector.
- Security and Accountability for Every (SAFE) Port Act of 2006 amends the Maritime Port Security Transportation Act, establishes new port facility requirements, calls for the development and implementation of the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-PAT) and amends the Homeland Security Act of 2002 to establish the Office of Cargo Security Policy.[97]
- The Coast Guard Authorization Act of 2007 authorizes the reconstruction of the Deepwater Program, and requires the Coast Guard to resume its role as the lead systems integrator and restructure the program portfolio into individual acquisition programs.[98]
- The Coast Guard Authorization Act for FY2010 and FY2011, if passed, will authorize appropriations for operation and maintenance, general administration, acquisition reform and contracting practices. Specifically, Section 401 mandates the establishment of a Chief Acquisition Officer by October 1, 2011 and Section 402 appropriates funds for the establishment of an acquisition directorate.[99]

Conclusions

Focusing on homeland security activities at the national level, this section presented the key DHS-related legislation and acquisition guidance efforts affecting the U.S. homeland security market. Interestingly, recent regulatory efforts have focused on improving the oversight and management of ongoing and future R&D and procurement programs.

EU-U.S. Comparative Analysis

The final section of this paper presents a comparative analysis of the EU and U.S. regulatory environments for security and sheds light on the strengths and weaknesses of both.

Political Structure

Functioning largely under the purview of national jurisdiction, the EU security market is highly fragmented and complex. Market fragmentation is further exacerbated by the absence of a single Directorate General (DG) in the European Commission charged with centralizing EU security initiatives.

In the United States, the Department of Homeland Security is responsible for coordinating and leading homeland security missions and generating the capabilities to do so. Through its Directives and publication of acquisition manuals and guidance, the Department is able to foster a more centralized, transparent and competitive security market than its European counterpart.

Acquisition and Procurement Directives

In Europe, the Defense Procurement Directive is the first and only piece of legislation that pertains to the defense and non-military security sector at the institutional level and establishes the basis for a European Defense Equipment Market. Nevertheless, the EU does not have of a "European Standardization Handbook for Security Procurement" nor a corresponding "Code of Conduct," for procurements not covered by the Defense Procurement Directive.[100]

The Defense Procurement Directive and Code of Conduct are similar to the Department of Homeland Security's HSAM, HSAR, and the FAR in that they establish the principles and procedures of DHS acquisition and procurement strategies at the federal level. However, unlike the United States, the EU does not have an equivalent oversight body to facilitate the harmonization of acquisition practices.

Security Strategies and Acquisition Guidance

The European Security Strategy of 2003 and the Internal Security Strategy of 2010 are important EU achievements as they aid in the development of a clear and definable industrial policy or future roadmap for the security market. Specifically, the Internal Security Strategy re-establishes common threats and obstacles, defines a European Security Model and contributes value-added, concrete objectives in a manner similar to the DHS Quadrennial Homeland Security Review, which largely inspired its framework. The above-mentioned EU security strategies also strongly resemble the DHS Strategic Plan Fiscal Years 2008-2013 which describes the Department's strategy and quantifiable goals and objectives for 2013.[101]

International Standards and Certifications

Currently, the EU lacks the legislation necessary to provide liability protection and product and service testing and evaluation of new capabilities before deployment. The United States, on the other hand, has developed the Office of Test, Evaluation and Standards and has enacted the SAFETY Act.

Regulatory Activity in Key Areas

Several areas have experienced significant legislative and regulatory activity in the United States and the EU.

Biometric and privacy protection

The United States has established a stronger regulatory framework for biometrics that has, in large part, guided the development of this capability in other countries. The U.S. Enhanced Border

Security and Visa Entry Reform Act of 2002 not only mandates the use of biometric data in U.S. visas but equally requires that foreign consulates and embassies install biometrics in all travel documents for individuals traveling to the United States.[102]

In compliance with U.S. regulation, EU Council Regulation (EC) 2252/2004 mandates the use of biometric identifiers in all passports and travel documents; however biometric finger scanning for non-EU citizens at ports of entry has not yet been established.

Legislation governing privacy protection for biometric identifiers in the EU is primarily regulated by member states who remain reluctant to store personal data in centralized databases, which has not yet been mandated by EU regulation. In the United States, privacy protection is regulated at the federal level through the Privacy Office.

Border security: aviation, maritime and port security

Developments such as the International Civil Aviation Organization (ICAO) and the European Civil Aviation Conference for aviation security and the International Ship and Port Facility Security Code (ISPS Code) for maritime security have been fundamental in bringing about global legislative harmonization. As this paper demonstrates, in the United States and EU, legislation in these fields is similar; however, U.S. standards and requirements are often more stringent than those in Europe. This is due to the more centralized U.S. structure, where border security activities are overseen at the department level and implemented by numerous components (TSA, U.S. Coast Guard, and Customs and Border Protection). Additionally, the presence of U.S. certifications and standards as well as liability protection through the SAFETY Act, have fostered a more uniform security market. The EU, however, continues to suffer from national legislative fragmentation and a lack of equipment interoperability due to the absence of uniform standards. This has largely hindered the development of harmonized procedures in the aviation and maritime domains.

Preparedness, response, and infrastructure protection

The legislative environments for infrastructure protection are also similar between the EU and the United States as both seek to identify and define their respective critical infrastructures and key resources. The fundamental difference is that critical infrastructures in the United States operate across federal, state and local levels whereas, the European Critical Infrastructures (ECIs) function transnationally.

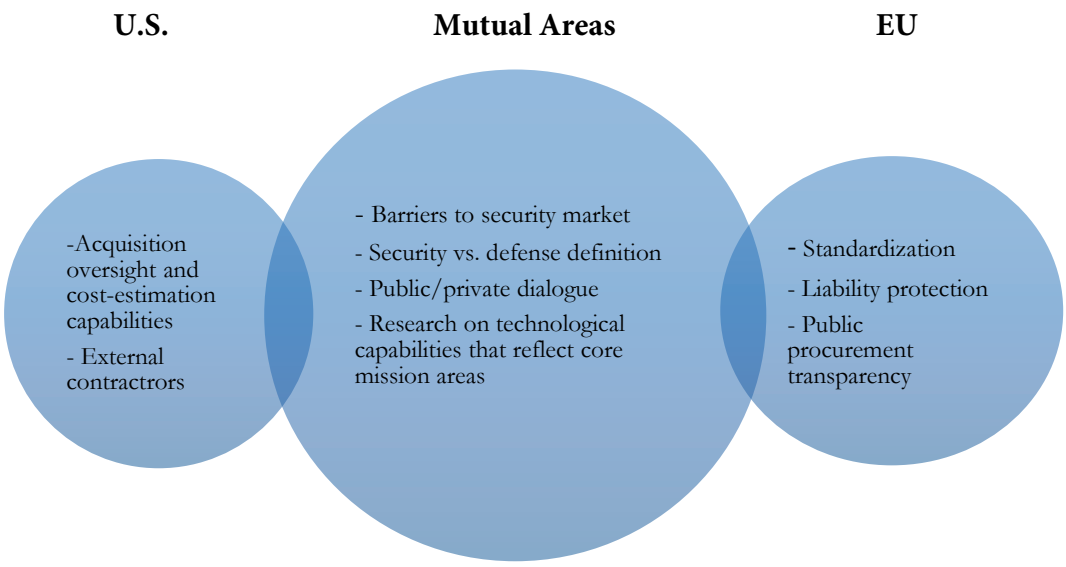
Ultimately, the EU lacks legislative force governing this domain and Council Directive 2008/114/EC is the only directive which addresses ECI protection, establishing the process by which member states must identify ECIs by January 12, 2011.[103]

Acts and initiatives related to infrastructure protection also frequently pertain to EU preparedness, response, resiliency and consequence management to terrorist attack.[104] In the United States, however, greater distinction is made between these two security areas. Preparedness, Response, and Recovery (PRR) is considered a DHS priority and one that is strongly intertwined with all of the department's activities.

Recommendations

We propose a series of recommendations designed to strengthen the regulatory frameworks for, and the functioning of, the security markets in the United States and Europe. They are not all-encompassing, yet address the identified key legislative gaps and underdeveloped areas within the security market. Figure 6 provides an overview of the recommendations broken down by regional applicability.

Individual and Mutual Areas of Insufficient Security Market Development



Source: CSIS.

European Union

The most critical issue for the EU is the reduction of market fragmentation toward a single security market and the adoption of a more homogenous regulatory framework. This endeavor will require the harmonization of security strategies and policies across all 27 member states and constitutes the driving element for all EU-related recommendations. Additionally, instituting EU-wide security standards and requirements for security-related technologies will be fundamental for harmonizing and opening the EU security market as it will provide for a level of equipment interoperability that has not yet been achieved. The EU security market would also greatly benefit from the creation of an EU equivalent to the U.S. SAFETY Act, as liability protection would increase competition, foster innovation, and expand the number of products and services available. Greater transparency at the institutional level regarding public procurement practices and procedures could further strengthen the security market. Harmonizing European procurement guidance would lower market entry barriers for companies and streamline the acquisition process. Specifically, the creation of an EU Security Procurement Directive, covering the areas not governed by the Defense Procurement Directive, would help clarify the distinction between security and defense technologies and minimize the difficulties associated with dual-

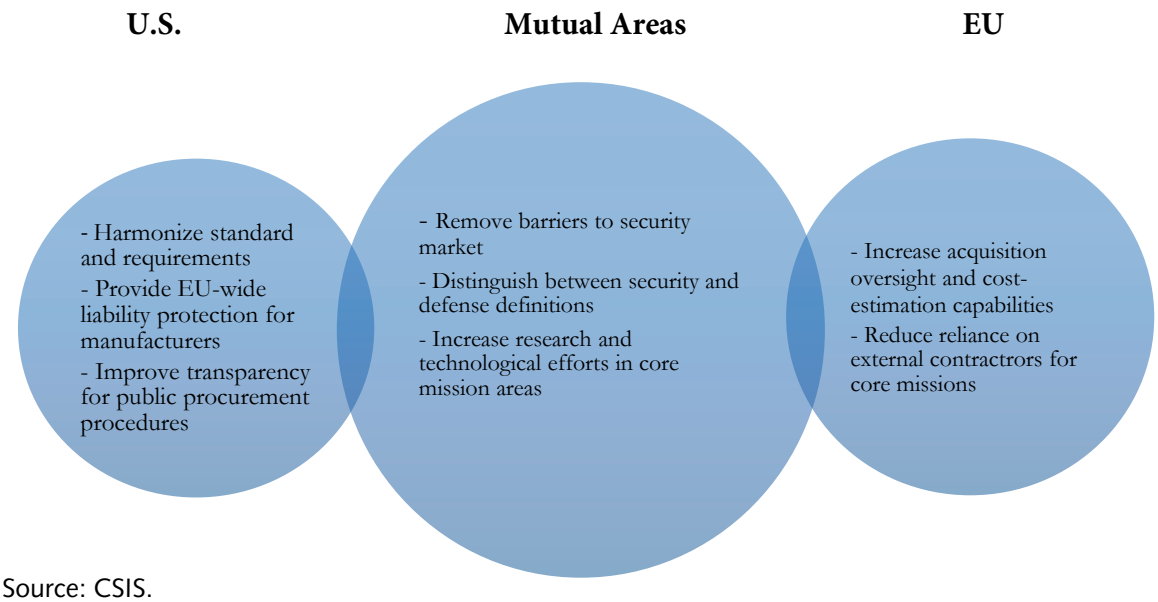
application technologies. The development of a European Handbook for Security Procurement would also standardize current security procurement practices and facilitate EU-wide expansion of the market sector in a uniform manner.[105]

United States

As this report illustrates, the DHS's unrealistic cost-estimates and program evaluations have, in recent years, led to a significant increase in expenditure and undermined the development of new security capabilities. Initiatives to enhance oversight and improve management are a good start but must be followed-up on.

Moreover, the department's reliance on outside contractors for undertaking core missions has also come under increased scrutiny, both internal and external. To address this issue, DHS is reducing the number of external contractors and increasing internal capabilities (an approximate 27 percent or nearly $1 billion decrease in budgetary spending on professional service contracts by August 2010). Insourcing, however, will only prove to be more cost-efficient if DHS develops and maintains a framework that can effectively oversee and manage the activities and collaboration of a larger workforce. The recently drafted DHS Workforce Strategy for Fiscal Years 2011-2016, if properly implemented, will be instrumental in this process.[106]

CSIS Recommendations for the Security Market



Source: CSIS.

TRANSATLANTIC INDUSTRIAL POLICIES IN THE SECURITY SECTOR

Valerio Briani, *Researcher, IAI,*
and Nicolò Sartori, *Junior Researcher, IAI*

Introduction

This paper assumes that after the end of the Cold War, and even more after the 9/11 terrorist attacks, the attention of Western governments, companies and societies has increasingly shifted from the defense to the security sector. The aim of this paper is not to verify such assumption but, rather, to investigate how this interest in security is translated concretely into EU and U.S. industrial policies and what consequences this shift may have on transatlantic industrial relations.

In order to reach this goal we

- assess the characteristics of the U.S. and European defense and security sectors, in terms of market dynamics and industrial structure. This will give us a starting point to understand the evolution of the security sector and judge whether the defense sector is being chosen as a model for development;
- identify which initiatives have been taken in order to influence developments within the security sector and investigate to what extent these initiative may have on the establishment of a security industrial policy in the EU and the United States;
- assess the potential impact of these policies on the future of the transatlantic relations, and suggest some ideas in order to foster what we do believe is the best evolution of the security industrial base, seen in the framework of transatlantic industrial relations;

The Defense and Security Sectors: Characteristics and Developments in the United States and in the EU.

In this paragraph we will briefly expose the main characters of the defense and security markets and industries, as they were at the end of the Cold War (and largely still are). In our view, the two sectors can be seen at the opposite end of an imaginary continuum in terms of market structure; a monopsonistic and almost monopolistic market with high entry barriers and high technological level on one side (defense), and a fragmented, more low-tech and unregulated sector on the other side (security). Clarifying the main features of these two poles will give us a reference points to evaluate, in the following paragraph, if and how the post 9/11 security market is evolving and what role the EU and the U.S. governments are playing.

The Economics of Defense Industry

The defense industry has historically been a sector in which the highest national security interests overlap and intertwine with political and economic interests. On both sides of the Atlantic, the Defense Industrial Base (DIB) is largely considered both an economic and a strategic asset. According to generally accepted definitions, the DIB is composed of a public and private industrial complex with capabilities to perform research and development (R&D), design, produce, deliver and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Several academic studies have been carried out to investigate the economic functioning of the defense industrial sector, and its main characteristics can be summarized as follows:

- Monopsony structure on the demand-side
- Monopoly/oligopoly structures on the supply-side
- High R&D intensity and long-term production cycles
- Decreasing production costs
- Public subsidies in the R&D phase
- Associated spin-offs

Defense markets are imperfect. On the demand-side, governments maintain a relevant monopsony position as the sole buyer, at least in the most significant segments of the market. Small arms and, in the United States, some kind of armored vehicles are also available to private citizens or companies, but the size of these markets pale in comparison to that of governmental expenses. This allows states to maintain close control over the dynamics of their domestic defense markets.

Monopolies, duopolies or, at least, oligopolies characterize the structure of the supply-side, in which large integrated firms operate as exclusive prime contractors in a sector with high barriers of entry for newcomers. Production trends in the sector are basically affected by quantity and output. High R&D fixed costs are progressively rising in real terms, following the continuous technological evolution which characterizes the defense sector. Large-scale production allows economies of scale and learning, favoring decreasing unit costs.

Relevant technological spin-offs, the civilian/commercial application of a product or a technology originally developed for defense missions, affects the companies' industrial organization. In order to exploit the huge amount of technological spin-offs between the defense and civilian sectors, multi-product firms increasingly replace single-product specialists. This is the case, for instance, of the civil-military aerospace and defense firms, which rely upon massive civil profits to remain in the defense market.

All these elements result in highly concentrated industrial segments dominated by small numbers of large integrated firms. High fixed costs for research, high levels of technological know-how, advantages deriving from economies of scale and learning as well as integrated organizational practices. All provide effective barriers of entry and exit as well as limit industrial competition and create markets dominated by a handful of well-established giant firms.

Defense is a strategic issue for the large majority of the world's countries, and for this reason political factors and security concerns dominate the sector's management and evolution. The role

of the state remains paramount in shaping the nature of the defense market, particularly with regard to competition and international openness.

Like market dynamics, government choices also play a large role in shaping the defense market. Governments' planning powers, procurement spending and normative authority have relevant capacities to determine the size and the structure of their DIBs as well to control the evolution of the defense industrial sector. Tightly supervising the defense industry's activities; control by public authorities assures some strategic benefits:

- the independence and security of supply (re-supply) in equipment procurement;
- the development of specific equipment responding to national Armed Forces' requirements and needs;
- deeper information and control on products characteristics;
- bargaining powers when considering foreign acquisitions;
- surpluses for the balance of payments deriving from exports earning and imports savings;
- socioeconomic externalities such as
  - creation of high-wage jobs;
  - technology spin-offs and benefits.

During the Cold War period, governments, through ministries of defense, managed military products, setting needs and requirements; supported R&D for new weapon systems; negotiated contracts with suppliers; oversaw and evaluated program developments; set accounting and security restrictions on private companies. Defense business were kept under controld in order to protect national security and keep the technological base ahead of that of potential enemies as well as to retain some national autonomy for the defense industrial base. In these circumstances, the defense industries were, in essence, a manifestation of national sovereignty, and despite some degrees of military and political integration deriving from the participation of NATO or the EU, Western governments jealously defended their political control over the defense industry's management.

Protected by national governments, the defense business evolved largely isolated from commercial pressures and dynamics while, in some European cases (France, Italy), the state directly assumed full control over the defense industry. Governments often sacrificed the economic and commercial efficiency of their defense businesses and provided subsidies to the defense industry in order to correct certain types of "market failure," supporting company's high costs of entry in new strategic markets, maintaining R&D levels required to guarantee desired industrial output and preserving positive externalities such as jobs, technologies and spin-offs. Conversely, issues of market efficiency and value-for money were often put aside. The focus of defense industrial policies was mainly on obtaining the most advanced weaponry regardless of the costs.

With the end of the Cold War, new trends and drivers began to shape the industrial dynamics of the defense sector, and Western countries had to cope with new challenges and situations. These new elements, characterizing both the political and industrial environment, can be summarized as follows:

- decline in defense budgets and military expenditure;

- increased interoperability/communality requirements;
- privatization of services that once were provided by the military;
- technological evolution and growth of R&D costs;
- globalization and transnationalization of production and supply chains;
- openness of the research sector.

In order to deal with both budget reductions and increasing R&D costs driven by technological evolution, companies were required to ensure more commercial discipline and efficiency when procuring armaments. Therefore, as in both the United States and in Europe there was massive overcapacity, companies, backed by national governments, started responding to the new situation by restructuring and consolidating their assets.[107] Rapid, wide-ranging consolidation of the global defense industry in the past decade has left only five big defense and aerospace prime contractors in the United States and just four giant firms in Europe.[108] Together with some efforts toward restructuring and consolidating, the shrinking defense budgets increased the attraction of joint programs[109] and, therefore, the participation of overseas companies in the U.S. defense industrial base.[110] The collapse of the Soviet Union also meant that the countries previously included in the Soviet sphere of influence entered the marketplace. Companies started looking abroad for new potential customers in the attempt to globally spread their high fix costs, while taking advantage of economies of scale. The processes of globalization and transnationalization of markets and supply chains in part favored such developments, though in the defense sector political pressures and corporate reticence pushed for maintaining national control over a large part of the defense industrial assets.

At the end of the 1990s, many decision-makers and scholars started believing that these drivers would have fostered deeper industrial relations between Europe and the United States,[111] and that a competitive transatlantic defense market would have strengthened political relations within NATO as well as enhanced military interoperability, improved the quality of products and reduced the cost of equipment procurement.[112] In reality, transatlantic defense business remains today largely fragmented, with market closures and protectionist behaviors, which often constrain competitive industrial practices. Industrial tie-ups such as mergers, acquisitions or teaming arrangements that would enhance cooperation between Americans and Europeans actors are, therefore, hindered by the enduring protectionist attitudes of many national military-industrial complexes. This is further aggravated by their reluctance to open their defense markets to transatlantic allies, as well as by Europe's chronic industrial fragmentation and national divisions. Finally, the desire to maintain strategic independence through a national defense base has not faded away in the United States or in Europe.

In addition to political and regulatory limits, economic and commercial challenges also contribute to a delayed and effective opening of the two markets.[113] The existing technology gap between the United States and Europe is probably the most serious of these challenges. The global military economy has transformed over the last two decades, largely the result of technological developments that have reinforced the dominance of the United States over the transatlantic industrial sector. Differences in R&D resources and technological capabilities generate a lack of general balance between the two industrial systems, rendering attempts to promote market openness between the two sides of the Atlantic very difficult.

The Economics of Security Industry

During the Cold war, the security sector was much closer to any other market than to the defense sector. Moving from the analysis of the economic characteristics of the defense industry, we can assess that the security sector presents the following elements:[114]

- market structures extremely fragmented;
- short/mid-range product life cycles,
- mostly private R&D funding;
- low and mainly production costs;
- associated spin-offs.

The security market's structure presents a much more competitive environment when compared to the defense sector. On the demand-side, public authorities (not-exclusively military) remain the most important security customer, but it is questionable whether this assertion holds true (that is, whether public authorities represent more than half of the market). Security customers are highly diversified among both public institutions, central and local and private entities. These can be either large customers such as infrastructure operators (airport and port companies, rail operators, energy providers, telecommunications firms) or smaller, less demanding actors (companies, private citizens). Customer needs are, therefore, much more diverse and can be satisfied by a wide-range of products, from the more technologically intensive (for example access control technologies) to the most basic products (closed circuit televisions for domestic security).

Fragmentation of the demand, and, therefore, of customer needs, implies a very diverse range of suppliers. The supply-side is thus characterized by the coexistence of several firms, differing from one another in terms of dimension, organization, specialization and revenues. Some IT and defense giants operate in some segments of the sector (mainly systems of systems), along with many specialized security firms and SMEs with disparate specializations. Due to the heterogeneity and fragmentation of the demand, entry barriers on the supply-side are very limited to the low-end security sector, while higher-end segments require more technologically intensive R&D. In the systems of systems segment barriers to entry may be as high as in the defense sector; since very few firms possess the necessary systems integration capability this is, in fact the segment in which defense companies show the most interest.[115] Such fragmentation makes it harder for any actor on the demand-side to assume a leading position and exercise control over the industrial dynamics of the security sector through the sheer weight of its procurement.

Production trends in the sector are not heavily affected by quantity and output. R&D fixed costs may also be important in the security sector, especially in the higher segments, but their weight on company's industrial planning is sensibly lower. In the *systems of systems* segment, which is the more technologically intensive, R&D costs may also be lower than expected as these products are often the result of a successful integration of already existing products (or, products for which R&D has already been paid, often derived from defense research). Indeed, competition and low-tech requirements force firms to adapt and respond rapidly to the free market's short-term changes: emphasis is put on time and costs, rather than on performances and reliability.

Given these circumstances, government (both central and local) and private customers, do not have strong incentives, neither economic nor political, to maintain close supervision over the

security industry's activities. Issues considered fundamental in the defense sector, such as the independence and security of supply, are less relevant when considering the security domain.

Therefore, the security industrial base is generally organized and operates according to economic factors rather than political and strategic ones. Although the security industry certainly has a strategic value, providing public authorities and private operators with equipment and technologies necessary to cope with some of the most demanding challenges for the new century, political concerns do not have a key role in shaping the sector's features. Multinational companies (in particular in the ICT sector with companies like IBM and Cisco) as well as some niche firms specialized in sectors such as biometrics, tracking, detection, sensors exploited such market fluidity to develop their businesses on the two shores of the Atlantic. For instance, a large number of Automatic Identification Systems (AIS) and Long-range identification and tracking (LRTI) producers, both American and European, operate competitively in the maritime security sector.[116] Competitive dynamics dropped the company-level market shares, making it difficult to identify any dominant company really leading the market.[117] Also in the detection segment, despite the fact that the majority of the firms are based in the United States, some European players operate and make huge profits in the transatlantic market.[118] Smiths Detection, UK leading producer of various types of detection equipment is probably the most prominent example with 31 percent of the global market share.[119]

Security Industrial Policies in the EU and the United States

The evolution of the global security scenario, and in particular, the threats and challenges that we have to confront, is leading to an evolution of the market structures outlined in the previous paragraph. The security sector, in particular, is bound to undergo a deeper transformation, as its structure is, by far, less articulate and less institutionalized in comparison to the defense one. The evolution of the security market and of the security industrial base will be heavily influenced not only by external market forces, but by political choices of U.S. and EU governments in their double capacity as market regulators and potential procurement agents.

In this section we will try to outline the contour of such intervention by describing the EU and U.S. informal industrial security policies. "Informal" refers to the fact that neither the United States nor the EU currently have a formalized policy document which outlines objectives and tools to steer the direction of the security industrial output and structure. However, governments on both sides of the Atlantic sought after a large number of interventions, which are tantamount to an industrial policy, albeit a potentially incoherent one. In fact, the European Commission is starting to elaborate a formal security industrial policy, which makes the evaluation of the initiatives taken so far all the more urgent. Having identified the main trends in government's intervention in the sector will allow us to question its impact on the transatlantic relationship.

The concept of "industrial policy" is multidimensional. Some authorsstress the fact that an industrial policy refers to a specific industrial area, the development of which is believed to bring benefit to the economy as a whole.[120] From this point of view, the development of a specific industrial sector is undertaken in order to maximize the economic health of a country, not merely to increase the productivity of firms operating in the sector. An increase in quality and quantity of industrial output is also a pursued objective, but it is a subsidiary one. The choice of the sector for an industrial policy should, therefore, fall only on the industrial sector which has a potential to produce a cascade effect on the economy. Others stress the role of an industrial policy in the

transformation of the industrial structure in a desired direction (i.e. favoring the development of large companies, or maintaining a certain level of competition between producers). This conception is more apt to be applied in sectors which possess a significant strategic relevance for the state.[121]

It should be underlined that any concept of industrial policy implies some degree of skepticism in the functioning of free-market dynamics. If the "invisible hand" is considered sufficient to develop an industrial sector to its fullest potential, there should be no need for governmental intervention. It is tempting to assume that traditional U.S. and European views of free-market dynamics have influenced the way governance of the security sector is being addressed. Overall, we can assume that EU countries, given the influence of social-democratic and catholic political doctrines, are traditionally more open to the acceptance of governmental intervention in the economy; while the more traditionally liberal United States (in the economic sense of the word) has a stronger free-market leaning, and is, therefore, more suspicious of anything resembling governmental interference in the economy. Our analysis seem to suggest, in fact, that most U.S. initiatives in the security sector are merely geared toward obtaining better homeland security management, with very few regards to the development of the security industrial sector. EU initiatives, on the contrary, has been directed at influencing and shaping the market itself, as a prerequisite for enhanced societal security as well as for a cascade effect on the European economy.

The first, and main, U.S. initiative has been the forming of the Department of Homeland Security (DHS) in 2002. This was done in order to centralize and coordinate the various homeland security activities performed by some 22 federal agencies, thereby enhancing the governance of the homeland security activities. The Department of Homeland Security, being a procurement agency, doted itself on unified regulations for the procurement of products and services. From the market point of view, the creation of the DHS had a twofold effect. As highlighted by the CSIS-IAI paper, "The Regulatory and Acquisition Environment for Security in the EU and United States," it acted as an aggregator of demand: the DHS now accounts for approximately 50 percent of the U.S. federal homeland security budget. If we consider that the DoD accounts for another 27.5 percent of homeland security funds, we can say that the creation of DHS has led to a considerable reduction in the fragmentation of the U.S. public market. This, in turn, favored the entry of large defense companies into the security market, as these already possessed a long record of government-related procurement.

Another initiative which could have a significant impact on the U.S. security industrial base is the Export Control Reform Initiative.[122] Announced in August 2009, it aims to establish new criteria for determining what items need to be controlled, based on a three-tier construct and an interagency set of policies. However, the reform is still developing and it is too early to assess which kind of impact it could have.

European authorities, on the contrary, have been, from the outset, extremely interested in the potential benefits associated with the development of an industrial security sector. Between 2004 and 2010 EU authorities, institutions and various private and public stakeholders engaged in a very lively public debate on the security market in general and also on the possible development of a security industrial policy.

The first step was taken with the institution of the Group of Personalities (GoP) in 2004. The GoP, composed of a large number of prominent public and private security stakeholders, was tasked with developing a strategy to enhance European security research. The report produced by

the GoP[123] fell short of asking for a whole industrial policy in the field of security (which was not, after all, its goal) and focused quite strictly on European research needs, proposing the creation of an European Security Research Program and of a Research Advisory Board to prepare its agenda. However, the GoP report struck some chords, which would be accepted as the basis for the European discourse on security industrial policy: the need to overcome market fragmentation, the need for more coherent requirements and the need to fully exploit the synergies between security and defense technologies and goods.

The European Security Research Advisory Board (ESRAB) proposed by the GoP published its final report in 2006. The report, "Meeting the challenge: the European security agenda," also contained hints regarding issues which were, according to the authors, beyond the original ESRAB mandate, but which were considered too vital to be overlooked. ESRAB proposed a Strategic Security Agenda, which would act as a framework for all activities directed at increasing European security, including research, policies, legislation and standardization as well as a European Security Board with the aim of advising on the content of a Strategic Security Agenda. This request amounts to a call for an advisory body for a security industrial policy.

The call was effectively answered with the establishment of the European Security Research and Innovation Forum (ESRIF), whose final report strongly argued for the formulation of an industrial policy able to overcome the perceived main weakness of the security market, fragmentation. It called for legislative and regulatory guidelines to level the field and encourage private companies to enter the sector. The ESRIF report also underlined the importance of a predictable level of demand as a prerequisite for the development of the security sector. Finally, the ESRIF report strongly highlighted the large number of commonalities between the security and defense sectors, and endorsed the exploitations of synergies between security and defense solutions.

The debate has not been lost on the European Commission, which proceeded to increase its work on the establishment of a security industrial policy. The EC responded to ESRIF suggestions with a Communication, which fully endorsed the need for an ambitious industrial policy in the security sector.[124] This communication singled out two main objectives for an industrial policy: to overcome market fragmentation and to strengthen the industrial base. The first objective would require tackling issues such as the lack of a certification, validation and standardization, the lack of a harmonized European regulatory framework and lack of technical and organizational interoperability. Strengthening the industrial base would in turn require a mapping out of the current security industrial base, enhancing European innovation policy and synergies between security and defense policies as well as promoting the "security by design" concept.

The Directorate General for Enterprise and industry is, thus, currently working to develop a general definition of the sector and to understand the perimeter of industry by commissioning research projects, within the 7FP framework.[125] This will provide understanding as to what are the most innovative security sectors to be brought into the Lead Market Initiative as well as understanding on how to enhance synergies between security and defence R&D activities.

The Commission also recognized the security sector as one of the most important industrial areas to develop within the framework of a more comprehensive European industrial policy. The Commission's Communication on an Integrated Industrial Policy for the Globalization era[126] singles out the security industry as one of the sectors which deserve specific initiatives, along with the space sector, transports and energy intensive industrial fields. In its Communication the EC recognizes the current limitations of the security market: its fragmentation (both from the

demand and the supply-sides), the heterogeneity of national regulatory environments and the diversification of the different categories of security products. It also lays out the main areas, which will be the object of communitarian intervention: a fast track system for the approval of priority technologies, further progress on standardization and harmonization and more research on security technologies. The document also hints at the possibility of coordinated security procurement, probably between states. These ideas will be further developed in a Security Industry Initiative and through the setting up of a European Security and Dual-use Platform.

In September of 2010, the European Commissioner for Industry and Entrepreneurship Antonio Tajani expressed his intention to present a paper calling for an industrial policy for the security sector.[127] The paper, to be published by the second half of 2011, should focus on the areas of innovation, standardization and certification, pre-commercial procurement and dual-use synergies with defense R&D. This latest development should represent the final step of the elaboration phase of a European security industrial policy and signal the beginning of a new and more concrete phase.

What Future for the Transatlantic Security Sector?

The evolution of the security sector has been much different from that of the defense sector. During the whole Cold War period and beyond, defense has always been considered a strategic sector with regard to both national security and economy. This led to a tendency of protectionism and strict control from national authorities as a means to orient industrial output in the desired direction and deny products and technologies to foreign states when deemed necessary. The end of the bipolar confrontation is forcing both governments and industry to recalibrate their relationship, by stressing, more forcefully, the issues of efficiency and competition. In the EU, this effort has also translated into a movement toward a common European defense market.

The security sector may be experiencing exactly the opposite development. During the Cold War, the security sector's political significance was closer to that of any other industrial sector; at the very least, security was not considered as much as a strategic field as defense. Consequently, its governance was mostly left to free market dynamics. The emergence of new threats during the 1990s, and even more after 9/11, forced governments to reevaluate the handling of the security market. Security systems instantly gained a strategic significance they never had even in the most dangerous times (for example, during the heights of international terrorism of the Palestinian Black September).

It is difficult to evaluate the consequence of such a shift in the handling of the security sector. The EU and the United States responded to this new challenge with quite different approaches. First of all, both aimed at tackling the fragmentation of the security market. This goal has been more easily attainable in the United States, for the obvious reason that the U.S. government already represents a single procurement agent, compared to the 27 national agencies in the EU. Therefore, all it took was the centralization of all procurement lines into the two departments of Homeland Security and Defense. On the European side, reducing fragmentation is bound to take a variety of different measures. The centralization of procurement would be the most effective but also the most politically delicate in a short-term perspective. A common measure both the EU and the United States are taking is to improve their respective regulatory environments, in order to provide a more even playing field for companies to compete. Another common endeavor,

however, more effective in the EU than the United States, has been the attempt to establish better communication between demand and supply.

All these initiatives are steps in the right direction and should have positive effect on the functioning of the security market, as they tackle serious efficiency issues well-known by the business community. They also are shaping, or attempting to shape, the security market in a way similar to the defense sector; more centralized demand, close demand-supply relation, R&D costs incurred by the public sector and strict regulations. It would be very useful, therefore, to remind a couple of lessons learned from the development of the defense market. First of all, too much fragmentation is bound to limit the maturation of an industrial sector, but too much centralization could lead to inefficient monopolies in certain niche and specialized areas, with the consequent loss of competition. The efforts to reduce fragmentation should be carefully weighted in order to avoid excessive regulations and constraints. Also, a reasonably fragmented security market is an opportunity for small and medium enterprises, more suited to deal with small customers such as local police, etc. Secondly, a transatlantic dispute over security standards should be avoided at all costs. European stakeholders should take this into account, and engage their American counterparts in order to produce commonly accepted standards without prejudice to either industrial base. Third, the range of security issues the EU and the United States face is almost the same. All efforts should be made to link the EU and U.S. security markets, and all attempts to create excessively restrictive export control regulations should be avoided. In this regard, the current U.S. efforts to relax its export regulations should be sustained where possible. Furthermore, any initiative which could potentially bind the two markets together should be considered. The recent EU/U.S. agreement on cooperation in the field of security research is a step in the right direction and could be expanded.[128] For example, the United States could be engaged as a partner in the EU security research programs, similar to the model of the partnership already established with Israel. However, the partnership should be based on the concept of reciprocity, as it would not be in the interest of the European Union to provide R&D funding for U.S. companies in the absence of any similar policy on the other-side of the Atlantic.

Notes

[1] Except if we consider the Galileo program (space based navigation system funded by the EC), or part of it, as a security system.
[2] *ESRAB report: Meeting the challenge, the European Security Research Agenda*.
[3] Moreover, other resources within the 7FP are allocated to the JRC (1750M€ for non-nuclear research), but a relatively small and imprecise part is related to security. The EC allocated also about 745M€ for 7 years to the framework program "Security and safeguarding liberties."
[4]FRONTEX Intellops and Blueprint project. EDA BIO-EDEP project, MIDCAS, SDR project. EUROPOL has established an operational agreement with the U.S. for exchange of personal data on specific kind of crimes.
[5] COM(2009)691 final, p. 4.
[6] Ecorys Research and Consulting, *Study on the Competitiveness of the EU security industry,* Within the Framework Contract for Sectoral Competitiveness Studies–ENTR/06/054, Final Report, Client: Directorate-General Enterprise & Industry, Brussels, 15 November 2009, p. 30.
[7] Congressional Budget Office.
[8] CIVITAS, *The Homeland Security Market essential dynamics and trends* (2006).
[9] http://www.dhs.gov/files/grants/gc_1247254578009.shtm.
[10] *Homeland Security, FY 2011 budget in brief*, p. 136.

[11] See FY *2011 Budget in brief, Homeland Security department*. Details on the budget for each area and related technologies are available at the following internet page: http://www.dhs.gov/ynews/releases/pr_1265049379725.shtm.
[12] CIVITAS report, op. cit.
[13] Homeland defense is defined at the armed forces assets dedicated to the terror protection of the Homeland.
[14] Interviews conducted by the authors.
[15] CIVITAS Report, op.cit., and the *"Global Homeland Security 2009-2019"* report, published by the HSRC in June 2009.
[16] Ecorys Report, op. cit.
[17] *European Security Directory 2009*, ESD Partners, p.16.
[18] Ecorys, op.cit., p.12.
[19] *European Security Directory 2009*, op.cit., p. 36.
[20] Civitas Group, Homeland Security Research Corporation (HSRC), Jane's Information Group, Security Industry Association (SIA), National Defense Industrial Association (NDIA) market reports and economic study.
[21] "American market sparks European influx," *HS Today*, 31 July 2008.
[22] Since May 2005, and the merger between Snecma and Sagem, the new Safran group is organized in 3 branches of activities: Aerospace propulsion, Aircraft equipment, and Defence Security.
[23] In November 2009, Sagem Sécurité announced the launching of a new U.S.-based company called MorphoTrak, which will offer a host of biometric and identity solutions to the federal, state and commercial markets. The new company is a combination of its Sagem Morpho subsidiary and Printrak. Furthermore, in May 2010, the Safran group has decided to consolidate all security businesses within the group under a single name, "Morpho."
[24] The group is a member of several U.S. teams selected by the federal administration, e.g. Lockheed Martin Team in charge of the FBI's next generation identification system.
[25] "New facial, gait recognition software to be integrated in CCTVs," *HS Newswire*, 25 February 2009.
[26] Ecorys Report.
[27] Of course most initiatives remain on the national level. For reasons of space constraints, however, we will not delve on national cases in this particular study but concentrate on the supranational EU level as such.
[28] http://www.generaldynamics.com/ (Accessed 10 Nov. 2010).
[29] http://www.asd-europe.org/site/index.php?id=2 (Accessed 10 nov. 2010)
[30] http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122 (Accessed 22 Nov. 2010).
[31] http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122 (Accessed 22 Nov. 2010).
[32] http://www.sipri.org/research/armaments/production/Top100 (Accessed 6 Dec. 2010).
[33] See http://www.src09.se/upload/External%20Documents/gop_en.pdf, pp. 4-5 for complete list of the participants.
[34] COM(2004)590 final), *Security Research: The next Steps*, available online at: http://cordis.europa.eu/documents/documentlibrary/69322111EN6.pdf.
See also European Commission, IP/04/1090: *EU blueprint for Security Research programme*, 9 September 2004, available online at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/04/1090&format=HTML&aged=0&language=EN&guiLanguage=en.
[35] Call for proposals 2004: ftp://ftp.cordis.europa.eu/pub/security/docs/sec_04_45_en.pdf; call for proposals 2005: ftp://ftp.cordis.europa.eu/pub/security/docs/pow_2005_en.pdf; call for proposals 2006: ftp://ftp.cordis.europa.eu/pub/security/docs/en_pow_13022006_final.pdf.
[36] *Meeting the Challenge: the European Security Research Agenda*. A report from the European Security Advisory Board. p.15. (http://www.src09.se/upload/External%20Documents/esrab_report_en.pdf).
[37] European Security Research Advisory Board, *Meeting the challenge: the European Security Research Agenda*, September 2006, available online at: http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf.
[38] For a complete list of these members, see www.esrif.eu/documents/members_22012009.xls
[39] http://www.esrif.eu.
[40] For more information see: European Commission, CORDIS – About Security Research website: http://cordis.europa.eu/fp7/security/about-security_en.html; European Commission, DG Enterprise and Industry – Security Research and Development website: http://ec.europa.eu/enterprise/policies/security/research/index_en.htm.

See also http://www.eurunion.org/eu/index.php?option=com_content&task=view&id=303&Itemid=58.
[41] European Commission – Joint Research Center's website:
http://ec.europa.eu/dgs/jrc/index.cfm?id=2350&lang=en.
[42] Didier Bigo, Julien Jeandesboz, *The EU and the European security industry questioning the 'public-private dialogue*, INEX Policy Brief no. 5/February 2010.
[43] Report available online at http://www.eos-eu.com/LinkClick.aspx?fileticket=7nRk3CbrwkM=&tabid=239.
[44] Interview with security industry representative, Stockholm 2 June 2010.
[45] See ASD website: http://www.asd-europe.org/site/index.php?id=4.
[46] *ASD Key Priority 4: A Harmonised European Security Environment*, available online at: http://www.asd-europe.org/site/fileadmin/user_upload/ASD_KP_4-Security.pdf.
[47] Bullock, James, A. et al. (2006) Introduction to Homeland Security, Butterworth-Heinemann Homeland Security Series. p. 459.
[48] See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm.
[49] See http://www.aaas.org/spp/rd/dhs09s.pdf.
[50] See http://www.aaas.org/spp/rd/09pch11.htm.
[51] *USA Today*, "Homeland Security generates multibillion dollar business," 9 October 2006.
[52] See http://www.cfr.org/publication/14827/homeland_security_technologies.html.
[53] Available online at http://www.hstoday.us/component/option,com_sobi2/catid,225/Itemid,325/
[54] See http://projects.washingtonpost.com/top-secret-america/companies/.
[55] "Synergy in Security: National Security Complex," *Dollars and Sense* magazine, March/April 2010.
[56] "Investors favor homeland security firms," *HS Today*, 22 October 2009.
[57] "Homeland Security Industry Shows Impressive Growth," *Frost & Sullivan*, Feb. 4, 2010.
[58] Council of the European Union, *A Secure Europe in a Better World. European Security Strategy*, Brussels, 2003. Available at http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.
[59] "Towards a European Security model," 23 Feb 2010, EU Council.
[60] "The EU Counter-Terrorism Policy: main achievements and future challenges," Communication from the Commission, COM (2010) 386 final, 20.7.2010.
[61] Communication from the Commission to the Council and the European Parliament: Critical infrastructure protection in the fight against terrorism [COM (2004)702 final - Not published in the Official Journal].
[62] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (OJ L 355, 30.12.2002.
[63] The most important implementation acts are Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security (OJ L 89, 5.4.2003) replaced by Regulation (EC) No 820/2008, laying down measures for the implementation of the common basic standards on aviation security of 8.8.2008 (OJ L 221, 19.8.2008).
[64] Equipment shall be capable of detection small items of different metals, with a higher sensitivity for ferrous metals in all foreseeable conditions.
[65] Equipment shall provide for the necessary detection, measured in terms of resolution, penetration and discrimination, to ensure that prohibited articles are not carried on board aircraft.
[66] See DefSec report, pp. 183-186.
[67] See http://www.dhs.gov/xlibrary/assets/brief_documentary_history_of_dhs_2001_2008.pdf (4/35).
[68] Key DOD acquisition related legislation in recent years includes the Weapons System Acquisition Reform (WSARA) Act of 2009 and the Implementing Management for Performance and Related Reforms to Obtain Value in Every (IMPROVE) Acquisition Act of 2010.
[69] See https://www.safetyact.gov/jsp/homepages/displayHomeAbout.do.
[70] See http://www.dhs.gov/files/laws/gc_1158333877680.shtm.
[71] The FY 2011 Presidential budget is $56.3 billion. http://www.fas.org/sgp/crs/homesec/R40642.pdf.
[72] See http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsam.pdf.
[73] See http://www.uscg.mil/acquisition/newsroom/pdf/msam.pdf (10/468).
[74] See http://homeland.house.gov/press/index.asp?ID=565&SubSection=2&Issue=0&DocumentType=0&PublishDate=0.
[75] See http://hsc-democrats.house.gov/SiteDocuments/d10588SP.pdf (10/92).
[76] See https://www.hsdl.org/?view&doc=2805&coll=limited.
[77] See http://www.dhs.gov/xabout/laws/gc_1217614237097.shtm.
[78] See http://www.fas.org/irp/offdocs/nspd/hspd-7.html: Section 1016(e) of the USA PATRIOT Act of 2001– (131/132).

[79] See http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf: Section 2(9) of the Homeland Security Act of 2002 (7/187).
[80] See http://www.dhs.gov/xlibrary/assets/CII_Act.pdf (7/11).
[81] See http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#0.
[82] See http://www.opencongress.org/bill/112-h174/show.
[83] See http://www.fas.org/irp/offdocs/nspd/hspd-8.html.
[84] See http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf (4/4).
[85] *FEMA Strategic Plan Fiscal Years 2008-2013*. FEMA P-422, Jan. 2008 (pdf) (11/64).
[86] See http://www.govtrack.us/congress/billtext.xpd?bill=h112-57.
[87] See http://www.dhs.gov/files/laws/gc_1229618480915.shtm.
[88] See http://npl.ly.gov.tw/pdf/5480.pdf.
[89] See http://www.dhs.gov/files/laws/gc_1172765386179.shtm.
[90] Office of the Press Secretary. Statement by the President on the Passage of the Southwest Border Security Bill. August 12, 2010.
[91] The SBInet, as of January 2011, has since been cancelled ; http://www.gop.gov/bill/111/2/hr6080.
[92] See http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/08062010_2.xml.
[93] See http://www.govtrack.us/congress/bill.xpd?bill=h112-77.
[94] See http://www.govtrack.us/congress/bill.xpd?bill=h112-770.
[95] See http://homeland.house.gov/SiteDocuments/20090514101342-31125.pdf.
[96] See http://www.govtrack.us/congress/bill.xpd?bill=s112-318
[97] See http://www.govtrack.us/congress/billtext.xpd?bill=h109-4954.
[98] See http://www.gao.gov/new.items/d10790.pdf (18/43).
[99] See http://www.govtrack.us/congress/bill.xpd?bill=h111-3619.
[100] See http://ec.europa.eu/enterprise/newsroom/cf/document.cfm?action=display&doc_id=5579 (30/318).
[101] See http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.
[102] Originally requiring 2-print finger scans, as of 2008 DHS has mandated that all ports of entry be equipped with 10-print finger scanning for international visitors.
[103] See http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm
[104] Examples include COM (2009)0149, COM (2004)698, and COM (2004)701.
[105] http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf (30/318).
[106] See http://www.dhs.gov/ynews/testimony/testimony_1286227672682.shtm.
[107] The U.S. 50 largest defence suppliers of the early 1980s have become 2000s top five contractors, creating a sort of oligopolistic market. In Europe, most firms continued to look inwards, and consolidation mainly took the form of large national defence champions acquiring small domestic firms. At the same time, the merger of DaimlerChrysler Aerospace AG (DASA) of Germany, Aérospatiale-Matra of France, and Construcciones Aeronáuticas SA (CASA) of Spain, gave life to EADS, the very first European company in the sector.
[108] In the U.S., Boeing; Lockheed Martin; Northrop Grumman; General Dynamics; Raytheon. In the EU, BAE Systems, EADS; Finmeccanica; Thales.
[109] The Joint Strike Fighter program represents a transatlantic case in point in this sense. Eurofighter, as well, can be considered a representative European consortium.
[110] Rolls-Royce acquisition of Allison and GEC-Marconi take over on Tracor.
[111] K. Hayward, *The Globalization of the Defence Business*, in G. Adams (et al.), *Europe's Defence Industry: a Transatlantic Future?*, CER, 1999.
[112] A. James, *The Prospects for a Transatlantic Defence Industry*, in Burkard Schmitt (Eds), *Between Cooperation and Competition: The Transatlantic Defence Market*, EUISS Chaillot Paper 44, 2001.
[113] K. Hartley, *Defence Economics and the Industrial Base*, Centre for Defence Economics, University of York.
[114] Of course, the Security Industrial Base (SIB) includes also dedicated divisions or subsidiaries of large defense firms (i.e. Finmeccanica's Selex Sistemi Integrati, Selex Galileo and Elsag Datamat; BAE's Detica; Boeing's Tapestry Solutions; Lockheed Martin's Homeland Security Division).
[115] For a more precise picture, see *The security market in the EU and the U.S.*, by H. Masson and L. Marta.
[116] Leading transatlantic vessel-traffic equipment manufacturers are: Northrop Grumman Space & Mission Systems Corp, USA; Kongsberg Maritime – Group Kongsberg, Norway; Jotron, Norway; Sam electronics, Germany; Thrane & Thrane, Denmark; CNS Systems, Sweden; Maris, Norway; Samyung, USA; Transas,

Ireland; Comar Systems, UK; Bluetraker, Slovenia; Marinetrack, UK; Bureau Veritas, France; Satamatics, UK.
[117] Ecorys, 2009.
[118] Leading detection equipment companies are: Smiths Detection, UK; L3 Security & Detection Systems, U.S.; Rapiscan Systems, U.S.; AS&E, U.S.; Bruker Daltonics, U.S.; Environics OY, Finland; ICx Technologies, Rae System U.S.
[119] Smiths Group Official Webpage, available at http://www.smiths.com/smiths_detection.aspx.
[120] See for example H. Pack, K. Saggi, *The case for industrial policy: a critical survey*, January 16, 2006, http://siteresources.worldbank.org/INTRANETTRADE/Resources/Internal-Training/HowardPack_KamalSaggiPaper.pdf.
[121] Jacques Gansler, *U.S. Defence Industrial Policy*, in "Security Challenges," vol. 3, n.2, June 2007.
[122] See Us government website at http://www.export.gov/ecr/index.asp.
[123] *Research for a secure Europe*, http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf.
[124] EC COM 2009(691), http://ec.europa.eu/enterprise/policies/security/files/mami/comm_pdf_com_2009_0691_f_communication_en.pdf.
[125] See the ECORYS-led *Study on the competitiveness of the EU security industry*, November 2009, http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf; or IAI-led *Study on the industrial implication of the blurring lines between security and defence*.
[126] European Commission, *An Integrated Industrial Policy for the Globalisation Era; Putting Competitiveness and Sustainability at Centre Stage*, COM(2010)614.
[127] See DG ENTR website, http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?item_id=4593&lang=en&tpa=0&displayType=news&ref=newsbytheme%2Ecfm%3Flang%3Den%26displayType%3Dnews%26fosubtype%3D%26tpa%3D0%26period%3Dlatest%26month%3D%26page%3D10.
[128] See the EC website at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/616&format=HTML&aged=0&language=EN&guiLanguage=en.

ISSUE 4

THE TRANSATLANTIC RELATIONSHIP AND EU-U.S. COOPERATION IN SECURITY

INTRODUCTION

Yves Boyer, *Deputy Director, FRS* [1]

It was clear from examining each of these cases that transatlantic cooperation in the security sphere needs to take into account broad changes in the international environment.

In the second decade of the 21st century signs of a turning point in international relations are noticeable, such as the emblematic shift of power in favour of China. The rise of Asia is creating a radically new situation and the international scene is entering into a radically different geopolitical period that should persist for several decades ahead. The emergence of new great powers, the likelihood of growing difficulties to access scarce resources such as energy, the existence of an increased number of failed states, the regional instabilities deriving from the spread of terrorism and the unrest that climate changes or demographic imbalance with mass migration might induce, are among the diverse factors that will bear upon interstate relation and above all on international stability. Political leaders have already touched upon the meanings such transformations are producing in international relations. The international scene will be characterised by the coexistence of various major powers, but none of them may be dominant enough to be able to impose its vision and choices on the world scene when at the same time non-governmental actors will bear upon world issues such as climate changes, the rule of law, etc. This form of "relativism" in international relations—i.e., all major powers are becoming more equal in their capacity to shape world events—may lead to blurring boundaries and interest among nations.

As far as NATO is concerned in this changing environment, any earlier notions of transforming the Alliance into the protector of western interest everywhere and on everything, from defence to energy has lost any practicability. The recent Strategic Concept of the Atlantic Alliance mostly reflects this realistic conclusion. The Concept narrows down the tasks which NATO can be assigned. Although, it does not give up the idea that the alliance's mission is to tackle any significant security threat. That point goes directly to the present state of the U.S.-European relationship. While U.S.-EU relations have been improving after the strains of recent years and probably will continue to do so, the vision of the transatlantic community as a single entity on the world scene is over—except, of course, in terms of defence if and when Article 5 of the Washington treaty is at stake. The Atlantic community does continue to subsist as far as shared values and common interests are at stake; it is fading away as far as political norms are concerned. Such evolution gives de facto limits to the perimeter of potential cooperation between the EU and the U.S., noticeably after the semi-failure of the West in stabilizing Afghanistan. That said, allies agreed in the new Strategic Concept adopted in Lisbon that the global nature of the security environment requires NATO to deal with diverse threats and challenges at strategic distances to effectively protect the territory and interests of its members.

Given the disappearance of an existential threat, as well as the transformation of the West with the development of the EU, political consensus between the two sides of the Atlantic can no longer be guaranteed when confronting new international challenges. A different dynamic has started particularly in the transatlantic space, where societal and homeland security are of greater concern than classic hard security issues. Military balance no longer dominates world equilibrium and leads most European nations to plan for reductions in their defense budgets. Environmental issues, long terms effects of biotechnologies, societal issues such as the place and role of religion in public policy, organized crime with globalized networks of corruption, monetary issues with the need to find a substitute to the role played by the U.S. dollar, the impact of globalization on democracy and the nation-state, and the growing role of trans-national corporations are all issues that now give rise to new stakes on the international stage and redistribute cards among nations. Indeed, one of the crucial difficulties that have to be transcended between America and the EU is closely related to diverse if not divergent cultural influences that now shape their respective vision of the world. Common points of reference are sometimes missing in analyzing increasingly rapid and complex international transformations, either to understand their origin or to envisage their potential political and strategic consequences.

Globalization has brought the biggest challenge to the perpetuation of transatlantic security cooperation. Frictions resulting from political, economic, trade or monetary divergences are indeed more frequent than ever between Washington and European capitals. These differences of opinion now extend to a wide array of topics ranging from the application of extraterritoriality laws to disputes on environmental issues, as recently witnessed at the world conferences on climate change in Copenhagen and Cancun. Indeed, at a time when U.S. and others envision using NATO as an instrument of stability outside the North Atlantic region, an instrument to tackle many security challenges existing on the world scene, one runs the risk of overloading the boat because political differences over such missions could undermine the strength of the Alliance. At a time when there is a growing need for the Europeans to assert their role on the international stage, a genuine partnership among equal partners offers a long term prospect to sustain the Alliance in the emerging world order.

In this new complex world, Europe has a major role to play. How should it be implemented? One option to consider would be to relegate the EU to being a soft power with hard military operations remaining the province of NATO under U.S. leadership. As a result, Europe's military ambition should be kept limited within narrow boundaries. Such a perspective does not, however, meet the realities of the geopolitical environment which oblige Europeans to envisage an uncertain future with growing rivalries among states or among a large number of actors. In this context, Europe cannot afford to limit its ambition to a narrow concept of security and continue to rely on the U.S. for guaranteeing its military security, as has been largely the case in the last decades of the 20th century.

According to the Maastricht and Lisbon treaties, CSDP (Common Security and Defense Policy) is to be the armed branch of the EU as a political entity on the international scene. Despite such commitment, this vision has not yet been realized but is still high on the agenda as recalled by the President of the EU Commission M. Barroso in his State of the Union 2010 speech, "let's be under no illusions: we will not have the weight we need in the world without a common defence policy." Six EU member states account for 82 percent of all defense expenditure by the EU-27. As a result there is a growing heterogeneity of knowhow and capabilities within the EU that make any positive move on CSDP more than difficult and will probably take a long time to materialize.

Will this situation last for long? It is difficult to predict but at least three observations can be made. First, the EU—despite the reluctance of most of its members—will face situations where it will have to assert, if not defend, its interest at a time where the U.S. will not be concerned or is preoccupied with engagements elsewhere. Then CSDP will become a necessity out of virtue. Secondly, a long period of growth has permitted strong defense spending in the U.S. with positive "collateral" benefits for Europeans. The new economic era combining enormous public debt with slow growth in most western countries will impact U.S. defense spending and priorities and should compel Europeans to rationalize their own defense efforts. If European leaders draw that lesson and take the necessary steps that would undoubtedly favor CSDP. Third, new types of threats combining unrest with instabilities and greater assertiveness in new centers of power may impact Europe in different ways than North America, forcing Europeans to invent their own mode of regulation of this new disequilibrium including in defense.

Such developments will soon raise the question of how best to adapt the security relationship between the EU and the U.S. NATO will remain the essential military alliance for ensuring that Americans, Europeans, and others can work together militarily in Europe and beyond. However, it is the nature of contemporary "grand strategy" that responding to threats and instability require application of all instruments of state power. Such engagements can only be afforded in the EU by aggregating national capabilities.

For the foreseeable future, influencing the United States will remain essential to European Foreign and Security Policy. However, the limits and unintended consequences of U.S. strategy in Iraq have also profoundly shaken American confidence, leading to a profound rethinking of the nature of American strategic leadership. Indeed, the very damage to American power and prestige that occurred has reaffirmed the conviction that allies and partners are important in a complex world in which one cannot be effective without being seen as legitimate. As power moves inexorably to the East, transatlantic solidarity will be vital if emerging state power is to be embedded in functioning institutions, such as the United Nations, that are so central to European "grand strategy." After all, this is the essence of effective multilateralism, and only Americans and Europeans in harness can achieve such a goal. There is thus every reason to believe that the transatlantic relationship could be rearranged as a meaningful politico-security idea and a fuller partnership.

There will be problems on one hand in the U.S. where politics inside the Washington Beltway still makes it difficult for American leaders to accept the constraints imposed by partnership. On the other hand, the lack of a strategic tradition in many European countries means that the relationship between membership in a strategic community and the responsibilities it imposes are little understood. In order to create common ground and to better share responsibilities with the U.S., Europeans must develop their strategic credibility as actors. That means a better organization both within the EU and a stronger, direct EU-U.S. relationship. Above all, it demands increased European investment in strategic civil and military capabilities and capacity. Such a pragmatic approach to the transatlantic relationship would also have a profound effect on Europe's profile in the world and the ability of the EU to share with the U.S. a positive role in contributing to the maintenance of international stability.

The four case studies examined in the framework of cluster 4 highlight the limitations when Europe does not deliver and the potential of such EU-U.S. cooperation—provided it is developed in a spirit of partnership.

THE NUCLEAR STANDOFF WITH IRAN AND THE FUTURE OF TRANSATLANTIC SECURITY RESPONSIBILITY-SHARING

Riccardo Alcaro, *Researcher, IAI*[2]

Introduction

The dispute over Iran's nuclear program, widely suspected of having a secret and illegal military purpose, is a major flashpoint. A nuclear Iran would revolutionise the power balance in the strategic Gulf area and jeopardise the Nuclear Non-Proliferation Treaty (NPT), to which Iran is a party as a non-nuclear state. The magnitude of the issue has prompted a number of countries to step in to curb Iran's nuclear plans. The European Union and the United States have been at the forefront of this effort. However, it has been only at the end of a gradual, irregular, and difficult process that the two sides have been able to reach convergence.

When the controversy emerged, the two had for years followed radically different approaches. Whereas the United States refused to recognise the clerical regime and championed Iran's isolation, the European Union established promising trade relations with it, complemented with a political dialogue. These broad policy orientations contributed to shaping the U.S. and EU's initial response to the nuclear challenge. Over time, however, the dispute led to a policy re-appraisal on both shores of the Atlantic.

Faced with Iran's rejection of their offer of dialogue and cooperation, the Europeans have agreed to incrementally ratchet up pressure on Iran by way of UN condemnation and UN and EU sanctions. The U.S.'s change of tack has been significantly more pronounced. At the end of a painfully slow process, marked during the Bush administration by a degree of indecision and ambivalence, the U.S. reached the conclusion during the Obama administration that it had a pragmatic interest in engaging the Islamic Republic over its nuclear program.

Transatlantic convergence has had important positive effects on the crisis management exercise. However, it is uncertain whether it can actually lead to an end result mutually satisfying for both the West and Iran, not least because it might have come too late. Nonetheless, analysis of the process that has led the EU and the U.S. to join forces illuminates the evolution of transatlantic security cooperation in the emerging multipolar world.

EU and U.S. Iran Policies Prior to the Nuclear Crisis

Prior to the nuclear crisis, the European Union and the United States pursued quite different approaches towards the Islamic Republic of Iran. After the electoral landslide of the reform-oriented Mohammed Khatami in Iran's 1997 presidential elections, the European Union attempted an upgrade of its relations with Iran by establishing a broad platform for dialogue on issues ranging from trade and energy to political dialogue and human rights issues. This process came to an end in June 2003, when the European Commission was instructed to put talks over an EU-Iran Trade and Cooperation Agreement (TCA) on hold due to mounting worries about Iran's nuclear activities.[3]

In contrast to its European partners, the United States pursued a policy of isolation of Iran for over twenty years. In 1996 Congress passed the Iran-Libya Sanctions Act (later simply Iran Sanctions Act, ISA), providing the president with the authority to impose restrictions on the U.S.-based activities of foreign companies doing business in Iran's energy resources sector. The ISA created a spat with the European Union, whose engagement strategy also aimed at safeguarding the interests of a number of big European energy companies involved in the development of Iran's lucrative hydrocarbon resources. The two sides were eventually able to find a compromise, as President Clinton agreed to a de facto exemption of EU companies from the ISA in exchange for the EU's commitment to support U.S. efforts to contain Iran's proliferation and terrorism-sponsoring activities.

These diverging policy orientations contributed substantially to determining EU and U.S. initial response to the challenge represented by Iran's nuclear plans. The latter emerged in full scale in early 2003, when the International Atomic Energy Agency (IAEA) confirmed that Iran's nuclear programme was much more advanced than previously known.

The E3/EU Action

The Bush administration was uninterested in engaging a clerical regime it openly despised. The U.S. would hardly have been in the position to initiate a dialogue anyway, as decades of isolation policy towards Iran had deprived it of tested channels of communication with Tehran. Consequently, it wanted the issue to be referred to the Security Council, but opposition on the part of veto-wielding permanent members Russia and China made this position a non-starter.

The Europeans, for their part, were of the opinion that Iran's nuclear activities presented a serious challenge to both regional stability and the non-proliferation regime. Like the Chinese and the Russians, however, they worried that the U.S. could be tempted to act unilaterally and strike Iran's nuclear facilities, as some Washington pundits had hinted.

Unlike the U.S., European countries had not cut off ties with Iran. The three largest member states of the EU—Britain, France, and Germany (the E3)—calculated that this had lent them the necessary credibility to sound out Iran's interest in a negotiation over its nuclear programme. The E3 counted on the fact that a European-brokered mediation could be appealing for the Iranians because it would have moved away from the spectre of a U.S. military strike. Their calculation proved accurate, as in October 2003 a negotiation process officially started. In late 2004 the E3 won open support by their fellow EU partners and were joined by the EU High Representative for the Common Foreign and Security Policy, and from then on acted under this peculiar E3/EU format.

The E3/EU approach revolved around a bargaining process. European negotiators assured Iran that it would have access to the international nuclear fuel market and that they would provide technical assistance in the nuclear field. They backed up the offer with the promise to resume talks over the EU-Iran TCA and to support Iran's application for membership in the World Trade Organisation (WTO).

Crucially, the E3/EU pledged that it would oppose Iran's referral to the Security Council as long as negotiations were ongoing. In return, the Europeans wanted the Iranians to freeze uranium enrichment, a legal but highly sensitive process that can serve both civilian and military purposes, and intensify cooperation with the IAEA.

Incentives as well as demands were worked out incrementally throughout the negotiation period. The Europeans and the Iranians reached a first arrangement in October 2003 (the Tehran 'Agreed Framework'), which they upgraded the following year in Paris. Under the Paris Agreement of November 15, 2004, Iran agreed to suspend all uranium-enrichment activities and confirmed it would implement the IAEA Additional Protocol, the 1997 text expanding the agency's inspection and verification powers, pending ratification by the Majlis, the Iranian Parliament (which has never followed). However, the negotiation over a final, mutually acceptable solution soon ran into trouble, as the two sides were unable to come to an agreement on the extent and duration of the enrichment freeze. The Iranians viewed it as a gesture of goodwill and took every chance to recall its "temporary" and "voluntary" character. The Europeans, on their part, pushed for a halt until confidence in Iran's intentions was restored.

The gap between the two positions proved insurmountable. After Iran's new, more hard-line administration of Mahmud Ahmadinejad restarted enriching uranium in early 2006, the Europeans opted to support Iran's referral to the UN Security Council for the imposition of sanctions. However, they did not give up on the diplomatic track, insisting instead that the offer of incentives could co-exist with the adoption of punitive measures.

The E3/EU's failure to eliminate the proliferation threat emanating from Iran's nuclear programme has been thoroughly scrutinised by security experts. The E3/EU was criticised for applying too strict a form of conditionality, while offering in return inadequate incentives. One of the E3/EU's main assets, the Trade and Cooperation Agreement, was a rather basic text. Moreover, the E3/EU opted for retaining the actual delivery of any incentive until the nuclear dispute was settled. This resulted in a situation in which the Iranians saw no rewards other than pledges for having frozen enrichment and signed the IAEA Additional Protocol.[4]

The weakest strand of the E3/EU strategy, however, was its inability to address the reasons why Iran could have felt the need to go nuclear or, at the very least, to acquire nuclear capability: a sense of insecurity and vulnerability (augmented by the U.S. invasions of Afghanistan and Iraq, its eastern and western neighbours, respectively) combined with a desire to play a role commensurate with its history and ambitions. The E3/EU was ready and willing to meet Iran halfway in this regard. Over the course of almost thirty years since the 1979 anti-Shah revolution, the Europeans had learned to appreciate the Iranian leadership's combination of realism and sense of national pride. They saw a hazy ambition to foment an Islam-rooted revolutionary wave in the Gulf turn into a pragmatic search for national security, regional influence, and consolidation of the clerical regime.[5] In the opinion of the Europeans, the Islamic Republic presented no real ideological challenge. On the contrary, intensified cooperation with an Islamic country would have helped to fight back the perception that after 9/11 western powers were pursuing an anti-Islam agenda. More importantly, the Europeans maintained that Iran could have an important, if not fundamental, role to play in stabilising Afghanistan and Iraq.

However, giving Iran a role in the re-making of the Gulf was, and still is, beyond Europe's power. The last word on this should necessarily come from Washington, whose political clout and military strength is felt all across the region. For the Iranians, therefore, the European strategic assessment that cooperation with the Islamic Republic was possible and indeed desirable was much less important for its own merit than for its potential to influence the United States. From this perspective, one important

reason why the Iranians accepted the European proposal for nuclear talks was the hope that the U.S. would be brought onboard. As this did not take place, the Iranians calculated that they would be better off re-activating frozen nuclear activities, and lost interest in the negotiation with the Europeans.[6,7]

This is not to say that the E3/EU action achieved nothing.[8] The E3/EU action raised international awareness of the dangers related to Iran's nuclear ambitions, while strengthening the case for Iran to remain within the treaty and subject to IAEA inspections.[9] Following the deals reached in Tehran and Paris in 2003 and 2004, Iran ended up under intense international scrutiny. The Iranian government felt compelled to take the costly decision to open the nuclear program to more intrusive inspections than required under the IAEA-Iran standard safeguard agreement. Although Iran's level of transparency was far from ideal, and glaring holes remained on the actual extension of its activities, the agency was able to give a more detailed account of the state of advancement of the nuclear programme at least until February 2006, when Iran stopped implementing the Additional Protocol. A more important consequence of the deals with the E3/EU is that Iran kept sensitive parts of its nuclear programme frozen for around two years.[10]

Another achievement of the E3/EU is that it has set the course of action to deal with the nuclear standoff. In all probability, the IAEA could not have referred Iran to the UN Security Council without the E3/EU action.[11] During the 2003-2005 negotiation period, the E3/EU walked a tightrope in engaging the Iranians while trying to invigorate consensus for their action within the EU and avoid fatal clashes with the U.S. (for being too soft) and with Russia and China (for being too tough). The culmination of this delicate process was the association in January 2006 of the U.S., Russia, and China to the E3/EU negotiating group, which has convened since under an E3/EU+3 format (the group is more commonly but less accurately known as the 'P5+1' or 'Iran six'). European insistence on gradualism proved to be a sensible choice, as consensus on sanctions within the Security Council was reached only after Iran persistently failed to comply with a series of increasingly firmer demands by the UN.[12]

Finally, and perhaps more importantly, the E3/EU provided the U.S. with a way out of its Iran 'non'-policy, which oscillated between vague dreams of forced or induced regime change and the sterile continuation of the unilateral containment strategy it had pursued with no results for over twenty-five years.

The Bush Administration: Strategic Ambivalence

The Iranians' hopes that assistance to anti-Taliban operations in Afghanistan in late 2001 and early 2002 could bring about a policy reappraisal in the U.S. were brutally dashed when President George W. Bush declared Iran part of an "axis of evil" that also comprised North Korea and Iraq. In May 2003 the Iranian administration made a second attempt, signalling its readiness to address all controversial issues on which Iran and the U.S. were at loggerheads, including the nuclear programme, in exchange for the normalisation of relations. The White House, apparently upon insistence by Vice President Dick Cheney, spurned the Iranian overture. Instead, it toughened its rhetoric in a way consistent with a regime change policy, leading the Iranians to accept the E3 offer of dialogue as a way to soften U.S. pressure and gain negotiating strength. At this point in time, U.S.-Iran reciprocal mistrust was probably at its peak.

The Bush administration's ostracism of Iran weighed heavily on the European-Iranian talks. Administration officials undermined the E3 initiative with statements expressing strong scepticism and describing Iran as a rogue state not worth talking with. And yet, the E3 initiative was not an entirely unwelcome development in Washington. As a matter of fact, having ruled out dialogue with

Iran, in 2003 the U.S. was short of options to deal with the nuclear issue. The intervention in Iraq and Afghanistan had raised the stakes of a strike against Iran's nuclear facilities, both politically and militarily. Moreover, the toppling of Saddam Hussein and the Taliban, two of Iran's main foes, had undermined the U.S.'s own containment policy. Like the Iranians, the Americans also seemed to view the E3 initiative as a "convenient buffer", a time-buying expedient that would defer confrontation until they felt ready for it.

In March 2005, the Bush administration suddenly decided to give indirect support to the E3/EU endeavour; although it made it clear it had no intention to join the talks.[13] In return, it extracted from the Europeans the promise that, if their attempt at engagement were to fail, they would support Iran's referral to the Security Council.

U.S. backing did not result in increased leverage for the E3/EU. To the contrary, the Europeans saw their room for manoeuvre constrained. At the time they were debating an Iranian offer for a comprehensive settlement, which was centred on the acceptance of an enrichment capacity. The Europeans had their own reasons to doubt Iran's sincerity and were inclined to uphold the enrichment freeze redline anyway, but U.S. intransigence led them to put aside any discussion about the possibility to detail, together with the Iranians, a roadmap at the end of which Iran would be allowed to enrich. The U.S. also refrained from backing the E3/EU's idea of including the supply of a light water reactor (LWR) in a proposal presented to the Iranian administration in August 2005. The French firms expected to provide LWR-related technologies backtracked in the absence of an explicit guarantee that they would not incur U.S. sanctions, leading the E3/EU to drop the idea.[14]

Against this backdrop, it is hard to describe the U.S. attitude in 2005 as truly supportive of the E3/EU. The Bush administration, then in its second term, was interested in reviving a transatlantic relationship still convalescent from the Iraq wound, but was not ready to renounce its policy of antagonism towards the Iranians. Its involvement contributed to making the European negotiating platform more rigid.

It was only after the E3/EU group expanded into the E3/EU+3 in early 2006 that the U.S.'s change of tack gained substance. Facing an ever more ferocious insurgency in Iraq, the Bush administration calculated that making some concessions to the E3/EU would best serve its interest in UN sanctions as it was the only option on hand to keep Iran under pressure. The Bush administration opted then to support the diplomatic track of the E3/EU approach, although it remained adamant on its refusal to engage with Iran as long as it continued to enrich uranium. In June 2006 the U.S. agreed to a new offer of cooperation and dialogue that the E3/EU handed the Iranians with Russian and Chinese backing. This time the Americans did not object to making an explicit pledge to support construction of an LWR in Iran with state-of-the-art technologies. In June 2008 U.S. Secretary of State Condoleezza Rice even put her signature on a letter accompanying a renewed E3/EU+3 offer to the Iranians.

In the meantime, however, the Bush administration persisted in treating Iran as a foe. In the 2006 U.S. National Security Strategy the Islamic Republic was described as "an enemy of freedom, justice, and peace" and singled out as the greatest challenge to the United States. More broadly, a sub-text of regime change policy was almost always discernible in the administration's public statements. The U.S. kept on pressing its partners in Europe and elsewhere hard for the adoption of tough sanctions against Iran, if not at the UN level (where Russia and China's resistance had only allowed for the adoption of targeted measures), then unilaterally. An informal campaign led by the U.S. Department of the Treasury partially succeeded in persuading ever more European governments and companies to rein in their businesses with Iran. However, the department's bullying attitude and its tendency to get past governments and directly address banks and companies ruffled many feathers in Europe. Despite the

fact that it could count on the support of Britain, France (which had become more hawkish under President Nicolas Sarkozy) and, to a lesser extent, Germany, the Bush administration was unable to generate enough consensus within the EU for the adoption of unilateral measures against Iran.

The Iran policy that President Bush bequeathed to his successor, Barack Obama, was therefore characterised by a good deal of strategic ambivalence which had multiple, negative net effects. Keeping the portrayal of Iran as evil while at the same time reformulating ever less stringent redlines convinced the Iranians of both the U.S.'s insincerity and its weakness. Furthermore, the limited nature of his concessions was seized not only by Russia and China but also by EU member states as a legitimate reason to resist tougher action.

The Obama Administration: Tactical Prudence

While committing to both components of the 'double track' approach (sanctions included), the Obama administration has worked on reducing the disconnect between policy and rhetoric. President Obama has put an end to talks of regime change, agreed to join the E3/EU+3-Iran talks without pre-conditions, sought greater cooperation from Russia by launching its 'reset' policy, and shown a willingness to engage the Iranians beyond the nuclear issue, with the aim of laying the foundations of a sustainable *modus vivendi*. He seems unconvinced that a strategic about-face similar in magnitude to the Nixon administration's decision to engage China in the early 1970s is attainable in the current predicament. Instead, he has opted for a more prudent approach, whose credibility relies on the consistency of the message: the U.S. is serious about the negotiations (as it is about sanctions) rather than on the offer of more lucrative incentives than hitherto promised.

Indeed, the Obama administration has shown a remarkable ability to stay the course, not least because Obama's advent to the White House overlapped with the authoritarian turn in Iran that followed the controversial re-election of the hard-line Mahmoud Ahmadinejad as president in June 2009. In October 2009, at a meeting in Geneva, the E3/EU+3 and Iran reached an agreement, largely devised by U.S. officials, on what could be described as the closest thing to a breakthrough since the November 2004 Paris Agreement. Iran gave its consent to send up to three quarters of its low enriched uranium to Russia and France, where it was to be further enriched and turned into nuclear fuel for a Tehran research reactor producing medical isotopes. This would have deprived Iran of the necessary nuclear material to potentially build a bomb for a year, thus giving more leeway to launch a broader negotiation on Iran's enrichment capacity.[15] In late 2009 it became clear however that Iran had back-pedalled on the Geneva deal. U.S. officials seized on this to overcome resistance from Russia and China over a round of UN sanctions significantly tougher than previous ones, and intensified talks with the E3/EU over potential follow-up measures on the part of the EU.

The process was neither smooth nor risk-free. The Obama administration managed to persuade an increasingly impatient Congress, where strong anti-Iranian sentiments cross party lines, to delay enactment of a much-awaited U.S. law expanding and toughening the 1996 Iran Sanctions Act. The White House feared that the new law could alienate its partners within the E3/EU+3 and derail talks over the new UNSC resolution, since the amended ISA explicitly targets foreign companies doing business with Iran with fines on their U.S. activities and denials of government contracts. The EU resented the extraterritorial application of the new law and lobbied U.S. authorities as hard as possible to get special exemptions.[16] The Obama administration was eventually able to safeguard the president's power to suspend sanctions against companies from countries that cooperate with the U.S. on Iran, even if this waiver authority is subject to more constraints than the EU hoped for. More important however was that the White House succeeded in postponing the law's passing until after the vote in the Security Council, as this made it possible for the EU to follow up with additional measures. UNSC

resolution 1929, adopted in mid-June 2010, provided the legal and moral basis for those EU member states doubtful of measures not specifically targeted on Iran's nuclear and ballistic activities to give the green light to a broader set of sanctions.[17] This is a crucial achievement, as the EU is, along with China, Iran's main trade partner, and sanctions from its side have could have a significant impact.

The Obama administration was also able to fend off an eleventh-hour attempt by Iran to derail the sanctions train. In May 2010, Iran agreed to a fuel swap proposal put forward by Turkey and Brazil that, while closely resembling the Geneva agreement, was nonetheless short of confidence building measures. The biggest loophole was that it revolved exclusively around the fuel swap as if this were an end in itself, whereas the West had seen it as just a means to create a mutually trustful environment for a negotiation on Iran's enrichment activities.

At the end of a months-long period during which it had to work hard on multiple fronts, the Obama administration met some important results. First, it ensured the unity of the E3/EU+3 by resisting pressure from Congress for immediate action. Second, it succeeded in cajoling its E3/EU+3 partners into its sanctions plan, so that between June and July 2010 the UN, the U.S., and the EU slapped punitive measures on Iran in rapid-fire succession.[18] Third, by avoiding chastising Brazil and Turkey for their untimely deal with Iran, Obama was able to give Iran a way back to talks without giving the impression of bowing to western pressure. In sum, by adopting the E3/EU-devised double track approach with more consistency than its predecessor,[19] the Obama administration has managed to preserve the diplomatic framework for a compromise with Iran while at the same time building a far greater sanctions coalition than had been possible in previous years.[20]

Some Lessons for Transatlantic Security Cooperation

The process leading the European Union and the United States to join forces in the attempt to curb Iran's nuclear programme offers some important lessons to better understand how transatlantic security cooperation is evolving and how it can be made best use of.

The first lesson is that transatlantic divergence does matter. When the United States and the European Union followed a radically different approach to the nuclear issue, Iran was able to exploit that difference to its advantage. By agreeing to enter talks with the Europeans, Iran managed to ease the pressure from the United States. The initial fractiousness of the transatlantic front also made it easier for it to advance its nuclear expertise. Thus, it was allowed to create facts on the ground that have become very difficult, if not impossible, to reverse. Today the overwhelming majority of experts recognise that no compromise seems conceivable if it does not include an Iranian enrichment capacity, albeit under strict IAEA supervision. This could have been different if the U.S. had agreed to join the Europeans during their 2003-2005 nuclear talks with Iran, during which the Islamic Republic had agreed to suspend work on enrichment.

The second lesson is that, even when the United States and the European Union are able to agree upon a common line—in this case, the 'double track' approach—this is of little help if their strategic objectives remain distant. The Bush administration's half-hearted support for the diplomatic track—resulting from its refusal to accept Iran as an interlocutor—narrowed the E3/EU's room for manoeuvre, thus diminishing the chance of a breakthrough. It also complicated cooperation with EU member states and between the EU and the U.S. on the one hand and other key actors, notably Russia and China, on the other. The validity of this argument is attested to by the fact that the Obama administration's more consistent embracement of the double track approach has allowed for the

creation of a larger and more cohesive front against Iran's nuclear ambitions. Not only have Russia and China agreed to a tougher set of UN sanctions than the previous ones, but the European Union itself has finally bowed to long-standing U.S. requests for additional restrictions.

A third lesson is that EU/European political and economic assets represent a critical, if not fundamental, crisis management resource, in particular when the United States is short of options. When the nuclear dispute broke out, the Bush administration had basically no room for manoeuver. The continuation of the unilateral policy of containment promised to be as sterile as it had been in the previous twenty-five years. Engagement was out of the question for ideological and geopolitical reasons. With containment being ineffective, engagement unconceivable, and a military attack too risky a gamble, the U.S. had placed itself into a corner. It has been the Europeans that have taken Washington out of it. Not only have they given it a policy it could align with, they have been instrumental in racketing up the pressure on Iran through the imposition of unilateral EU sanctions and expanding the international front opposing Iran's nuclear plans.

An extremely important corollary can be drawn from the above. The Iran case provides ample evidence of the fact that even joint EU-U.S. action can be insufficient to address a highly complex issue of international concern like the proliferation crisis with Iran in a long-term fashion. Broader participation is needed, in particular by rising or resurgent powers like China and Russia, increasingly active players such as Turkey, and other countries key to the successful implementation of sanctions (most notably the Gulf states and the U.S.'s Asian and Pacific partners). The Iran case shows that, in today's emerging multipolar world, the ability to shape a narrative and to persuade through diplomacy, bargaining, and compromise has become as important as power and influence to form coalitions of like-minded states. In this context, the transatlantic ability to caucus assumes a new, fundamental importance.

Also related to the previous argument is the conclusion that, in the nuclear standoff between the international community and Iran, a significant precedent for the future of crisis management has been set. The E3/EU+3 represents an interesting evolution of the 'contact group' phenomenon, according to which a given international issue is dealt with by a select group of countries on an informal basis. With respect to past experiences, however, the E3/EU+3 stands out for the significantly wider range of its action. Whereas other similar groupings, for instance the Contact Group for the Balkans, have usually acted as guarantors of the correct implementation of an already arranged settlement, the E3/EU+3 performs crisis response, management, and settlement tasks. In other words, it is more an actor than an arbiter, more a lead group than a contact group.

A similar reasoning can be made with regard to the European Union. The Union has been able to occupy one of the front burner seats in the nuclear dispute with Iran because of the unorthodox format—the E3 plus the High Representative—under which it has been working. Without the E3 taking the lead, it would hardly be conceivable how the EU HR could end up acting as the main interlocutor with the Iranians for the whole E3/EU+3, as has been the case since spring 2006. It is unlikely that the United States—not to mention Russia and China—could have consulted on such a delicate issue with the European Union without the mediation of its three largest and most influential member states.[21] From this perspective, the E3/EU sets as an important precedent for EU foreign policy-making as the E3/EU+3 does for the future of cooperative crisis management.

Conclusion

The United States and the European Union have not eliminated the threat emanating from Iran's nuclear plans. On the contrary, Iran has acquired the expertise to enrich uranium, the most sensitive part of a nuclear programme, and is getting closer to cross the nuclear weapon threshold. In this regard, the EU-U.S. performance cannot but be judged negatively.

However, a number of elements concur in qualifying this severe judgment. Thanks to U.S. and EU efforts, there is now an international consensus that the scarce transparency of Iran's nuclear policy poses a challenge to both regional stability and the nuclear non-proliferation regime. The transatlantic partners have been able to turn such concerns into a demand for action by the Security Council and the IAEA, whose role has been growing over the years. This has both increased pressure on Iran and restored centrality to the multilateral institutions that were marginalised during the Iraq crisis.

The adoption by the Security Council of a double track approach combining the offer of dialogue and incentives with sanctions is the result of a process leading the U.S. and the E3/EU from policy divergence to almost full convergence. Although it has taken years to get to this point, Americans and Europeans are now rowing in the same direction.

The picture would change if the U.S. were to opt for a military strike—alone or along with Israel—to slow down Iran's nuclear progress. Perhaps some EU member states, including France and Britain, would refrain from openly opposing any U.S. action. However, several EU member states are unlikely to buy the argument that the failure of the European years-long effort to persuade Iran to come clean on its nuclear ambitions has rendered an attack unavoidable. EU-U.S. cooperation on Iran would diminish considerably because intra-EU cohesion would dissolve. This would greatly reduce the appeal of a intra-EU 'lead group' acting on behalf of the Union in highly sensitive security issues, along the pattern of the E3/EU, and this could well result in the U.S. further 'bilateralising' its relations with EU member states. So, an attack against Iran is likely to undo, or at least jeopardise, whatever benefit may have accrued to the transatlantic partnership from the E3/EU+3 process.

Circumstances resembling the Iran case could arise in the future. The emerging multipolarity in political and security matters may still have a long way to go before matching the interdependence much of the world has attained in economic terms. But it has developed enough to compel the U.S. to thoroughly ponder the consequences of using its still superior military against a regional power the size of Iran without sufficient international support. In fact, the E3/EU+3 offers the highest-level example so far of an ad hoc crisis management mechanism, the lead group, which fits in an international multipolar system where competition and cooperation among states, and between states and international organisations, coexist. As the EU-U.S. ability to caucus becomes ever more important in such a context, strategic planners on both shores of the Atlantic should devote much greater attention to the fact that, in cases like Iran's nuclear issue, transatlantic convergence can turn out to be not an accessory, but a necessary component of an effective policy.

AFGHANISTAN: A STRESS TEST FOR TRANSATLANTIC SECURITY COOPERATION

Stephen Flanagan, *Senior Vice President and Henry A. Kissinger Chair, CSIS;* T.J. Cipoletti, *Research Associate, Henry A. Kissinger Chair, CSIS;* and Amanda Tuninetti, *Former Intern, Henry A. Kissinger Chair,*[22] *CSIS*

Introduction

Afghanistan has become a stress test for transatlantic cooperation in maintaining global stability. European solidarity with the United States in the aftermath of the attacks of September 11, 2001 was strong. However, differences between Washington and most European governments on the nature of the threat, strategy, and the goals of Western engagement have emerged. The mission in Afghanistan has become more demanding and complex than envisioned at the outset. After nine years of engagement, with limited gains in Afghan security and development, growing human and financial costs, and enduring doubts about the capacity of the Karzai government, commitment on both sides of the Atlantic is waning. NATO has pursued a more effective and better resourced strategy since early 2009 and the Alliance and its partners in the International Security Assistance Force (ISAF) have declared an "Enduring Partnership" with Afghanistan stretching to 2015 and beyond. All these factors and the success of the current strategy will influence the durability of this pledge and future transatlantic engagement in stabilization and reconstruction operations.

This paper examines U.S. and European strategic assessments and commitment, the convergence of their efforts, variables that will influence outcomes in Afghanistan, and the impact that possible denouements will have on the broader U.S-EU security relationship. While this case-study focuses on lessons of the Afghanistan mission for relations between the United States and the European Union and its member states, given that the preponderance of transatlantic engagement in the country is through NATO ISAF, this paper also examines relevant elements of European-American relations within NATO and NATO-EU relations.

Evolution of Transatlantic Engagement in Afghanistan

About a month after the attacks of September 11, 2001, the United States launched Operation Enduring Freedom (OEF). Working with the Northern Alliance and other anti-Taliban groups, this ad hoc coalition, comprised of several European states, Canada, Australia, and New Zealand, easily routed the Taliban and following intense fighting in December, a majority of al Qa'ida and many Taliban leaders fled into neighboring Pakistan. The United States and European governments supported United Nations-hosted talks on the country's future leading to the Bonn Agreement, which established a provisional government in Kabul backed by a UN-mandated security force. In August 2003, with

encouragement from the United States and other European governments, NATO agreed to assume command, coordination, and planning of ISAF. Transatlantic engagement has deepened since.

Current State/Strategic Approach

Over the past nine years, U.S. and European engagement have helped the Afghan government enhance security, governance, and economic development in several sectors.

The Afghan security forces, particularly the Army, have grown in numbers and effectiveness. In August, the Afghan National Army (ANA) fielded 138,200 soldiers—exceeding its 2010 headline goal of 134,000 troops three months ahead of schedule—and aims for a force of 171,000 by October 2011. Afghan forces have assumed lead responsibility for security in Kabul province since August 2008, and have become involved in combined operations with ISAF around the country. The Afghan National Police (ANP) has also exceeded its 2010 goal, reaching 120,500 personnel in September 2010. The ANP hopes to grow to a force of 134,000 by October 2011, but continues to suffer for shortages of qualified personnel and corruption. The ANP's paramilitary civil-order forces (ANCOP) have recounted themselves well in preserving order in major cities and assisting local police in high-threat areas during emergencies.

ISAF and Afghan government planners have focused counterinsurgency and development efforts on 80 key districts where the majority of Afghans live and that include centers of economic productivity and key infrastructure and commercial links to the wider world. The 27 Provincial Reconstruction Teams (PRTs) and about 40 of their subordinate District Support Teams (DSTs) are focused on these key districts and 41 other areas of interest.[23]

The pace of improvements in Afghan governance, rule of law, and development has been very slow. In addition to the security problem, rampant corruption has limited the central government's effectiveness and credibility in many provinces and districts. With encouragement from Washington and EU governments, the Karzai government has formed a Peace Council in an effort to begin a dialogue with the elements of the Taliban and other insurgents who renounce violence and are willing to abide by the Afghan constitution. However, the effectiveness of the leaders of the Afghan government's Peace Consultative Jirga to engage with the insurgency has been questioned and finding credible interlocutors among the fighters has proven difficult. Planning for reconciliation and reintegration of fighters as part of a peace settlement has not matured.

The Afghan economy has rebounded somewhat since 2001, but is heavily dependent on foreign assistance. There have been gains in the agriculture sector, due to enhanced access to internal and international markets via new roads, as well as a revival of the service sector. The importance of private sector growth for Afghan development was underscored at the London Conference in January 2010 where the international community endorsed the Integrated Plan for Economic Development proposed by the Afghan Government. Opium remains the largest cash crop in Afghanistan and production, focused in the south and southeast, has increased since 2001. About 12 percent of the population is involved in opium poppy cultivation, and the UN estimates that the total value of the opium harvest to farmers, laboratory owners, and traffickers was about $4 billion in 2007, equivalent to 44 percent of the licit GDP.[24]

Before the late 2009 surge in military and civilian personnel, Afghanistan was slowly deteriorating in nearly every available metric. The trends in violence were up sharply in 2009 from 2007 levels, and civilian casualties were the highest on record since 2001. Ninety-five percent of Afghans said corruption was a problem in their area (up 23 points since 2007), and about 80 percent of Afghans live in rural areas and in poor conditions.[25] Winning government support among the population remains a

major challenge. Still, the fragile gains from the campaigns in the Taliban strongholds of Marja and Kandahar as part of the implementation of the new strategy have led to mounting doubts about both the strategy and goals of international engagement in Afghanistan.

Comparison of U.S. and European Commitments

United States

Threat assessment

After the 9/11 attacks, American leaders saw al Qa'ida, given its global reach, messianic ideology, and interest in acquiring weapons of mass destruction (WMD), as an overarching, existential threat to the United States, its democratic allies, and many partners around the world. President George W. Bush declared a "War on Terror," with the Afghanistan campaign as a central element of that war.

Strategy

U.S. strategy was widely perceived in Europe as overly militarized with little regard to international law and norms. The Bush administration's decision to conduct the initial stages of the Afghanistan campaign as a "coalition of the willing" left many European governments doubting Washington's commitment to NATO. After achieving a rapid defeat of the Taliban, U.S. strategy was to continue to pursue al-Qa'ida and other extremists in the region, and to work with the international community to provide humanitarian and other assistance necessary to rebuild Afghanistan and prevent it from serving again as a safe haven for terrorists. However, the Iraq War soon dominated political attention and drained military and development assistance resources. In 2006 the administration affirmed that Afghanistan and Iraq were the front lines of the "War on Terrorism," but it was then looking to NATO allies, the European Union, and other international partners to take on a larger role.

President Obama came to office in 2009 arguing that the Iraq War was a diversion and that Afghanistan is the "central front" in the struggle against violent extremism. Obama committed 17,000 additional troops to Afghanistan within a month of taking office, and articulated a comprehensive new strategy for Afghanistan and Pakistan on March 27. This new strategy narrowed the mission to focus on efforts, "to disrupt, dismantle, and defeat al Qaeda" through increased aid to Pakistan, establishing a better way to measure progress in combating terrorists, and ramping up efforts to train the Afghan army and police force with the deployment of an additional 4,000 trainers.[26] The Obama strategy also placed a new emphasis on civilian capacity-building, which European governments found appealing. Obama named General Stanley McChrystal, known for pioneering the U.S. Army's counterinsurgency concepts in Iraq, as commander of the ISAF mission.

As security continued to deteriorate over the course of 2009 and General McChrystal submitted his assessment of the conditions on the ground, the Obama administration again raised the stakes. After a lengthy policy review, President Obama refined his strategy in December and decided to send 30,000 additional troops to the region. Obama also announced that the transfer of American forces out of Afghanistan would begin in July 2011—the first American withdrawal timeline of the war. This new strategy includes three main elements designed to turn the tide: 1) U.S. and ISAF partners working to target the insurgency where it is concentrated, secure key population centers, and enhance capabilities of Afghan security forces; 2) Work with partners to improve accountable and effective Afghan governance at the national, regional, and local level, and focus assistance on areas that can have an immediate and enduring impact; 3) Forge a strategic partnership with Pakistan. This plan called for

more robust counterinsurgency efforts to protect Afghans living in Taliban strongholds in the south and east of the country, as well as an escalation of targeted military strikes against al Qa'ida, Taliban, and other insurgent leaders in both Afghanistan and Pakistan.[27]

U.S. relations with the Karzai government have become strained due to its general lack of capacity, continued allegations of corruption, and questions about the fairness of the August 2009 presidential elections. These doubts about the Karzai government have complicated execution of the Obama administration's strategy and efforts to maintain Congressional and public support.

The most vexing element of the strategy remains relations with Pakistan. Despite good relations and expanded assistance to the Zardari government, cooperation between elements of the Pakistani Inter Services Intelligence agency (ISI) and radical extremists, including al Qa'ida appears to persist. This relationship, coupled with Pakistan's reluctance to commit sufficient resources to gain control of its frontier regions along the Afghan border, provide Afghan insurgents with valuable safe havens.

Resource Commitments

The United States is shouldering the bulk of the burdens for maintaining security in Afghanistan and training of their security forces. As of November 2010, the United States fielded about 90,000 troops as part of ISAF and an additional 10,000 operating independently of the NATO mission. Total U.S. force levels in Afghanistan are expected to remain constant at the 100,000 level through mid-2011. Washington provides 76 of the 150 OMLTs (Operational Mentoring and Liaison Teams) for training the ANA and 279 Police Operational Mentor and Liaison Teams (POMLTs) for the ANP; NATO as a whole currently only fields 38 POMLTs.

The United States has provided approximately $13.4 billion between 2002 and 2010 in non-military assistance to Afghanistan.[28] These resources have supported programs to strengthen Afghan governance, infrastructure, economic development, education, rule of law, and counter-narcotics programs. The Obama administration has increased U.S. civilian assistance to Afghanistan and Pakistan over the past two years, with a focus on new alternative development programs, strengthening the rule of law, and short-term job creation programs, in the south and east of Afghanistan and the frontier regions of Pakistan. The United States has also initiated an "uplift" of civilian personnel in Afghanistan to help stabilize key regions and manage expanded assistance programs. The U.S. civilian presence in Afghanistan has grown from about 360 to 1,100 personnel between January 2009 and the end of 2010, but given security and other operational limitations, only about 400 of those personnel are working with PRTs and DSTs in regions outside Kabul. The civilian uplift goal is to place 1,500 personnel in country by January 2012.[29]

Political Support

After nine years of engagement, with an expanding presence and mounting casualties, American legislators and citizens increasingly want assurance that their investments are producing tangible results. A Bloomberg poll in October 2010 revealed that only 40 percent of respondents believed that it was worth it to keep fighting, and an earlier Newsweek poll found that only 26 percent of Americans believe the U.S. is winning the war. Only 33 percent believe that it is even possible to achieve stability in the region. Nonetheless, sizable majorities of Americans remain convinced that stabilization of Afghanistan will improve U.S. security and that eliminating the terrorists' bases there is worth the commitment of U.S. military forces.[30]

European and EU Commitments

Threat assessment

Most EU governments accept that the 9/11 attacks demonstrated the potential for catastrophic terrorism and that extremist safe havens in Afghanistan and Pakistan threaten regional and transatlantic security. Many European leaders don't, however, subscribe to President Obama's contention that Afghanistan is "the central front" in the struggle against terrorism and have had strong reservations about U.S. strategy and calls for greater resource commitments. European governments opposed Taliban rule and agree that its return to power would be damaging to Afghan civil liberties and regional stability. Without a sense of global commitment and existential urgency, European involvement in Afghanistan has been more fragmented and hesitant than that of the United States.

Strategy

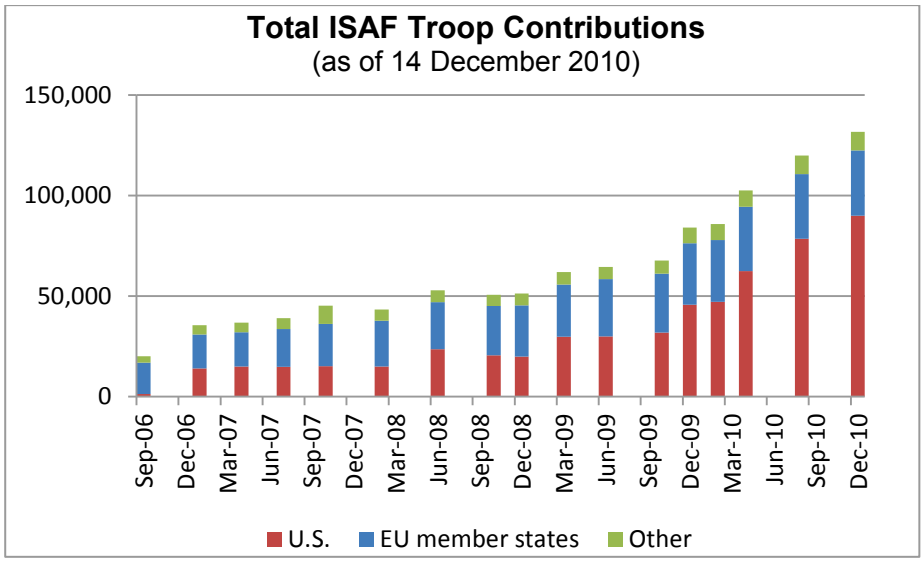
The initial intervention in Afghanistan came after the first-ever invocation of Article 5 of the North Atlantic Treaty, and was strongly supported by individual European states. However, Europeans objected to what they saw as the overly militarized nature of U.S. strategy in OEF. Europeans have felt that the threat is better addressed by the security services and law enforcement authorities, coupled with enhanced development assistance and other support to the Afghan government. Differences with the Bush administration over the initiation and conduct of the Iraq War further strained relations. Washington convinced hesitant European governments to agree to a NATO takeover of ISAF and expansion of the mission with assurances that the insurgency was largely defeated and that this would be a challenging peacekeeping mission. As the Taliban regained strength and mounted widespread attacks after 2006, many European governments and publics grew uncomfortable with the mission and mounting pressures from the U.S. and other allies to adopt more aggressive rules of engagement and counterinsurgency tactics. Few accepted that Europe's security needed to be defended at the Hindu Kush.

Most European governments are reticent to employ their military forces overseas other than in UN-mandated peacekeeping or humanitarian operations. U.S. Defense Secretary Gates has publicly lamented the "demilitarization of Europe."[31] In many EU countries the debate over whether or not to label the Afghan conflict a "war" still rages. President Sarkozy and others heralded the NATO strategy embraced in April 2009 as a triumph of the European vision with more focus on "building Afghan capabilities than on killing the Taliban." Most European leaders still do not share the depth of the U.S. conviction that the ongoing counterinsurgency and counterterrorism operations in Afghanistan are essential to preventing future terrorist strikes on the West.

Resource commitments: Contributions to NATO operations

The differences in threat perceptions and thin public support have resulted in European human and financial commitments in Afghanistan considerably smaller than those of the United States. With the exception of Cyprus and Malta, all EU member states have contributed troops to ISAF, with the UK, Germany, France, and Italy providing the largest European contributions. EU member states have slowly, but consistently, increased their troop contributions to ISAF since 2006. Securing the deployment of these forces, however, required major internal battles and concerted transatlantic diplomacy. Following President Obama's December 2009 announcement that the U.S. would deploy 30,000 more troops to Afghanistan, several EU member states pledged about 7,000 additional troops. As of December 2010, EU member states' troop contributions to ISAF totaled 32,481 and represented

25 percent of the total ISAF troop count. These totals include about 1,200 trainers and responsibility for 48 OMLTs out of a total of 150. Not all European countries have committed personnel to NTM-A, and many have provided fewer troops than promised, leading to significant gaps in trainers and mentors that have been or will be filled by U.S. and Canadian forces.



Source: ISAF Placemat, 14 December 2010.[32]

EU member states have also contributed to civilian security efforts through NATO. In March 2009, the member nations of the European Gendarmerie Force (EUROGENDFOR)—France, Italy, the Netherlands, Portugal, Romania, and Spain—agreed to a French proposal to conduct police training in Afghanistan. EUROGENDFOR personnel have partnered with NTM-A (NATO Training Mission Afghanistan) to fill about 200 of the mission's 609 positions for gendarmerie trainers, including contributions to POMLTs and have the lead for training and mentoring ANCOP forces at Regional Training Center-North. Poland, Spain, the UK, and Denmark also contribute to POMLTs.

Resource commitments under CSDP

The EU has also undertaken communitarian efforts in Afghanistan as part of CSDP. In 2005, the EU and Afghanistan issued a joint declaration on an EU-Afghanistan partnership based on shared priorities such as the establishment of strong and accountable institutions, security and justice sector reform, counter-narcotics, and development and reconstruction. The EU has since made strengthening the rule of law in Afghanistan through the development of a strong police force and justice system its key priority. The Country Strategy Paper outlines the EU's commitment to Afghanistan until 2013, citing rural development, governance, and health as its three focal areas. The EU has posted a Special Representative in Kabul since early 2002 to liaise with the Afghan government and the international community, and the incumbent, Vygaudas Ušackas, has authority to advise on EU Afghanistan policy, coordinate its implementation, and negotiate on behalf of the Union.[33]

Germany agreed to take on the task of police training in Afghanistan, but after the project suffered from poor recruitment and performance, NATO asked the EU to take control and EUPOL was established in June 2007. EUPOL works to develop and execute training techniques for the Afghan

Police, as well as other civilian officials in the Afghan government. EUPOL comprises the bulk of the EU civilian presence in country. EUPOL was authorized to deploy 400 police officers, but had 301 international staff and about 172 local employees as of November 2010.[34] EU governments have had difficulty recruiting for the Afghan mission, in part because sizable numbers of active duty and retired European police officers are currently serving in the missions in Bosnia and Kosovo. The lack of an EU agreement with NATO on sharing classified information has somewhat restricted EUPOL's situational awareness and operations in dangerous operating environments. In terms of effect, experts on security sector reform have questioned whether the European "community policing" model can be successfully applied in Afghanistan.

The EU (European Community and member states combined) have committed some €8 billion in assistance to Afghanistan for the period 2002-2010. Of this amount, over €1.3 billion has been contributed through the EC budget covering a range of activities, including governance, support to the ANP and justice sector reform, alternative livelihoods, health, and border management. EU budget assistance is slated to rise to €200 million a year for the period 2011-13, with focus on the priority programs identified by the Afghan government at the Kabul Conference.

Political support

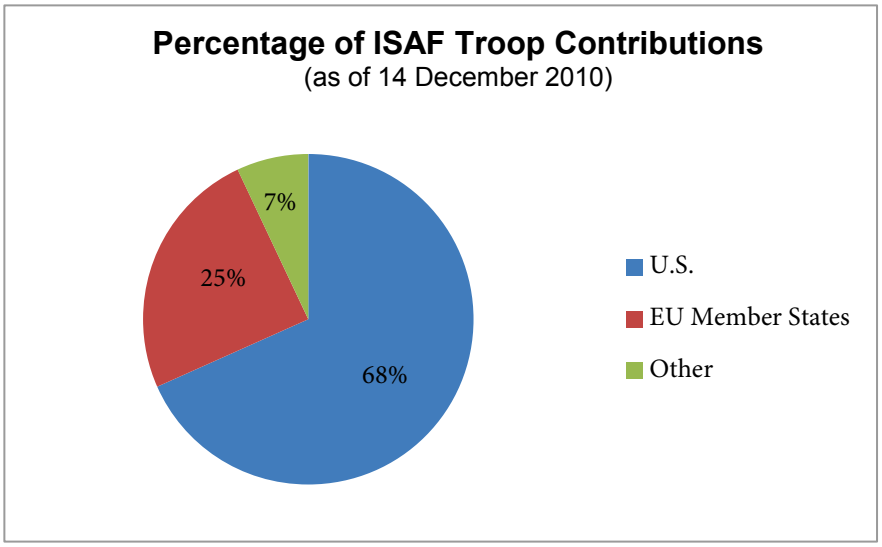
Political leaders and citizens in most European countries have been largely unenthusiastic about the international engagement in Afghanistan. While public support for the Afghan war in Europe has recovered slightly from the all-time lows of fall 2009, anti-terror efforts and the war in general have received much less public support in Europe than in the United States.[35] In France 70 percent of adults polled are either completely or mostly opposed to the mission. In Germany 35 percent of the public want their troops removed immediately, and 44 percent want them to return by the end of 2011, conditions permitting.[36,37] As the number of British soldiers killed in Afghanistan approached (and has since surpassed) 300 in April 2010, public support for the war was at an all-time low, with only 32 percent of those polled in favor of the military operation and 55 percent opposed, a number that has since increased to 60 percent.[38] European leaders who do support continuation of the international presence often cite that it prevents a return of Taliban rule, which would have abhorrent consequences for human rights.

Increased casualties since 2009 have re-energized public opposition to the war in most European countries. Prime Minister Balkenende's effort to extend the deployment of 1,950 Dutch troops to the end of 2010 led to the collapse of his government, and Dutch forces began withdrawing in August 2010. A number of other European governments have begun discussing withdrawal dates including Germany, Italy, Poland, Denmark, and even the UK.

Convergence of Effort?

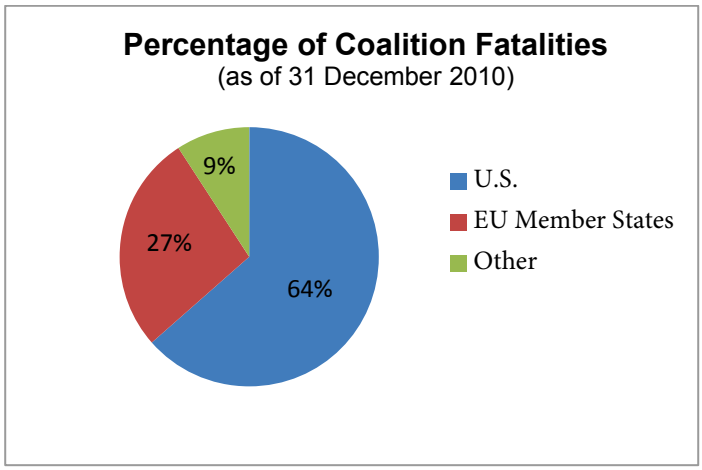
Despite the many setbacks and disagreements between Washington and various European capitals over strategy, military operations, and resource commitments, there has been considerable convergence in political engagement with the Afghan government and civilian assistance efforts. Overall convergence of effort has grown during the Obama administration. European governments and publics have generally welcomed Obama's decisions to narrow the objectives, increase the civilian role in stabilization programs, and set July 2011 as a target date for military disengagement. While these developments have led to improvements in transatlantic security cooperation concerning Afghanistan, the U.S. and Europe still disagree on important policy and operational matters. There are also shortcomings in the overall coordination and integration of military and civilian stabilization and reconstruction efforts.

Washington has expressed frustration for several years with imbalances in both the level of U.S. and European military contributions and the risks to which they have been exposed. Europe was slow to provide forces for the initial rounds of ISAF. However, European governments were also dismayed by Washington's decision to opt out of that mission, preferring to focus its efforts on OEF. U.S. contributions to ISAF began to grow after 2006, but at the time President Obama came to office, European and partner governments were still providing 43 percent of total ISAF forces and had incurred about 35 percent of the casualties. The Obama administration has used subsequent U.S. troop 'surges' to pressure European allies to also increase their contributions, but with limited success. President Obama called the modest allied pledges following the Strasbourg/Kehl Summit a "down payment." Obama's inability to secure more substantial allied commitments, at a time when he enjoyed enormous popularity in Europe, led critics in Congress and the media to contend that his new strategy and style of leadership were no more effective than those of President Bush and reinforced the sense in U.S. political circles that Europe is unwilling to pull its weight in safeguarding transatlantic security from global threats.



Source: ISAF Placemat, 14 December 2010.[39]

Differences in doctrine, capabilities, and national "caveats"—which restrict the operational or geographic activities of most European military forces in Afghanistan—have long perturbed U.S. and NATO military commanders. Several NATO allies did relax their national caveats somewhat following the 2006 Riga Summit to allow deployment in "emergency" situations, and France dropped nearly all operational restrictions on its troops. However, the refusal of about half of European governments and parliaments to modify these restrictions has exacerbated divisions both across the Atlantic and among European NATO members over the increasingly evident inequities in risk-sharing, as well as burden-sharing, in Afghanistan. Public complaints by U.S. officials and commanders about the caveats and other shortcomings of European forces have sometimes been counterproductive with European politicians already bucking domestic opposition. In addition, incidents of unintended Afghan civilian casualties, as happened when German forces called in a U.S. airstrike on a tanker convoy near Kunduz in September 2009, have reinforced European concerns about less restrictive rules of engagement.



Source: iCasualties.org.[40]

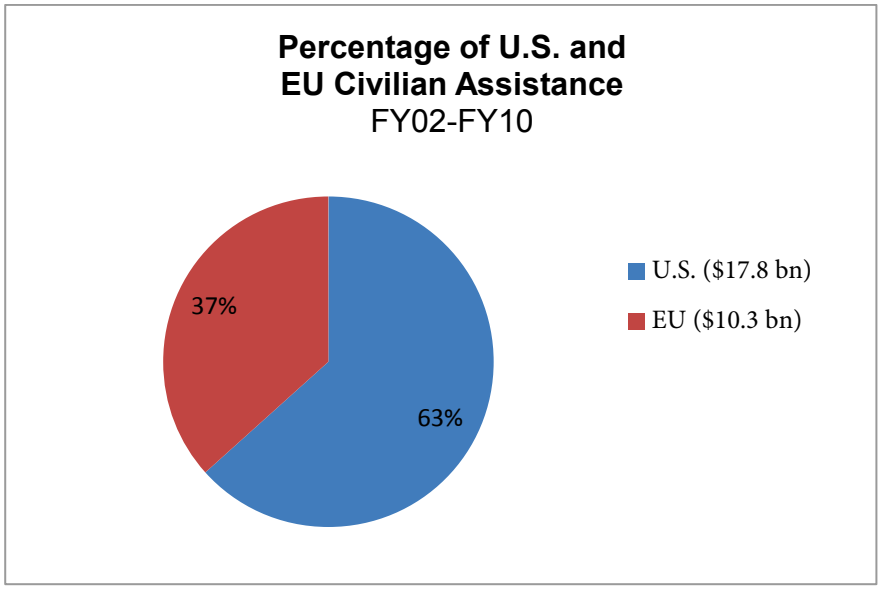
The lack of a common NATO counterinsurgency (COIN) doctrine and failure of most European militaries to embrace COIN tactics has also constrained integration of European and American military operations and cultural differences may well make it hard to achieve. The Alliance has made progress in doctrinal, training, and operational issues, particularly with the development of the NATO Special Operations Headquarters (NSHQ). However, many European governments remain wary about the conduct of counterinsurgency operations and some are subject to legal and/or parliamentary restrictions due to lingering negative political connotations associated with the strategy.

Most European governments are reluctant to undertake or lack a mandate for military counterterrorist operations, including the targeted killing of key al Qa'ida and Taliban insurgents. Operational reports disclosed by Wikileaks in July 2010 strengthened parliamentary objections. The expanded U.S. use of drones in Afghanistan and Pakistan for these operations has also become controversial in some European countries.

Washington has lamented the failure of several EU member states and the EU to meet commitments to support police training, rule of law, and judicial reform programs in Afghanistan. The modest size of EUPOL, coupled with logistical and other complications, have limited the EU contribution in this area. Harmonization of U.S. and European efforts in security assistance and training programs has also been problematic. Multiple and sometimes conflicting inputs from different contributors and stakeholders (NATO, EU, UN, and national governments) have often led to a disjointed and confusing approach to police training. This led to the creation of the International Police Coordination Board and various subgroups, which are designed to ensure more effective integration of various police training activities and provide policing advice to military leaders and the Afghan government. NATO has had a Senior Civilian Representative in Afghanistan since 2003 to liaise with the Afghan government and international organizations. In January 2010, former UK Ambassador to Afghanistan Mark Sedwill was appointed to the post, with a mandate to assume a greater role in coordinating the delivery of international civil support to the ISAF campaign.

While U.S. officials have been disappointed with the scope of engagement by the EU and its member states in civilian assistance, there appears to be considerable complementarity in transatlantic efforts. This has been achieved through coordination with respect to the planning for and implementation of plans flowing from various assistance conferences, beginning with the Bonn

Conference in 2001 and up through the 2010 London and Kabul conferences. U.S. civilian assistance has focused heavily on infrastructure projects (roads and power), economic development, education, and alternative (agricultural) development/counter narcotics programs. The European assistance priorities of governance, justice/rule of law, and health seem largely complementary. Nonetheless, there is still not an effective executive-level mechanism in Kabul for coordination of the civilian assistance of the international community—both official and non-governmental—with the priorities of the Afghan government.



Sources: EU Engagement in Afghanistan Factsheet[41] and U.S. Foreign Operations Congressional Budget Justifications, 2002-2011.[42]

Factors/Variables Influencing the Outcome

Several major factors will influence the outcome of U.S. and European engagement and 2011 will be a decisive year. Rising casualties and the limited success of the campaigns in Marja and Kandahar, coupled with the need to reduce governmental spending in the midst of the enduring financial crisis, have increased pressures on both sides of the Atlantic to meet the targets for transition to an Afghan lead in security between 2011 and 2014. A number of European governments are right on the edge of acceptable levels of casualties and many have seen the fall of the Dutch government in 2010 as a cautionary note.

The strength of the insurgency and the ability of the Afghan government to take on increased responsibility for security are also key variables impacting U.S. and European commitment. There are signs that U.S. counterterrorism operations against key al Qa'ida and Taliban fighters are increasingly eroding insurgent morale and recruitment. The Afghan government has launched its reintegration campaign to convince mid- and lower-level Taliban fighters to lay down their arms. If these efforts, coupled with the development of a political dialogue with Taliban leaders, are successful, the strength of the insurgency could begin to wane. The progress of efforts by the Pakistani government to cut its ties with the Taliban and gain control over its frontier areas will be another major factor in

diminishing the strength of the insurgency. The capacity of the Afghan government to enhance governance, deliver essential services, combat corruption, and implement effective justice and rule of law will also be decisive.

Dramatic developments in the region, such as further political instability in Pakistan, or the emergence of another major international crisis (Iran or North Korea), could also have an impact on political attention and commitment to the mission.

Scenarios

There are a number of scenarios that one can envision for Afghanistan. Three seem most plausible:

1. A continuation of currents trends through 2011, with limited success against the insurgents, modest gains in Afghan governance, and mounting public disaffection with the mission in Europe and the United States.
2. Dramatic breakthroughs in the security situation in Afghanistan or Pakistan, including a collapse of the insurgency and some form of reconciliation with elements of the Taliban and reintegration of some insurgents.
3. A major setback such as the collapse of the Karzai government or of the counterinsurgency campaign in the south and east, perhaps as a result of a catastrophic attack on ISAF forces or a base (something akin to the 1993 ambush of U.S. forces in Mogadishu or the 1983 bombing of the U.S. Embassy in Beirut).

Pressures for withdrawal would build under the first and the third scenarios, with many objectives of transatlantic engagement incomplete or even undone. Transatlantic engagement through 2014 and beyond can probably be sustained under scenario one, but would be far more likely under scenario two.

U.S. and European leaders have found it difficult to articulate what would comprise success of transatlantic engagement in Afghanistan. The 2001 Bonn agreement and the 2004 Afghan constitution envisioned a highly-centralized democracy. President Karzai's government has tried to make this model work, with some devolution of authority to local officials. However, it is unlikely it can be sustained given the limited legitimacy and capacity of the central government, as well as Afghanistan's political culture and history. Much less ambitious end states could safeguard transatlantic strategic interests. A decentralized model, which retained national control over foreign policy, the armed forces, customs, and counter-narcotics operations, but granted provincial and local governments considerable latitude in economic, social, and law enforcement policies, would be more likely to engender the support of the country's various ethnic and sectarian groups, as well as reformed elements of the insurgency.[43] Most European governments appear comfortable with this end state.

Mixed-sovereignty would be a more radical move away from the post-2001 governance model, but Afghanistan functioned under this model in relative stability for much of the 20th century. It would acknowledge the de facto arrangements that have seen several provincial governors leverage their own security forces and power bases to reach *modi vivendi* with the central government. It could preserve transatlantic strategic interests if the United States and other members of the international community were willing to support the central government in enforcing this power sharing arrangement with regional warlords through the threat of punitive military actions and allocation of foreign assistance.

This outcome would require more substantial U.S. and possibly European engagement in Afghanistan and neighboring countries to ensure regional stability.

A number of other outcomes for Afghanistan are possible that would threaten transatlantic security interests. De facto partition between the Pashtun-dominated south under Taliban control and the largely Tajik, Uzbek, and Hazara areas in the north and west of the country, or into a number of mini states, is one scenario that some experts on the region envision. This outcome could result from a political settlement or a reconciliation deal wherein the central government gave the Taliban too much autonomy in the south. It could lead to further internal conflict in Afghanistan and provide the Taliban with safe havens for cross-border operations designed to destabilize Pakistan with much larger strategic consequences—including the emergence of a "Talibanistan" armed with nuclear weapons.

If the Karzai government collapses, Afghanistan could revert to the kind of anarchy and civil strife of the 1990s that set the stage for the Taliban's rise to power. Afghanistan would likely reemerge as a lawless and ungoverned space and an ideal base for extremist groups to plan terrorist strikes and destabilize Pakistan and other neighbors. It would be seen as a complete failure of engagement by the United States, NATO, the United Nations, the European Union, and other elements of the international community, with global repercussions.

Impact of the Afghan Engagement on the EU/U.S. Security Relationship

The Afghanistan case illustrates a number of difficulties in transatlantic security cooperation on emerging global challenges. Differences in conceptual understanding of the conflict and the nature of the mission have led to asymmetrical and incompatible human and financial contributions, threatening not only the goal of stabilizing Afghanistan, but also the future of EU-U.S. security cooperation.

The envisioned NATO-EU division of labor in which NATO does the fighting and establishes a secure environment and the EU then takes responsibility for reconstruction is not working. The Afghan engagement has highlighted the limits of the EU as an actor in semi-permissive environments and exposed its lack of doctrine and capacity in security sector reform. At the same time, NATO has consistently underperformed in this field as well, and the lack of civilian capacity in NATO is well known. As both institutions now consider how best to develop these capabilities, this opens new opportunities for cooperation, particularly in light of enduring fiscal constraints.

It is hard to envision another transatlantic undertaking in the security area on the scale and scope of the current engagement in Afghanistan in the near future. However, irregular warfare and regional instability are likely to remain among the leading threats to transatlantic security in the coming decade. The new NATO Strategic Concept and Lisbon Summit Declaration reaffirm that enhanced cooperation with the EU and other partners is essential to successful implementation of the comprehensive political, civilian, and military approach to crisis management and response. NATO leaders have also agreed to develop a modest civilian capability to interface more effectively with partners in stabilization and reconstruction missions. The revised ISAF strategy may provide guidelines for ensuring better integration of NATO and EU efforts at the outset of future interventions in weak and post-conflict states.

While NATO-EU cooperation in Afghanistan has not provided a template for future engagements, it has advanced the transformation of European armed forces. European governments have been

required to restructure their forces to meet expeditionary requirements. Even though they still lag behind U.S. forces in such missions, Europe has the most combat-experienced and capable forces they have fielded in a long time.

Several policy recommendations emerge from this case:

- The EU countries need to expand their commitment to training the Afghan national security forces, particularly the police, and support to the development of the rule of law, in order to ensure the success of the transition plans agreed to at the Lisbon ISAF-Afghanistan Summit.
- Concerted efforts should be undertaken to augment funding and staffing for the EU's crisis response capabilities, including the Civilian Planning and Conduct Capability, and that those capabilities be better integrated with the development of NATO's comprehensive approach and new civilian planning capability to ensure more effective and efficient transatlantic civil-military management of future complex contingencies.
- An EU-NATO security agreement should be concluded to allow for easy exchange of classified information and overcome other operational limitations in the field that are diminishing the security and effectiveness of EU personnel in the field and the success of combined EU-NATO missions. Ad hoc arrangements are no longer adequate.

Given the complexity of the global environment and diverse national interests, common European and American strategic assessments may again prove difficult to attain in various future crises. In such cases, leaders on both sides of the Atlantic should strive to bridge those differences at the outset of a mission by articulating agreed goals and clear divisions of labor.

EU-U.S. RESPONSE TO THE HAITI EARTHQUAKE: A COMPARATIVE ANALYSIS

Erik Brattberg, *Research Assistant, UI*, and
Bengt Sundelius, *Board Member, UI*

Introduction

The recorded incidence of major natural disasters has sharply risen in recent decades, and is predicted to continue to grow in both scope and scale over the years to come. A variety of factors may serve to account for this trend, ranging from the effects of global climate change to environmental degradation to increased population growth and rapid urbanization. Many weak and fragile states are particularly vulnerable to such disasters, lacking adequate emergency response capacities, infrastructure and health services. International assistance is therefore crucial to assist these countries during the immediate phase of major disasters as well as in the long-term by focusing on both building resilience and on reconstruction and development.

Europe and the United States play a critical role toward achieving these goals. The EU and its member states together with the U.S. provide almost two thirds of global humanitarian assistance[44] and play a leading role when it comes to disaster relief, both in terms of supporting the UN-system and in terms of providing resources and personnel at disaster sites. At the same time, transatlantic cooperation on disaster relief is haltering with different polices existing on both sides of the Atlantic as well as within the European Union. Given the significance of the EU and the U.S. within the international donor community, the transatlantic partners must seek to cooperate more effectively during major international disasters. Not only would more effective joint handling of disasters reduce the likelihood of transboundary security threats spreading to the North Atlantic basin, but it would also certainly have a positive impact on the transatlantic relationship more generally.

In order to generate recommendations for how to strengthen transatlantic cooperation in the realm of international disaster relief, this paper will study the EU and U.S. responses to the Haiti earthquake in January 2010. This assessment will allow us to identify common challenges and opportunities. The paper proceeds as follows: first we provide a brief overview of EU and U.S. capabilities in the area of international disaster relief, respectively, before discussing their strategic and operational approaches pertaining to the Haiti disaster. We then discuss the key factors deemed important in influencing the patterns of U.S. and EU responses before moving on to presenting future scenarios for transatlantic cooperation in the area of natural disasters. Finally, we offer some key recommendations for strengthening the transatlantic partnership on disaster response.

Introduction to the Haiti Earthquake and the International Response

Haiti has an extensive history of endemic violence, failed governance, poverty, and devastating natural disasters. For decades, it has ranked as one of the world's poorest countries in almost every category including governance, corruption, standard of living, and life expectancy. Because of the continuous decline in development and investment, Haiti has become highly dependent on foreign aid and security assistance. The UN maintains a peacekeeping force of 9,000 as a part of the United Nations Stabilization Mission in Haiti (MINUSTAH). The Caribbean island state also has a long history of various natural disasters. In 2004 a hurricane struck the northwest part of the country, killing an estimated 3,000 people. And during the 2008 storms, four hurricanes resulted in almost a thousand people being killed and about a million made homeless.

No previous disasters, however, were as destructive as the one in January 2010. On January 12 a massive earthquake struck Port-au-Prince, bringing immense devastation in the already afflicted country. As a result of the first quake and the subsequent aftershocks, poorly constructed buildings in high-risk areas were demolished and critical infrastructure and public services such as electricity, telecommunications, hospitals, schools and government facilities were severely damaged, killing tens of thousands and wounding countless more. In total some 230,000 people are believed to have perished as a result of the earthquake, thus making the earthquake one of the most complex natural disasters to date, even outstripping the wide-spread havoc wreaked by the Asian tsunami in 2004.[45]

The Haitian government declared an emergency situation on January 13, 2010 and requested international assistance. The response to the Haiti disaster from the international community was immediate and reflected the massive scale of destruction. Already after a few days, the aggregated amount of international donations for humanitarian assistance totaled about $160 million.[46] International search and rescue teams began to arrive at the scene within a few days of the earthquake. The UN played a key role, deploying some additional 3,000 peacekeepers, and in activating its humanitarian machinery.[47] The total donations for long and medium term provided by the international community to Haiti reached over $9 billion by February 2010.[48]

Comparison of U.S. and European Commitments

This section will illuminate the convergence and divergence of the U.S. and the EU in terms of the nature and importance of their stakes, interests, strategic goals and operational approaches pertaining to the Haiti disaster; what the U.S. and the EU strategic and operational responsibilities were; and how the "burden/responsibilities sharing" between the two evolved. However, as an important backdrop to these discussions, it serves us well to first briefly account for the EU and U.S. capabilities in the area of international disaster relief.

United States

Organizing for disaster relief

Within the U.S. Agency for International Development (USAID), the chief U.S. agency in charge of international development, the Bureau for Humanitarian Response coordinates the agency's response to overseas emergencies. Additionally, USAID also comprises the Office of U.S. Foreign Disaster Assistance (OFDA) which facilitates and coordinates U.S. emergency response abroad. Besides USAID, the Department of Defense (DoD) also maintains certain responsibilities in foreign disaster relief and

response. Its Office of Peacekeeping and Humanitarian Affairs directs DoD's military response to disasters overseas. To improve civil-military cooperation in humanitarian assistance, the Office of Military Affairs (OMA) is located within USAID. Furthermore, each U.S. regional command harbors USAID staff on secondment.[49] Providing response to disasters overseas is becoming a top priority of the U.S. military, documented for instance, in the 2010 Quadrennial Defense Review (QDR 2010).

Stakes and interests in Haiti

The U.S. has traditionally retained certain responsibilities for assisting its trust and commonwealth territories in the Caribbean and the Pacific Ocean with disaster management. This type of bilateral engagement is considered important to the U.S.'s image in the region, both as a sign of commitment to the Western hemisphere and as a signal to the large Haitian community in the U.S. Furthermore, the earthquake also presented the possibility of massive refugee flows to the U.S. mainland—something the U.S. has already experienced in the past. A considerable Haitian population resides in the U.S. with some 420,000 Haitians living there legally and some additional 30,000 to 125,000 illegally.[50] Finally, the U.S. has commercial stakes in the country. It is both the largest exporter of products to Haiti and the major importing country of Haitian products. About 4,500 U.S. citizens were evacuated from Haiti.[51]

Strategy

It was a strategic objective of President Obama to demonstrate U.S. goodwill to the rest of the world.. A swift and forceful U.S. response would transmit a positive image of solidarity by the U.S. and of the Obama administration to the developing world. Furthermore, Obama clearly had domestic gains to make by responding swiftly and effectively to the disaster. His predecessor George W. Bush was widely criticized for his administration's response in the aftermath of Hurricane Katrina and Obama certainly wanted to avoid repeating the same mistake. Furthermore, the fact that China was the first country to land a search-and-rescue team on Haiti may have also served as a catalyst for the U.S. to quickly demonstrate its commitment.

Resource commitments

In the immediate aftermath of the disaster, on January 13, the U.S. Ambassador to Haiti Kenneth H. Merten declared a disaster due to the effects of the earthquake. The same day President Barack Obama pledged to provide assistance to Haiti, saying that "the people of Haiti will have the full support of the United States in the urgent effort to rescue those trapped beneath the rubble and to deliver the humanitarian relief of food, water and medicine that Haitians will need in the coming days."[52] Secretary of State Hillary Clinton reported that the U.S. would provide military and civilian disaster assistance to affected families.[53] As a result, the United States launched a major civilian and military response to the massive earthquake in Haiti.

The U.S. response to the Haiti disaster was orchestrated by USAID. The U.S. government immediately set up an interagency task force to coordinate and facilitate humanitarian response through the Response Management Team (RMT), headed by USAID and carried out by OFDA.[54] But the military also played a critical role in responding to the disaster, especially in the immediate aftermath of the earthquake, providing security and supplying essentials like medical services and food. In carrying out its humanitarian assistance, the U.S. Southern Command (SOUTHCOM) coordinated its efforts with the State Department and USAID.[55] As of May 2010, the total combined USAID and DoD humanitarian assistance to Haiti amounted to over $1 billion.[56] However, it has been reported that a large amount of this money has yet to be expended.[57] USAID/OFDA provided an initial $50,000

through the U.S. Embassy in Port-au-Prince for the implementation of an instant emergency response program.[58] Within twenty-four hours of the earthquake, the U.S. also began deploying SAR teams to Haiti. On January 14, President Obama announced an additional $100 million in humanitarian assistance to help meet the immediate needs on the ground. Furthermore, USAID declared that it would provide some 14,550 tons of food aid (valued at approximately $18 million) to assist disaster victims.[59]

The U.S. military, under the Joint Task Force Haiti and commanded by SOUTHCOM, responded quickly to the disaster by launching Operation Unified Response. The first U.S. forces arrived at the scene within 24 hours of the earthquake. At the early stage in the relief efforts, the U.S. military helped to provide security for UN personnel in Haiti, supplied medical services and food to the Haitian people, took over certain critical government functions such as controlling the Port-au-Prince airport, clearing the port, maintaining law and order, and worked to promote a workable environment for the international humanitarian community.

Operation Unified Response included personnel from all the military branches. In the first days after the disaster, the U.S. deployed around 13,000 troops. These troops included some 2,200 Marines. On January 21, 2010, additional troops set out for Haiti to take part in the relief efforts, bringing the total number of U.S. personnel involved to more than 16,000. At one point, the total deployment reached as high as 22,268.[60] By May 8, 2010, only some 1,300 U.S. troops remained in Haiti. SOUTHCOM announced that it had drawn back for the most part by the beginning of June 2010, leaving only some 500 National Guard and Reserve in Haiti to serve as aid workers.[61] Besides the Army, the Air Mobility Command (AMC) provided a range of transport aircraft. In total, 264 military aircrafts were sent to Haiti.[62] The Navy was also heavily involved in Operation Unified Response, deploying 23 ships to assist relief efforts. Additionally, the U.S. Coast Guard provided 10 ships to assist with air-life evacuation of U.S. civilian personnel.[63]

Europe and the EU

Organizing for disaster relief

During a crisis occurring outside of the EU, the Community Civil Protection Mechanism may be activated to facilitate cooperation in national civil protection assistance interventions in the event of major emergencies, requiring urgent response actions. The Mechanism has a number of tools intended to facilitate both adequate preparedness as well as effective response to disasters.[64] The operational heart of the Mechanism is the Monitoring and Information Centre (MIC), which monitors all disasters worldwide, activates for emergency assistance and coordinates participating states' assistance. Civil protection now falls under DG ECHO's mandate, which is intended to further strengthen the Union's ability to respond immediately to disasters. In October 2010, Kristalina Georgieva, the ECHO Commissioner announced plans to merge the ECHO and the MIC crisis rooms into a 'European Emergency Response Centre' located inside the Commission.[65] A further envisioned change would be that the Center be given access to pre-committed member state capacities on stand-by for EU operations and pre-committed contingency plans. To date, contributions to the Mechanism from the member states are still voluntary.

Following the so-called Petersberg Tasks, European military units have the authority to engage in "humanitarian and rescue tasks", but have not yet been deployed on strictly humanitarian missions, although military personnel and assets of EU member states are increasingly being used in emergency situations.[66] Given the breadth of experience it has in managing relief and post-conflict stabilization

measures, the Commission has appointed two representatives to the Civil-Military Cell in order to promote coherence between the planning assumptions of the EC and the CFSP measures.[67]

Finally, the main EU instruments for funding disaster preparedness and response, the Instrument for Stability (IfS) and the Development Cooperation Instrument (DCI), also deserve mentioning. Currently, the overall budget of the IfS amounts to €2.06 billion. The IfS consists of two components. The first is a short-term 'crisis response and preparedness' component, providing rapid and flexible funding to prevent conflict, to support post-conflict political stabilisation and to carry out early recovery after natural disasters whereas the second component is more long-term-oriented and is intended for use in more stable contexts.[68] DCI was initiated in 2007 with a budget allocation of about €2.2 billion. The instrument is divided into three components, all with the aim of providing aid to developing countries in post-crisis situations.[69]

Interests and stakes in Haiti

While Europe's economic ties with Haiti are quite limited, some European countries, particularly France, have historically been heavily involved in the country's affairs. The country became independent from France after an uprising in 1804 and French remains the official language of this Caribbean nation. Furthermore, there were roughly 2,700 EU citizens present in Haiti at the time of the earthquake (including Haitians with dual citizenship). Around 1,600 of those were French citizens. The EU also has interests and stakes in the wider region including preventing narcotics trade.

Strategy

Similar to the U.S., the EU also had an interest in displaying a clear presence in the aftermath of the disaster. The Haiti earthquake was the first major international disaster following the adoption of the Lisbon Treaty in December 2009. The Treaty created the new position of High Representative/Vice President for external policy, to which Baroness Catherine Ashton of the UK was appointed. As the new head of the European External Action Service (EEAS), Ashton was given prime responsibility for the Union's response to Haiti. Critical voices in Brussels and in the European capitals expressed concern over the lack of "EU-visibility" and the need for a faster and stronger "EU-response."[70] The new Foreign Policy High Representative was also criticized for responding too late to the disaster and for not visiting the site personally.

Resource commitments

EU member states offered a range of additional assets to support the Haitian government and MINUSTAH, including a military police protection team (UK), "Siroco" and "Batral" logistic ships with amphibious landing capability (France), two military building installations with first aid medical facilities (France), 109 police officers (France), "Cavour" Aircraft Carrier with enhanced hospital on board, engineering task force, 6 helicopters, and force protection elements plus one military police team and one scuba diver team (Italy).[71] Additionally, some EU member states sent personnel to support the UNDAC teams on Haiti. While some member states' response teams arrived at the scene very quickly—some European teams were even amongst the first international teams to reach Haiti—other member states took several days to mobilize key resources. All in all, EU member states made available over 2,000 troops.

On top of the resources provided by many member states, the EU quickly mobilized its funding mechanisms for humanitarian assistance. On January 14, the EU Commission, through ECHO, provided €3 million in fast-track funds for immediate relief, which is the maximum amount the EU

can allocate within 24 hours of an emergency. This funding was used to meet basic needs including shelter and medical assistance and was channeled through international relief organizations. Within a week, the amount of Commission funding for humanitarian assistance had climbed to €30 million, making the total EU support €122 million when factoring in member states' contributions.[72] The total EU financial pledge to Haiti amounted to over €1.2 billion as a part of a long-term reconstruction strategy for Haiti.[73]

Besides providing financial assistance, the EU also quickly activated the civil protection mechanism. Three days after the earthquake, contributions from 17 member states had been coordinated through MIC. Twenty-four European countries (including non EU-members Norway and Iceland) provided assistance through the EU Civil Protection Mechanism. All together, at least 800 EU experts were deployed to Haiti through the Mechanism. To ease coordination, member states were assisted by the set up of a Haiti coordination cell (EUCO) in Brussels at the Joint Situation Centre (Sit Cen) and in Haiti to facilitate coordination and exchange information about the civil and military resources contributed by the member states. There were also inter-service coordination and interaction activities taking place within the Council Secretariat. Some parts of the EU's Rapid Response Capacity were also used for the first time during the emergency in Haiti.[74]

Three EU Civil Protection teams were sent to Haiti to coordinate European assistance, carry out needs assessments and support the international relief efforts. The third team, "Charlies," was responsible for achieving coordination between EU military assets and civilian humanitarian efforts. The civil protection assistance provided by the member states included urban SAR teams, medical teams and supplies, shelter and water sanitation.[75] The EU Civil Protection operation was integrated into the overall UN structure, and the EU Civil Protection teams were based at the UN operations center in Haiti.

At the UN's request, the EU also decided on January 25 to dispatch 260 paramilitary police forces from France, Italy and Spain, drawing mainly on the cooperation within the European Gendarmerie Force (EUROGENDFOR), to assist MINUSTAH. EU Ministers further agreed to provide engineering expertise and a maritime logistical capacity. Evacuation of EU citizens was coordinated by the Spanish Presidency. By January 19, about half of the 2,700 EU nationals in need of evacuation had been brought back to their home countries.

Convergence or Divergence of Efforts?

From the information above we can infer the following. First, the U.S. and EU strategic and operational responsibilities differed widely. While the U.S. swiftly dispatched thousands of troops to assist in restoring order and logistical support, Europe's immediate assistance sought mainly to provide humanitarian assistance using civil means. Both U.S. and EU leaders called for transatlantic cooperation in the relief efforts. According to Clinton, there needed to be a "coordinated, integrated, international response" while Ashton expressed the EU's strong desire to "work closely" with the U.S. and UN in Haiti. Joint action on the ground in Port-au-Prince was apparently limited. In terms of long-term development assistance, Europe has played a significant role, taking the lead together with the U.S. at the international donors conference on Haiti held in New York on March 31, 2010. Furthermore, we can see some indicators of burden/responsibilities sharing between the U.S. and the EU. The U.S.'s strong and rapid military capacity allowed it to provide operational assistance in Haiti. Europe's resources and expertise in the area of humanitarian assistance and reconstruction development made it a major player for the long haul.

Key Factors/Variables Influencing the Outcome

This section analyzes the key factors which influenced the patterns of the U.S. and EU responses to the Haiti earthquake. These include both strategic and operational factors, such as positions of the local stakeholders and the key local conditions of the engagement; internal factors in the U.S. and Europe, such as internal political dynamics; as well as external factors such as the level and the nature of the implication of other global or regional powers, the potential influence of economic issues, etc.

Internal Variables

First, it is important to consider the organizational contexts at the policy levels. Whereas the U.S. approach to disaster relief can broadly be described as inter-agency, the EU's approach is inter-institutional and multi-level. As expected, the EU is therefore more fragmented than the U.S. in this policy area. Furthermore, the prompt U.S. action can be credited to the responsiveness of its political leaders. On the day after the earthquake, President Obama commented on the situation and pledged to provide U.S. assistance. Other top level government representatives, including Secretary of State Hillary Clinton also made commitments along the same lines.

By contrast, responsibilities for responding to international crises in the EU are dispersed among various EU institutions and the 27 member states. A major problem during the Haiti disaster was the apparent lack of political leadership. The new High Representative/Vice President Catherine Ashton did not immediately comment on the event, giving rise to confusion as to who in the EU was in charge. Moreover, tension has historically existed between the Commission's DGs ECHO/Dev and Relex over strategic or operational provisions of emergency assistance during disasters. To strengthen inter-institutional coordination during the Haiti disaster, the EU did set up some new coordination arrangements, which proved helpful.

In the EU, political considerations also include divisions between national and supranational competences. While the member states have traditionally been responsible for handling international relief operations, recent disasters such as the 2004 Indian Ocean Tsunami have highlighted the need for closer EU cooperation and coordination in this area. Recently and in line with the spirit of the Solidarity Clause of the Lisbon Treaty, common and stand-by civilian capacities are slowly being built to be able to enhance the readiness for future internal shocks or external assistance needs. Still, the divisions of judicial and political mandates across the many relevant institutions and between the sovereign member states and the supra-national level remain unresolved.

Another set of organizational considerations in both the U.S. and the EU is civil-military relations at the operational level. Clearly the massive devastation brought about by the Haiti earthquake called for large contingents of both military and civilian relief. A guiding principle when deploying these assets is civil-military coordination. In this area, the U.S. has well-established civil-military links. While the EU also has guidelines and processes for requesting and coordinating the use of military assets in international crises and disasters, some member states are reluctant to employ these assets, taking a more principled stance on humanitarian assistance that favors civil protection mechanisms. Although both the U.S. and European countries have signed the "Oslo Guidelines" for the deployment of military personnel during disasters, there are differences between the U.S. and some EU states as to the interpretation of the "last resort" principle, which states that foreign military assets should be requested only where there is no comparable civilian alternative and where only military assets can meet a crucial humanitarian need.[76]

External Variables

Since the Monroe Doctrine of 1823, the Caribbean has historically been seen as part of a U.S. sphere of influence. In present days, the U.S. retains certain obligations to offer disaster assistance to other neighboring countries in the region. This type of bilateral engagement is considered important to the U.S.'s image in the region, both as a sign of commitment to the Western hemisphere and as a signal to the large Haitian community in the U.S. Thousands of refugees have previously left for the U.S. from Haiti. This record certainly played a role in explaining why the U.S. administration acted with unprecedented force and speed.

Another important external factor is the lack of local capacities in Haiti to respond to the disaster. Already the poorest country in the Western Hemisphere, Haiti has extremely low employment figures and relies heavily on remittances as a primary source of foreign exchange, constituting of nearly a quarter of the country's total GDP. Haiti's infrastructure remains very weak, particularly at the local level, and it proved unable to respond adequately to the earthquake. Lacking its own army and a viable police force, Haiti is also highly reliant on external provisions of security. Finally, Haiti's dependence on the U.S. and the EU is accentuated by its relative isolation in the region. These local factors in combination with the magnitude of the devastation wrought by the earthquake made swift international assistance critical.

Lastly, we can note the importance of effective coordination with the international donor community. The massive relief efforts and the large number of humanitarian actors involved required effective coordination to the response. To promote coordination during the Haiti disaster, a cluster system, organizing the response through 12 clusters and 2 sub-clusters, was introduced. As a result, the humanitarian community was provided support from OCHA on inter-cluster coordination, information management and analysis, mapping, civil-military liaison, donor coordination, advocacy and media outreach. Efforts were also undertaken to ensure strategic coordination from the set up of the Coordination Support Committee (CSC), bringing together the government, MINUSTAH, donors and the humanitarian community, and representatives of the U.S. military.[77]

Scenarios

Based on a conceptual framework of six different "security spheres", we can derive several plausible scenarios for transatlantic cooperation in the area of natural disasters. According to this framework, there are three security domains: the *domestic sphere*, the *international sphere*, and the "*intermestic sphere*" located between these two. Concurrently, in each of these three spheres the U.S. and EU face three sets of objectives: "state security", "societal security", and "human safety." State security refers to the upholding of critical government functions, such as providing for national security, and maintaining law and order. Societal security, which may be described as the level situated between state security and human safety, refers to efforts aimed at enhancing societal "resilience", and could include building effective crisis management capacities and capabilities for governance. Finally, human safety has to do with satisfying the immediate needs of people, such as safeguarding and saving human lives in the event of disasters.

In *domestic* natural disasters, that is disasters occurring within the United States or in Europe, the state security objective has primarily to do with maintaining law and order—a task that could also include the military. Governments also have to ensure societal security through ensuring robust crisis management capacity and the functionality of critical infrastructures. When a disaster strikes in the

country, a central human safety objective is to quickly activate first responders, such as rescue services and public health services. National capacities in the U.S. and the EU for these three objectives are generally quite adequate, although far from perfect as illustrated by Hurricane Katrina. Demand for transatlantic cooperation during domestic disasters is likely to be less intense than in the international sphere, albeit still potentially relevant. One example of a domestic disaster triggering transatlantic assistance is Hurricane Katrina during which several European countries offered various forms of in-kind assistance to U.S. authorities.[78] A possible scenario could include a severe natural disaster occurring in Europe or in North America, exhausting domestic capacities and requiring additional resources from the Atlantic partners.

An additional domain is the *intermestic sphere*, located between and spanning across the international and domestic spheres. The convergence of the international and domestic spheres is especially prevalent in Europe, where, as a result of a process of European integration, individual member states today are highly interdependent. While this high level of mutual interdependence brings many obvious advantages, it also means that when a crisis occurs in one member state, it can easily spill over into another member state. To handle such "transboundary" disasters, European countries have to build capacities in advance to be able to assist one another in acute situations.

The state security objective has to do with upholding the core functions of a sovereign state also under severe external or internal pressures. The societal security objective concerns critical infrastructures and fundamental values that encompass the open and free societies of the EU. In this regard, the "Solidarity Clause" (Article 222) of the Lisbon Treaty will become an important tool in mobilizing collective support in future crises across Europe. Member states should also work jointly through the EU to ensure human safety through civil protection and mutual disaster assistance.

Although characteristically an EU domain, the "intermestic sphere" could also have transatlantic relevance. This is because a more coherent EU policy for embedded societal security would have implications for the security of the United States. Hence, the crafting of multilateral EU-U.S. partnerships in the many complex working areas of societal security would be prudent. The aim could be to transform the existing Atlantic alliance for state security into a Euro-Atlantic community for societal security and human safety. The EU would here be a more appropriate partner for the U.S. than existing NATO structures.

When it comes to natural disasters occurring in the *international sphere*, international assistance is crucial, especially in fragile and resource poor countries. Often there is very little local capacity in terms of emergency response capacities, infrastructure, health services, etc. Disasters may also strike a politically sensitive area, thus making the role of the international assistance much more ambiguous. For example, during the 2004 Indian Ocean Tsunami, which struck several littoral countries, international assistance efforts in Myanmar (Burma) were severely hampered due to the reluctance of that country's government to welcome such assistance. In severe international disasters, the U.S. and EU play key roles in all of the three objectives.

The state security objective of the U.S. and EU may be to contribute with defense capabilities. Military resources may also be used for the societal security objective of strengthening international crisis management capacity. Ensuring democratic governance, functioning critical infrastructures and building resilience —vital elements of the societal security objective in the international sphere —is an area where the EU holds a comparative advantage vis-à-vis the U.S. Both the U.S. and the EU, however, should contribute to human safety through offering international humanitarian assistance, working together and through the UN system. When providing assistance to politically sensitive settings, EU and U.S. efforts may have to be channeled through local organizations in order to be

effective. The EU has an established record of working through non-governmental relief organizations, an approach that seems fitting in many parts of the world.

Lessons of the Haiti Disaster for the Wider EU/U.S. Security Relationship

The United States and Europe have a long tradition of cooperating around traditional national security matters. A growing area of transatlantic cooperation over the next decades will be international crisis management and disaster relief for societal security. The blurring of external and internal security makes it ever more important for the U.S. and Europe to work together toward abating complex emergencies in various types of societies inside the North Atlantic Basin as well as in other parts of the globe. Inadequate handling of severe natural or man-made emergencies in failed and/or post-conflict states could easily spill over into affecting societal security in the trans-Atlantic arena in the forms massive refugee flows, the spread of infectious diseases, or environmental collapse. All of this havoc would be highly dramatized 24/7 on our local news broadcasts, affecting political debate and public sentiments.

Therefore it is pivotal that the EU and the U.S.:

First, consider developing more pre-established agreements built around "lead partner" criteria for different parts of the world. Recognizing that it is impossible to be 'anywhere, anytime', the EU and the U.S. should agree that the U.S. should take a lead in disasters occurring in the Caribbean and Latin America due to its geographical proximity to North America, whereas Europe could assume a leading role in the Balkans and the Mediterranean. Conversely, the transatlantic partners might also reach a burden-sharing agreement whereby the EU would focus on providing civilian assets and long-term reconstruction assistance while the U.S. prioritizes military and rapid response.

Second, explore efforts to link the continental Operation Centers in Washington and Brussels through regular exchanges of situation awareness reports and through interactive training workshops and joint training exercises. Additionally, efforts aimed at exchanging experiences and lessons learned should be explored.

Third, establishing protocols directly between the U.S. and EU Commission, rather than with member states, should be considered to signal U.S. support for EU coordination. While bilateral agreements with individual EU member states remain important, multilateral U.S.-EU agreements is preferred as it would help with limiting policy divergences, both within Europe and between the EU and the U.S. To this end, transatlantic working teams should be established to prepare for common outlooks among relevant officials.

Fourth, the strategic dialogue between USAID and DG ECHO should be expanded to also include other relevant institutions for emergency relief and preparedness, including the U.S. Department of State and the European Commission DG for Development and the new External Action Service.

Fifth, enhancing coordination between the strategic and operational levels of the response should be considered. In particular, ways of strengthening the role of NATO in international disaster relief should be explored. This could, for instance, include revisiting NATO's policy on "Enhanced Practical Cooperation in the Field of International Disaster Relief", which includes two main components: the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), a "24/7" coordination center for disaster relief efforts among NATO member and its partner countries located at NATO headquarters in Brussels; and the Euro-Atlantic Disaster Response Unit (EADRU), a "non-standing, multi-national

mix of national civil and military elements" drawn from EAPC countries and deployable in the event of large-scale disasters.[79]

Finally, the U.S.-EU Summits could be used to frame the overall approach to this effort in the societal security area, as has been done already in other policy sectors of mutual concern. An initiative could be taken to begin the work on a wider approach to transatlantic security than the presently prevailing focus on state security concerns. Building societal security through investments in shared resilience could be an appropriate way forward. It would also not be wrong to announce a Declaration on Transatlantic Solidarity, as a parallel to the Solidarity Clause of the Lisbon Treaty.

THE FIGHT AGAINST PIRACY OFF SOMALIA: A CONSENSUAL BUT ASYMMETRIC ENGAGEMENT

Philippe Gros, *Researcher, FRS*

Main Features of Piracy off Somalia

Powerful Pirate Networks Sharply Increased Their Actions since 2008

The recent renewal of piracy and the threat it represents for the sea lines of communication, vital for global commerce, create a real strategic challenge for the international community. While the struggle against piracy is a concern of nearly all major and various regional powers, the transatlantic partnership plays a leading role in addressing this challenge.

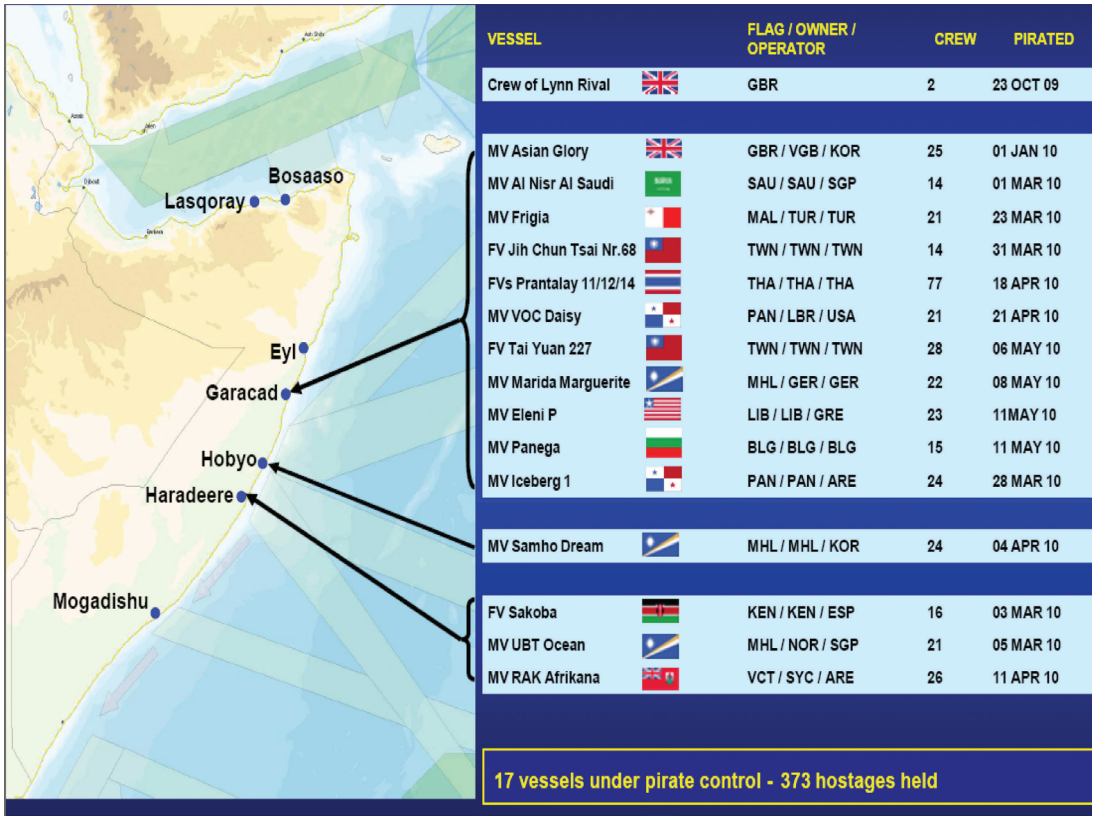
While piracy has been quasi eradicated in the Malacca Strait[80], it has exploded since 2008 in the waters off Somalia, the Gulf of Aden (GoA) and throughout the Indian Ocean[81].

Pirates operate from the coastal villages of Somalia between spring and fall of the year (between the Monsoon periods). While piracy may have stemmed initially from a range of complex factors including poverty and the grievances of the local population against "illegal" foreign shipping, it became the business of criminal networks increasingly structured, powerful and well equipped since 2004.

The oldest piracy cartel operates from Haradeere and Hobyo in the southern Mudug region, but many smaller groups are now spread out along the coast from Bossasso to Kismayo with the most important ones operating from Puntland coast, notably in Garacad.[82,83] A UN report outlines the difference between these networks: "*In contrast with central Somalia, where piracy may be accurately described as a product of statelessness and warlordism* [The Transitional Federal Government (TFG) at Mogadishu, recognized by international community, has a very limited authority]*, in north-eastern Somalia it benefits from the patronage and protection of State institutions.*"[84] The latter is estimated to turn 30 percent of collected ransom to his supporting Puntland authorities. Conversely, the more repressive posture of Somaliland would explain the absence of pirates along its coasts.

Pirates are reportedly well integrated in and supported by their local community whatever the size and organization of the gang[85]. They use to share ransoms between their sponsors and the supporting ground militia with the local community.[86]

EU NAVFOR Intelligence Update: Vessels Held



VESSEL	FLAG / OWNER / OPERATOR	CREW	PIRATED
Crew of Lynn Rival	GBR	2	23 OCT 09
MV Asian Glory	GBR / VGB / KOR	25	01 JAN 10
MV Al Nisr Al Saudi	SAU / SAU / SGP	14	01 MAR 10
MV Frigia	MAL / TUR / TUR	21	23 MAR 10
FV Jih Chun Tsai Nr.68	TWN / TWN / TWN	14	31 MAR 10
FVs Prantalay 11/12/14	THA / THA / THA	77	18 APR 10
MV VOC Daisy	PAN / LBR / USA	21	21 APR 10
FV Tai Yuan 227	TWN / TWN / TWN	28	06 MAY 10
MV Marida Marguerite	MHL / GER / GER	22	08 MAY 10
MV Eleni P	LIB / LIB / GRE	23	11MAY 10
MV Panega	BLG / BLG / BLG	15	11 MAY 10
MV Iceberg 1	PAN / PAN / ARE	24	28 MAR 10
MV Samho Dream	MHL / MHL / KOR	24	04 APR 10
FV Sakoba	KEN / KEN / ESP	16	03 MAR 10
MV UBT Ocean	MHL / NOR / SGP	21	05 MAR 10
MV RAK Afrikana	VCT / SYC / ARE	26	11 APR 10

17 vessels under pirate control - 373 hostages held

Source: Cdr Rune Bratland / Royal Norwegian Navy, Counter-Piracy Operations, Operations Headquarters EUNAVFOR ATALANTA, 10 Jun 2010 [http://www.rederiforeningen.no/publish_files/2_BRATLAND_Operativ_oppdatering_av_situasjonen.pdf].

A Significant Real but Limited Economic Cost

An driving factor in the development of piracy is the perspective of easy gain. The ships, either belonging to the World Food Program, attacked from 2005, or the commercial ones, have a limited crew and are not well defended. Moreover, most companies prefer to negotiate a settlement with pirates to free the crew, the boat, and its load[87]. In 2008, it is estimated that the ransom paid by the ship owners yielded between $30 million and $150 million to pirates.[88]

Moreover, piracy has caused insurance premiums, rise sharply, from $500 per transit in 2007 to $20,000 in 2008. With 20,000 ships transiting through the Gulf of Aden, the total cost amounts to about $400 million.[89] Defense measures such as security guards and deterrence devices cost about $ 80-90,000 per transit.[90] Re-routing the traffic through the Cape of Good Hope is not considered a viable option as it would cost ship owners billions of dollars[91] and would worsen the economic situation of Egypt.

There is no question that piracy has led to additional costs that can not be dismissed. Nevertheless, it is important to note that around 23,000 ships pass the GoA per year with 100 to 150 of them transiting at any given time[92], meaning that pirate activities take 0.2 percent of total traffic per year. Thus, current piracy activities do not yet threaten closure of the sea lines of communication or vital national economic interests.

A Complex Relationship between Pirates and Militant Groups

Relations between local militant groups, notably Al Shahab, and pirate networks are complex. Many observers believe there is no credible evidence of cooperation between these actors who belong to separate clans. Moreover, the Union of Islamic Courts (UIC) which had been toppled by Ethiopian forces in 2007, declared piracy contrary to Islam and has repressed it.[93]

Nevertheless, the more pragmatic issue of access to resources, according to some well-informed sources, may lead pirates and militants to some degree of cooperation: Al Shabab takes benefit from the money obtained by pirates and provide them with some support. One risk of this cooperation is to see some hijacked sailors "transferred" to militant groups as hostages. Other experts point out that terrorists could use the same hijacking tactics as pirates use, but with far more lethal outcomes.[94] The same competition for resources may eventually result in confrontation, as the control of the ports and the transiting flows of goods represent a major stake for local powerbrokers. In May 2010, pirates were threatened by Hizbul Islam militants and evacuated the Haradhere port, themselves driven off of Kismayo port by Al Shabab. A militant spokesman justified the move by the need to suppress anti-Islamic piracy, but also by recent pirate actions which disrupted the traffic of Indian dhows.[95] These boats are used to export goods in some Somali ports before being taxed by militants, while sometimes being hijacked by pirates who use them temporarily as mother-ships.

Increasing Commitment of Naval Forces Led by Europe and the United States

A Wide Political Consensus to Deal with Piracy

One of the most important issues in the struggle against piracy is the constraining political and legal framework. For example, in order to elude the maneuver of coalition warships chasing them, Somali pirates used to take benefit from the 12-mile strip of the territorial sea, which is under the sole sovereign control of the nation under the United Nations Convention on the Law of the Sea (UNCLOS) and the Montego Bay Convention of 1982.

The United Nations Security Council therefore issued in 2008, at the call of the IMO, a series of resolutions under chapter VII of the Charter with the support of the Somali TFG[96].

UNSCR 1814	May 15, 2008	Requested States and regional organizations to escort WFP ships
UNSCR 1816	June 2, 2008	Allowed international forces to operate within Somali territorial sea for six months
UNSCR 1838	October 7, 2008	Requested urgently that States take part in the fight against piracy
UNSCR 1846	December 2, 2008	Extended UNSCR 1816 for 12 months
UNSCR 1851	December 21, 2008	Allowed to wage ground operations in Somalia and engaged the international community to establish a mechanism of coordination

Source: Philippe Gros.

At the political level, and pursuant to UNSCR 1851, stakeholders established a Contact Group on Piracy off the Coast of Somalia (CGPCS) on January 14, 2009 "*to facilitate discussion and coordination of actions among states and organizations to suppress piracy off the coast of Somalia*"[97]. Its working groups manage all the issues related to piracy:

1. Military and Operational Coordination, Information Sharing, and Capacity Building, led by the UK ;
2. Judicial Issues, led by Denmark;
3. Strengthening Shipping Self-Awareness and Other Capabilities, led by the U.S.; and
4. Public Information, led by Egypt.

At the regional level, at the initiative of the IMO, all the African and Arabian coastal countries of the Indian Ocean agreed at Djibouti in January 2009 on a code of conduct (named "Djibouti Code of conduct") to fight against piracy and to create regional coordination and information sharing mechanisms.[98] This agreement is based on the model of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), which has been instrumental in suppressing piracy in the Malacca Strait.

A Strong Naval Deployment with EU, NATO, and U.S. Pillars

Until 2008, a limited number of naval assets operated in the area on national tasking or within the Combined Task Force (CTF)-150, established by U.S. Naval Forces Central Command (USNAVCENT) since February 2002 as a part of Operation Enduring Freedom, to execute counter-terrorism and maritime security operations[99]. From 2007 onward, they were increasingly involved in the prevention of pirate attacks on commercial ships transiting through GoA and the escort of the boats shipping aid of the World Food Program from Mombassa to Mogadishu.[100]

Within a few months, the naval deployments dedicated to counter piracy were expanded considerably:

- The largest counter-piracy's force in the area is now the European naval force (EU-NAVFOR) or TF 465. It carries out Operation Atalata[101] approved in November 2008 by the European Union Council and expanded in June 2010 until December 2012. Its mission is to "provide protection for vessels chartered by the WFP; […] for merchant vessels; and employ the necessary measures, including the use of force, to deter, prevent and intervene in order to bring to an end acts of piracy and armed robbery which may be committed in the areas where they are present."[102] Atalanta is under the operational command of Major General Buster Howes (UK), the Operational Headquarters (OHQ) being located at Northwood. The Force Commander at sea changes every 4 months. The size of the TF 465 may reach ten combatant and supporting ships at one time. It also includes 3 to 5 maritime patrol aircraft.
- The Combined Maritime Force established in January 2009 as a multi-national naval partnership to promote regional stability and security, now oversees CTF-150, as well as a new CTF-151, which deals specifically with counter-piracy, and CTF-152, which supports security and cooperation in the Arabian Gulf. U.S. Vice Admiral William Gortney, CMF commander, explained that "Some navies in [CTF-150] did not have the authority to conduct counter-piracy missions"[103]. CTF-151 is composed of 3 to 5 warships. Its command rotates between coalition participants.
- NATO is also involved in counter-piracy activities. The 2 Standing NATO Maritime Groups (SNMG) executed two short term operations in 2008, before EU involvement. The NATO

presence became permanent with Operation *Ocean Shield*, launched by the North Atlantic Council on 17 August 2009 and which will continue until December 2012.[104] *Ocean Shield* is under the responsibility of the JFC (Joint Force Command) Lisbon and under tactical control of Allied Maritime Component Command (CC-Mar), based at Northwood, UK. The deployed SNMG forms the TF 508 and typically comprises 4-5 frigates.[105]

- Finally, many naval units from many other countries including Malaysia, Russia, China, and India rushed into the area to participate in the counter-piracy operations. Western militaries also have national task forces in the region.

On the whole, the deployment of naval forces dedicated, either totally or partially to counter-piracy operations, may reach more than 30 warships at one time, consisting mainly of destroyers, frigates, corvettes, and amphibious ships as well as about 10 maritime patrol aircraft and some other surveillance assets such as unmanned aerial vehicles.[106] Moreover, many countries had formally deployed security teams aboard their national fishing, WFP or merchant ships.

The operational strategy followed by the international military forces is twofold:

- In the GoA, naval forces patrol, escort ships and exert a deterrent presence. These operations are defensive. CMF established in August 2008 a Maritime Security Patrol Area, complemented in 2009 by an Internationally Recommended Transit Corridor (IRTC) for merchant vessels. "*The aim is to deliver military response to a piracy attack in IRTC within 30 minutes*"[107]. Escort missions are either performed within IRTC through pre-assigned boxes (most EU, NATO or CMF ships), or outside IRTC as performed by several nationally-tasked ships, which is less efficient;
- In the Somali Basin, the naval forces are "*intended to identify and suppress pirate activity.*"[108] These disruption operations are more intelligence-driven and "offensive" in nature. Conversely, civilian ships are not escorted and must thwart aggression themselves. Some intelligence-surveillance and reconnaissance (ISR) assets monitor the Somali coast and a half dozen combat ships in the high seas intercept potential pirate skiffs for investigation. Other ISR assets are used for broader surveillance of the Indian Ocean as pirates expand their area of operations.

All these forces are de-conflicted through the *Shared Awareness and Deconfliction* (SHADE) staff-level meetings held on a monthly basis at Bahrain by CMF and chaired alternatively by CMF, EU-NAVFOR, and NATO.[109] Participating countries share information, offer their capabilities and arrange for patrol slots within the IRTC and other operations[110]. China and India were also increasingly involved in this mechanism.[111]

Coordination between the military forces and civilian shipping entities (World Food Programme (WFP) fishers, ship owners, insurance, etc.), is broadly managed by the CGPCS working group 3, as well as by several other organizations: the EU-led Maritime Security Center Horn of Africa (MSCHOA) established at Northwood with the launch of *Atalanta*[112], the NATO Shipping Center[113], and the UK Maritime Trade Operations (UKMTO)[114]. These structures are intended to maintain a comprehensive picture of maritime traffic, to report incidents, to disseminate best practices for navigation in this area, to dissuade attacks, and to facilitate the sharing of all relevant information.

EU and U.S. Also Pivotal to Implement a Comprehensive Approach toward Somalia

This naval deployment is supposed to be integrated within the so-called "comprehensive approach" to the much larger issues related to the situation in Somalia, including: regional stability, development, or the fight against terrorism. The UN, EU, U.S. and UK are engaged, in cooperation with countries in

the region, notably Ethiopia and Uganda, in a broad range of programs focused on the building of the security sector institutions of TFG, as well as economic development.

Since 2007 the African Union maintains the AMISOM (African Union Mission in Somalia), an 8,000-strong peacekeeping force. The EU has already pledged more than €100 million to support AMISON.[115] The U.S. pledged nearly $350 million over the 2009-2010 period but administration requests for 2011 have decreased to $53 million.[116]

The EU Commission committed another €215.4 million for development aid through the European Development Fund for the period 2008 to 2013. The U.S. has pledged around $30 million per year through such programs as Economic Support Funds (for governance and reconciliation) and other ones for health and more recently economic growth.

For security sector "reform", the EU also pledged €43 million to support the UNDP Rule of Law program mainly responsible for police training and launched a new mission (EUTM Somalia) in April to complement this effort. The main regional supporter of this initiative for police training is Uganda. The U.S. seems to be more focused on the building of national security agencies. Ethiopia focuses on the training of military capabilities and the UK on immigration and intelligence elements.[117]

EU and U.S. Political Commitments Are Asymmetric

The Struggle against Piracy: An "Ideal" EU Commitment

In relative terms, piracy is an important issue for the EU as there is clearly a direct stake for European economy in combating it. The U.S. Department of Transportation observed that "*Over 80 percent of international maritime trade moving through the Gulf of Aden is with Europe.*"[118] Besides, the most important container companies are European ones. The first three companies, APM Maersk (Denmark), MSC-Mediterranean Shipping Co (Swiss) and CMA-CGM Group (France) and the fifth one, Hapag-Lloyd (Germany) own about one-third of shipboard capacity out of the first twenty container companies.[119] The European -owned merchant fleet is more than ten times the size of the U.S. one (in terms of deadweight tonnage), the prominent part of the former being owned by Greece and Germany.[120]

But commercial interests do not completely explain the EU engagement[121]. EU members indeed could have decided to support a NATO operation, given the Alliance experience in terms of naval operations. *Atalanta* is mainly due to France's initiative, as it chaired the EU Council rotating presidency during the second half of 2008, supported by Spain and Greece. French President Sarkozy did see the opportunity to promote and expand the Common Security and Defense Policy, which is a long-standing goal of French foreign policy. A few months earlier, France and Spain initiated UNSCR 1816. France leveraged its partnership with Germany once again, which is often the key to advancing the EU security agenda. The German Navy was already deployed within CTF-150 partnering with the French (French-German Naval Force) and with EUMARFOR, outside of NATO. After an important debate on the legal framework, the German government agreed on *Atalanta.*

The EU agreement to launch *Atalanta* was decisively obtained when the UK decided to support it. Initially, London was reluctant, preferring a more robust NATO engagement in coordination with the EU. But NATO structures were already overstretched with other commitments, particularly in the Balkans and Afghanistan. Moreover, while defending this position, the British were rather isolated, giving up the initiative to other European countries for a maritime engagement, its traditional area of

expertise. Finally, EU members were inclined to give the operational command of *Atalanta* to UK OHQ at Northwood, as German and French OHQs were respectively dealing with EUFOR RD Congo and EUFOR RCA Tchad.[122]

One key rational of the EU engagement is that the struggle against piracy seems to fit perfectly the approach to international security operations of the most reluctant EU members, including Germany. As Lars Erselv Andersen put it from a Danish perspective "*As opposed to the war effort in Iraq and to some extent, in Afghanistan, the war against pirates is seems to be politically uncontroversial, as pirates are universally regarded as bandits of sea* […]." The operation is backed by UNSCRs, enjoys a very large political consensus "*This is therefore seen as international, legitimate and legal military operations*[123]" for politicians, military and strongly supported Danish ship owners. *Atalanta* is clearly an opportunity for a positive commitment. On the eve of German first deployment for Atalanta, Defense Minister Franz Josef Jung said that "*the anti-piracy mission has 'the most robust mandate we have ever had.*"[124] Contributing to reinforce this uncontroversial commitment, its humanitarian achievement is usually put at the forefront of the engagement by officials[125]. As the German Navy spokesman explained "*The main job is to give a safe way to the ships of the World Food Program from and to Somalia […]. Another responsibility is the protection of commercial vessels against pirates. But that comes second in the ranking.*"[126]

The political acceptability of this engagement also explains the commitment of NATO. NATO's operation *Ocean Shield* has complemented or as some contend competed with the EU mission, creating a kind of "maritime beauty contest" between both institutions.[127]

Stakes and Interests Are Less Critical for the United States

The stakes of piracy seem to be not the same in the United States. The Bush administration developed a U.S. national strategy to deal with Somali Piracy in December 2008. The document, entitled *Countering Piracy off the Horn of Africa–Partnership Action Plan*, called for global partnership and supported all the initiatives briefly explained above. Interestingly, it emphasizes that "*the U.S. objective is to repress this piracy as effectively as possible in the interests of the global economy, freedom of navigation, Somalia, and the regional states.*" [128] The document does not identify any direct and specific U.S. interests at stake by piracy. Since then, Secretary Clinton re-emphasized the U.S. commitment and announced some diplomatic and regional engagement initiatives.[129] Nevertheless, the 2010 National Security Strategy does not even mention Somali piracy once. Simply said, it seems that for the U.S., piracy is one concern, among others, associated with the issue of accessing and controlling the "*global commons*" vital for the globalization.

The U.S. would have certainly preferred a more robust commitment of NATO rather than *Atalanta*. But, as the EU operation is under Northwood command, the current situation does not seem to be an issue for Washington.

This relative asymmetry of interests is reflected at the operational level. While U.S. effort is more important than any other nations in this area due to their overwhelming naval capabilities, it spreads along several lines of efforts, including counter-terrorism and security cooperation and is less focused on the struggle against piracy than the European one. As Jonathan Stevenson, a professor at the U.S. Naval College pointed out, "*most naval commanders do not consider the containment of the piracy problem a central military task, seeing it as a distraction from core counterterrorism, counterproliferation, deterrence and war-fighting missions.*"[130] For example, Admiral Mark Fitzgerald, commander of U.S. Naval Forces, Europe and Africa, complained that "*We could put a World War Two fleet of ships out there and we still wouldn't be able to cover the whole ocean.*"[131] The U.S. therefore

welcomes this kind of burden sharing, which provides a text book illustration of the *Global Maritime Partnership* (GMP) concept, a cornerstone of current U.S. maritime strategy[132], as stated recently by Vice Admiral Gortney, head of CMF.[133]

	2007	2008	2009	2010 (until Sept)
Number of Attacks	44	110	217	164
Vessels hijacked		43	47	37
Rate of successful attacks		39 %	22 %	22 %
Crew personnel detained		815	867	As of 11 October, 389

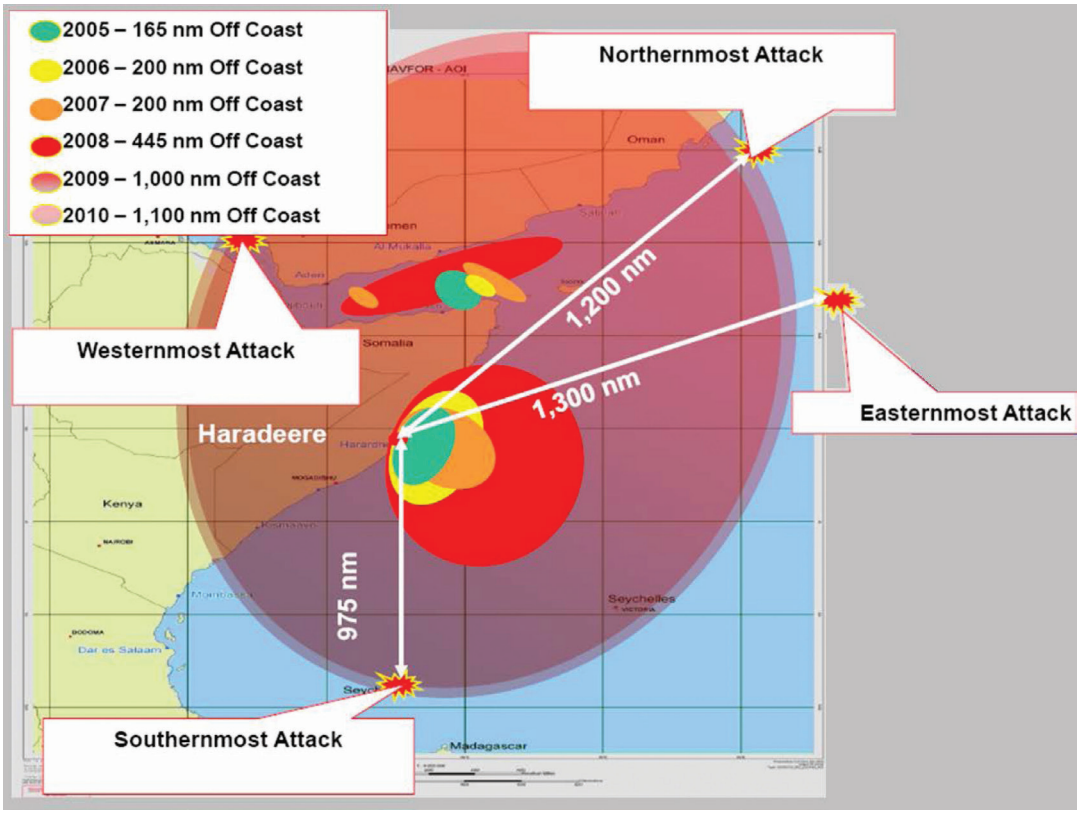
Source: IMB data quoted by Nicolas Gros-Verheyde, «Bilan des opérations anti-piraterie (EUNAVFOR Atalanta, CTF, Otan, Russie). Exclusif», *Bruxelles2 blog*, [http://www.bruxelles2.eu/bilan-des-operations-anti-piraterie-eunavfor-atalanta-ctf-otan-russie-exclusif] and United Nations Security Council *Report of the Secretary-General pursuant to Security Council resolution 1897 (2009)*, S-2010-556, 27 October 2010, 2.

The Current Naval Commitment Achieved Limited Effects

Real and Nondecisive Effects of the International Commitment

The intermediate result of this important international commitment is so far mitigated. The most important achievements are the successful escort of the WFP ships, not one of them being attacked since 2008, and the sharp reduction in the rate of successful pirate attacks, notably in the GoA. Today a ship transiting through the IRTC has a low risk of being hijacked. Instrumental to this result is the combination of the escort by naval forces and the implementation of a range of best practices by maritime vessels, including transit at maximum speed, the use of dissuasive devices and the security teams. CGPCS Working Group 3 chaired by the U.S. developed a Best Management Practices document, implemented on a voluntary basis by at least 18 transportation administrations.[134]

Piracy Expansion



Source: Cdr Rune Bratland / Royal Norwegian Navy, Counter-Piracy Operations, Operations Headquarters EUNAVFOR ATALANTA, 10 Jun 10, [http://www.rederiforeningen.no/publish_files/2_BRATLAND_Operativ_oppdatering_av_situasjonen.pdf].

Meanwhile, the number of attacks continues to increase. Like all complex phenomena, pirate networks have adapted to the international commitment. Gangs from central Somalia have particularly expanded their radius of operations throughout 2009 to the South and East and are able to reach targets at more than 1000 MN from Haraderra. They use mother ships able to deploy several skiffs at once, and more aggressive tactics.[135]

The Enduring Issue of Pirate Prosecution

One of the biggest issues faced by the international community is the management and prosecution of arrested pirates, namely "Persons Under Control" (PUCs).

- While UNCLOS allows states to arrest pirates, it is not applicable within territorial sea of another state.[136] To resolve the issue, UNSCR 1846 encourages states to use the Convention on the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) signed in 1988 after the hijacking of Achille Lauro by PLO terrorists.
- Secondly, several national legal frameworks strictly limit the ability of their national armed forces to execute judiciary operations and/or do not allow them to prosecute pirates without a clear national involvement.[137]
- The various nationalities of ship owners, registrations and crews further complicate prosecution.

It results in a great variety of situations in the handling of PUC, but nearly all of them are handed over by naval forces to local states, notably Kenya, which signed an agreement with the EU, Sechelles, Puntland, Somaliland, and Yemen.[138] After a crisis with Kenya, in April 2009,[139] UN Office on Drugs and Crimes (UNODC) launched a comprehensive Counter-Piracy Program to expand rapidly the police and justice capabilities of these regional actors[140], mainly funded by the European Commission, and supported by the U.S., Canada and Australia, and through a trust fund established by the CGPCS.[141]

Due to these factors, the rate of prosecution of pirates remains very poor. According to an informal count from April 2008 to August 2010, 1,162 pirates have been arrested by naval forces (542 executed by *Atalanta)* with only 493 having been prosecuted (UN reported 528 prosecutions later). It means an average rate of 42 percent, which jumps to 70 percent when arrests are performed by nationally-tasked assets.[142] Hundreds are released due to the lack of evidence and the inability to find a judicial structure to handle them. CGPCS working group as well as UNSC[143] continue to discuss the best legal framework to deal with this issue without clear consensus.[144]

The Range of Possible Futures and the Impact on Transatlantic Partnership

The following prospective exercise is of course not a forecast, but rather a way to consider the range of possible futures. The methodology starts with the identification of the alternative strategic options currently considered in the literature. A second step is to identify some key assumptions and variable factors which could affect the commitment of EU members and the U.S. in the struggle against piracy. The third step is to combine them into plausible scenarios and to draw up some thoughts on their consequence on the transatlantic partnership.

Alternative Options

Nearly all experts and officials explain that the current naval operations to counter piracy while necessary cannot be the decisive solution. Few observers raised doubts on the success of the complementing TFG capacity building effort.

Many of them consider other strategic options to the current one. [145]

- **The emphasis on self-protection of civilian vessels**. This option would limit the naval force commitments and let the ship owners assume a greater responsibility of the protection of their vessels, notably through the employment of private security companies. This option is advocated by many U.S. Commanders including Vice Admiral Gortney and General Petraeus.[146] An increasing number of ship owners (i.e. on U.S. or Spanish vessels) have already turned to this solution. Nevertheless, some associations point to the risk of escalation, the issue of the control over these firms or their lack of further capabilities if a situation were to get worse. Ambassador Chantal Poiret explains that most ship owners and states participating in the CPGCS working groups tend to prefer the use national military detachments rather than private security firms.[147]
- **Constabulary operations within Somali waters**. Advocates of such options argue that military capabilities are not well suited from an operational and legal standpoint and are currently wasted in this effort. A law enforcement approach, implemented by some kind of international collection of coast guards in Somali waters, would be more relevant.[148] Nevertheless, this option would not be decisive and require extensive capabilities to cover all the Somali coastal areas of interest.

- **Counter-piracy ashore**. This option would be to wage ground operations, either military raids to destroy pirate assets, or long-lasting law enforcement operations. The first one would offer tremendous and direct effects to disrupting piracy operations.[149] The U.S.-initiated UNSCR 1851 permits such approaches. But Secretary Gates expressed strong reservations on the ability of U.S. military to undertake such operations.[150] In reality, no one western decision-maker seems to consider seriously a direct engagement of its troops in what could become another fiasco like previous interventions in Somalia. Nevertheless, it seems that many countries have called for more active measures.[151]
- **Regional capacity building for maritime security**. Rand analyst, Peter Chalk, argues that the U.S. should leverage the states involved in the Djibouti Code of Conduct, support their security forces as well as Somali ones through a rapid security cooperation mechanism while alleviating local grievances, which constitutes the root of piracy.[152] But as Lesley Anne Warner points out, "*it is impossible to disaggregate Somalia's problems, whether on land or at sea, from other conflicts in the region, such as the proxy war often fought on Somali soil between Ethiopia and Eritrea, and Ethiopia's internal security concerns in the Ogaden region […] it might be advisable therefore to exclude [Ethiopia and Eritrea] from efforts to build capacity specifically to address instability there.*"[153]
- **Local sub-state capacity building**. Some experts argue that such agreements as the Djibouti Code of Conduct, contrary to the RECAAP in south-east Asia, would fail due to the weakness of TFG.[154] The solution would be to build on engagement already undertaken by international actors with the local "institutions", notably Puntland. Stig Harlen explains that "*Local entities such as Somaliland have so far been the most efficient durable onshore remedy against piracy outside Somalia. Supporting existing local institutions would not require a large military campaign, relevant institutions already have local support and they generally have rudimentary control of their local areas. Local institutions will also have local knowledge and access to local intelligence.*"[155] Supporting such actions, Puntland authorities seem to have hired, with the financial backing of an unnamed Muslim country, the assistance the South-African Saracem private military company to undertake the job.[156]

Most analysts consider that filling the Somali security and governance vacuum requires a comprehensive strategy combining some of these various alternatives.[157]

Drivers Shaping Future Effort against Piracy

Many factors might affect the future of the struggle against piracy. The first task is to distinguish assumptions (enduring factors) and factors which are more variable.

The assumptions for the mid-term

- Security through the GOA will remain in the economic interest of Europeans. At the same time, piracy should not in the near future be able to really disrupt this sea line of communication.
- Most stakeholders remain reluctant to intervene directly on the ground, particularly for enduring operations.
- Somali powerbrokers should continue to use foreign engagements for domestic purposes without adhering to their agenda.

The key variable factors

- The evolution of Somali's political landscape is the key driver of piracy:
  - The most probable option is the perpetuation of a political situation conducive for piracy. As summarized by UN Report, "Southern Somalia remains a patchwork of fiefdoms controlled by rival armed groups—a political and security vacuum in which no side is strong enough to impose its will on the others."[158] Besides, the money piracy injects into the local economy benefits many actors.
  - The other option is the establishment of powerbrokers in Somalia sufficiently strong, at least in coastal area, and hostile to piracy as was the case of the UIC in 2006. Puntland's recent initiatives may be heading in such a direction.
- U.S. policy is probably not fixed because of competing security priorities, a less critical stake than Europe, and the perceived stalemate of such engagement, already highlighted by Secretary Gates and some admirals. Plausible scenarios may include:
  - Maintaining current policy of direct naval engagement combined with support to regional capacity building;
  - A relative disengagement due to economic constraints and/or other maritime security issues: terrorism, piracy elsewhere (i.e. Nigeria), new crisis, etc.;
  - Conversely, in the case of an increased threat emerging from the evolution of the local situation, the temptation of limited operations ashore.
- The level of commitment of "emerging powers." Currently, this commitment is fairly modest. China raised its flag last year. But Chinese Navy (PLAN) seems far from having the capabilities to sustain a more important deployment and this kind of commitment is not one of Beijing's top priorities. India is strategically more concerned and involved as its navy permanently maintains capabilities in the GoA and in the Indian Ocean, increasingly threatened by piracy.[159] In a few years, this commitment may grow, but the Indian limited capabilities may constrain their capacity to take a leading role in anti-piracy efforts.
- Looking at economic factors, there are two scenarios to consider:
  - Current trends continue with rising pressure to limit overseas commitment due to increasing budget constraints given the growing public debt, notably in the in U.S.
  - A new economic crisis breaking in the context of already weak growth. This development could lead to contradictory consequences. On one hand, one could assume that it would lead to important restrictions in deployment, both for EU members and the U.S. On the other hand, it may make piracy less and less tolerable, particularly for Europeans countries that have a significant maritime economic dimension at stake.

Plausible scenarios for the evolution of piracy and the transatlantic relationship

The combination of these drivers and alternative strategic options allows one to consider a range of scenarios having some implications for the coherence or the importance of the transatlantic relationship. These scenarios may include, but are not limited to:

1. Piracy declines due to the progress of strong powerbrokers or local authorities hostile to piracy or having interest in the decline of its networks.

2. The international stakeholders continue the current strategy of containment of piracy within acceptable limits. While not decisive, it may represent for many years the preferred solution as it limits the effects of piracy without intervening on the ground.
3. While piracy continues to increase and spread throughout the Indian Ocean, a broad consensus emerges on the stalemate of naval anti-piracy operations. This direct engagement is sustained but with an increased role of regional states, notably India. The transatlantic partnership increasingly focuses on a more robust indirect approach aiming to improve the security capacity of regional states and local actors.
4. A new economic crisis erupts. In western countries, the support for naval anti-piracy operations crumble but no one wants to operate onshore to dismantle pirate networks. The U.S. decides to disengage from most anti-piracy naval operations and focus its commitment on more pressing security issues. This situation evolves into a diplomatic crisis with EU members, as they remain committed due to their direct economic interests.
5. Some breaking achievements by pirates combine with a political situation in Somalia to create a more pressing perceived threat. The new U.S. administration is inclined to execute limited operations onshore (raids, strikes), opening a new diplomatic crisis with European partners unwilling to commit to this escalation. The crisis also erupts within the EU, between the members definitely reluctant to engage onshore and the ones which agree to join the U.S.-led coalition.

Conclusion

The transatlantic partnership is currently necessary for the present fight against piracy off Somalia, not only for naval anti-piracy operations but also for the broader comprehensive approach to tackle the problem. This case is nevertheless unusual. In this instance the EU as an institution clearly co-lead the effort and, in relative terms, its members commit more resources than the U.S., whose direct interests are less at stake.

An important question is whether this kind of engagement represents a new durable step of CSDP, re-balancing the transatlantic security agenda, or if it is linked to other specific conditions. On one hand, it cannot be overstated that during the last ten years, CSDP has achieved remarkable progress that few considered possible at the end of the 1990's., Moreover, the EU has displayed a clear will to defend its direct economic interests.

On the other hand, it seems that the limited common denominator among various EU members' strategic cultures did not really change. The political perimeter of acceptable security-related engagements remains essentially the same for EU members and different from that governing U.S. actions. Simply put, the fight against piracy, primarily a law enforcement operation with a very limited use of force, undertaken under the umbrella of the consensus of nearly the entire international community, fit perfectly within this political common denominator. That is why we tend to argue that this commitment, and the related transatlantic configuration, does not represent a new era for CSDP but is explained by these specific strategic conditions.

Nevertheless, the current approach, combining naval containment and Somali state security sector building, has not achieved decisive effects so far. Many stakeholders, notably in Europe, may continue to be satisfied with this stance as potentially more effective operations on shore are too risky. However, there are signs that some countries, particularly the United States, may be increasingly reluctant to participate in this enduring stalemate. The struggle against piracy should not reach the top of the list of

transatlantic issues. But alternative strategies, as well as external factors such as the economic situation in our countries could either erode the current transatlantic and EU consensus and/or reduce the critical role of the West as the key axis to find a solution to this issue.

Notes

[1] Stephen Flanagan, Riccardo Alcaro and Philippe Gros provided invaluable suggestions in completing the final draft of this paper.
[2] Riccardo Alcaro is Transatlantic Research Fellow at the Istituto Affari Internazionali (IAI) of Rome and European Foreign and Security Policy Studies (EFSPS) fellow. This paper is part of a broader project funded by different sponsors: the initial phase of the research was made possible by the support of the Compagnia di San Paolo within the framework of the EU-wide EFSPS programme.
[3] For a short overview of EU-Iranian relations, see Sara Kutchesfahani, "Iran's nuclear challenge and European diplomacy" EPC Issue Paper No. 46, March 2006; Walter Posch, "The EU and Iran: a tangled web of negotiations" and Johannes Reissner, "EU-Iran relations: Options for future dialogues", in Walter Posch (ed.), *Iranian Challenges*, Chaillot Paper no. 89, European Union Institute for Security Studies, May 2006.
[4] Shannon Kile, "Final Thoughts on the EU, Iran, and the limits of conditionality", in Shannon Kile (ed.), *Europe and Iran. Perspectives on non-proliferation*, (Oxford University Press, 2005) SIPRI Research Report 21, 122-123.
[5] Volker Perthes, "Of Trust and Security: The Challenge of Iran", in Volker Perthes, Ray Takeyh, Hitoshi Tanaka, *Engaging Iran and building peace in the Persian Gulf region*, A report to the trilateral commission: 62, 2008.
[6] Shannon Kile, "Final Thoughts on the EU, Iran, and the limits of conditionality", in Shannon Kile (ed.), *Europe and Iran. Perspectives on non-proliferation*, (Oxford University Press, 2005) SIPRI Research Report 21, 122-123.
[7] Oliver Thränert, *Ending suspicious nuclear activities in Iran. Discussion of the European Approach*, SWP FG3-Working Paper, November 2004.
[8] For a critical discussion of Europe's leadership in the Iran nuclear dispute, the conclusions of the participants in a round-table organised by the Wisconsin Project on Nuclear Arms in February 2008 are of great interest: see *Iran Watch Roundtable: An assessment of Europe's leadership in confronting the Iranian nuclear challenge*. February 6, 2008, www.wisconsinproject.org/countries/iran/iranwatch-roundtable-eu-0208.htm. The participants in the round-table were Philip Gordon, Hans-Peter Hinrichson, Danielle Pletka, Simon Shercliff, and Terence Taylor.
[9] Eileen Denza, *The EU, Iran, and non-proliferation of nuclear weapons*, «European Foreign Affairs Review», vol. 10, no. 3, 2005, 310-311.
[10] While uranium enrichment remained frozen between late 2003 and January 2006, other related activities – most notably uranium conversion into gas and centrifuge production and testing –continued until November 2004. Uranium conversion was re-activated in August 2005.
[11] The IAEA board resolution that declared Iran in non-compliance with its transparency obligation and hinted at a possible involvement of the Security Council was adopted on September 24, 2005 (GOV/2005/77).
[12] The UN Security Council has adopted six binding resolutions requiring Iran to suspend uranium enrichment and intensify cooperation with the IAEA: UNSCRs 1696 (July 2006); 1737 (December 2006); 1747 (March 2008); 1803 (March 2008); 1835 (September 2008); and 1929 (June 2010). Four such resolutions – 1737, 1747, 1803, and 1929 – have imposed sanctions.
[13] The U.S. also lifted its veto on Iran's application for WTO membership and said it was willing to sell replacement components to Iran for its decrepit airline fleet. On the U.S.'s 2005 change of tack, see Peter Rudolf, *Amerikanische Iranpolitik: Stand, Optionen, Szenarien*, SWP-Aktuell 12, March 2005.
[14] Interview by the author with a former E3 foreign minister (March 2009) and an EU official (June 2010).
[15] For an analysis of the Geneva deal and the potential consequences of its floundering, see Mark Fitzpatrick, *Iran: the fragile promise of the fuel-swap plan*, "Survival", vol. 52, no. 2, June-July 2010.
[16] EU lobbying comprised a confidential letter to secretary Clinton by the new EU High Representative for Foreign Affairs and Security Policy, Catherine Ashton; regular exchanges between the European Commission

and the U.S. administration; and meetings with Congress staffers in which Commission officials highlighted the impact on EU companies of the new law (interview by the author with a European Commission official, June 2010).

[17] Interview by the author with EU officials (June 2010).

[18] UNSCR 1929 was approved on June 9; President Obama signed the Comprehensive Iran Sanctions, Accountability, and Divestment Act into law on July 1; EU sanctions were enacted with EU Council Decision 2010/413/CFSP on July 27, 2010.

[19] An EU official involved in Iran's nuclear dispute since the very beginning described current EU-U.S. cooperation on Iran as "full strategic convergence" (interview by the author, June 2010).

[20] Thousands of reserved cables by U.S. diplomats dealing with Iran, published by WikiLeaks on November 28, 2010, confirm that Obama's prudent but consistent tactics has been a key element to secure support for his sanctions plan (*In Arab world and beyond, deep distress over Iran*, The International Herald Tribune, November 29, 2010, 1 and 4-5.

[21] This conclusion is also drawn from over twenty interviews conducted by this author with E3, EU, and U.S. officials between February 2008 and June 2010.

[22] Alessandro Scheffler provided invaluable suggestions and research assistance in completing the final draft of this paper.

[23] Office of the Special Inspector General for Afghanistan Reconstruction, "U.S. Civilian Uplift In Afghanistan Is Progressing But Some Key Issues Merit Further Examination As Implementation Continues", SIGAR Audit-11-2 Strategy and Oversight/ Civilian Uplift, October 26th 2010, 35. [http://www.sigar.mil/pdf/audits/SIGAR%20Audit-11-2.pdf].

[24] See IMF Country Report No.08/76, "2007 Article IV Consultation," February 2008. [http://proxychi.baremetal.com/csdp.org/research/cr0876.pdf].

[25] Anthony H. Cordesman, "The Afghan War: The Campaign in the Spring of 2010," CSIS, May 23, 2010. [http://csis.org/files/publication/100524_AfghanCampaignMetrics.pdf].

[26] White House Press Release, "What's New in the Strategy for Afghanistan and Pakistan," March 27, 2009. [http://www.whitehouse.gov/the_press_office/Whats-New-in-the-Strategy-for-Afghanistan-and-Pakistan/].

[27] The White House, "Remarks by the President in Address to the Nation on the Way Forward in Afghanistan and Pakistan," December 1, 2009. [http://www.whitehouse.gov/the-press-office/remarks-president-address-nation-way-forward-afghanistan-and-pakistan].

[28] See U.S. Agency for International Development, "Fact Sheet on U.S. Assistance to Afghanistan, FY-2002-7," and FY 2008-10 Congressional Budget Justifications for Foreign Operations. [http://afghanistan.usaid.gov/en/Page.Budget.aspx].

[29] Roundtable with senior U.S. government official, December 7, 2010, Washington. Office of the Special Inspector General for Afghanistan Reconstruction, "U.S. Civilian Uplift in Afghanistan is Progressing But Some Key Issues Merit Further Examination as Implementation Continues," October 26, 2010. [http://www.sigar.mil/pdf/audits/SIGAR%20Audit-11-2.pdf].

[30] Kyle Spector, "Americans barely trust Obama on Afghanistan" July 19, 2010. [http://afpak.foreignpolicy.com/posts/2010/07/19/americans_barely_trust_obama_on_afghanistan]

[31] Secretary of Defense Robert M. Gates' remarks at the NATO Strategic Concept Seminar, National Defense University, Washington, D.C., Tuesday, February 23, 2010. [http://www.defense.gov/speeches/speech.aspx?speechid=1423].

[32] ISAF Placemat, 14 December 2010. [http://www.isaf.nato.int/troop-numbers-and-contributions/index.php].

[33] EU Council Secretariat Factsheet: EU Engagement in Afghanistan. [http://www.consilium.europa.eu/uedocs/cms_data/docs/missionPress/files/100218%20EU%20engagement%20Afghanistan-version5_EN.pdf]. Interview with the EU Special Representative, Washington, October 1, 2010.

[34] European Union, Common Security and Defense Policy, "EU Police Mission in Afghanistan," Updated November 2010. [http://www.consilium.europa.eu/uedocs/cms_data/docs/missionPress/files/101123%20FACTSHEET%20EUPOL%20Afghanistan%20-%20version%2022_EN.pdf].

[35] Pew Global Attitudes Report, 2010.
[36] IFOP, "Les Français et l'intervention militaire en Afghanistan Résultats détaillés July 2010", [http://www.ifop.com/media/poll/1212-1-study_file.pdf].
[37] German Marshall Fund of the United States, "Transatlantic Trends Survey 2010 - Topline Data", .39-42. [http://www.gmfus.org/trends/doc/2010_English_Top.pdf].
[38] Angus Global Reid Monitor, "Opposition to Military Mission in Afghanistan reaches 60 % in Britain", October 20th, 2010. [http://www.angus-reid.com/polls/43408/opposition-to-military-mission-in-afghanistan-reaches-60-in-britain/].
[39] ISAF Placemat, 14 December 2010.
[40] iCasualties.org, Operation Enduring Freedom [http://icasualties.org/oef/].
[41] EU Engagement in Afghanistan Factsheet, March 2009, [http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede250110councileuengagement_/sede250110councileuengagement_en.pdf].
[42] U.S. Foreign Operations Congressional Budget Justifications, 2002-2011. [http://www.state.gov/s/d/rm/rls/cbj/index.htm].
[43] See Stephen Biddle, Fotini Christia, and J Alexander, "Defining Success in Afghanistan" *Foreign Affairs* July/August 2010.
[44] Steets, Julia & Hamilton, Daniel (eds.) *Improving Humanitarian Assistance: A Transatlantic Agenda for Action*, Center for Transatlantic Relations, The Johns Hopkins University/Global Public Policy Institute, 2009, 3.
[45] U.S. Geological Survey website: [http://earthquake.usgs.gov/earthquakes/recenteqsww/Quakes/us2010rja6.php#summary].
[46] The UN OCHA Financial Tracking Service (FTS)
[47] The UN Office for the Coordination of Humanitarian Affairs (OCHA) has estimated 400 different humanitarian actors were present in Haiti by the end of January.
[48] BBC News "UN Haiti donor pledges surpass targets at almost $10bn" [http://news.bbc.co.uk/2/hi/americas/8596080.stm].
[49] Ibid. p.24
[50] BBC News "The long history of troubled ties between Haiti and the United States" [http://news.bbc.co.uk/2/hi/americas/8460185.stm].
[51] CNN "Haiti Earthquake" [http://edition.cnn.com/2010/WORLD/americas/01/19/haiti.updates.tuesday/index.html].
[52] White House, *Remarks by the President on Rescue Efforts in Haiti*, January 13, 2010. [http://www.whitehouse.gov/the-press-office/remarks-president-rescue-efforts-haiti].
[53] Department of State, *Remarks by the Secretary of State on the situation on Haiti*, 13 January 2010. [http://www.state.gov/secretary/rm/2010/01/135144.htm].
[54] CRS brief, *Haiti earthquake: crisis and response*, February 2, 2010. [http://www.fas.org/sgp/crs/row/R41023.pdf].
[55] Globalsecurity.org website – Operation Unified Response: [http://www.globalsecurity.org/military/ops/unified-response.htm].
[56] USAID factsheet number 53 – Haiti earthquake, May 7, 2010. [http://www.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/countries/haiti/template/fs_sr/fy2010/haiti_eq_fs53_05-07-2010.pdf].
[57] The Washington Post, "Another obstacle stalls $1.15B in US aid" [http://www.washingtonpost.com/wp-dyn/content/article/2010/11/04/AR2010110406378.html].
[58] USAID factsheet number 1 – Haiti earthquake, 13 January 2010. [http://www.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/countries/haiti/template/fs_sr/fy2010/haiti_eq_fs01_01-13-2010.pdf].
[59] USAID website – USAID to Provide Emergency Food Aid for Haiti Earthquake Victims, January 13, 2010. [http://www.usaid.gov/press/releases/2010/pr100113.html].
[60] SOUTHCOM – Operation Unified Response. [http://www.southcom.mil/appssc/factFilesLarge.php?id=138]

[61] Boston Globe, "U.S. military operation in Haiti draws to close" [http://www.boston.com/news/nation/washington/articles/2010/04/19/us_military_operation_in_haiti_draws_to_close/].
[62] SOUTHCOM op.cit.
[63] Ibid.
[64] See European Civil Protection website [http://ec.europa.eu/echo/civil_protection/civil/prote/mechanism.htm]
[65] Speech by EU Commissioner Kristalina Georgieva: "Creating a European Disaster Response Capacity", Brussels 28 October 2010. [http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/606&format=HTML&aged=0&language=EN&guiLanguage=en]
[66] Julia Steets & Daniel Hamilton (eds.) "Humanitarian Assistance: Improving U.S.-European Cooperation" The Johns Hopkins University, Center for Transatlantic Relations, 2009.
[67] Commission Communication - Reinforcing EU Disaster and Crisis Response in third countries [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0153:EN:HTML]
[68] European Commission, Europe Aid Developments and Cooperation, "How We Finance". [http://ec.europa.eu/europeaid/how/finance/index_en.htm]
[69] European Commission, Europe Aid Developments and Cooperation, "Development Co-operation Instrument (DCI)" [http://ec.europa.eu/europeaid/how/finance/dci_en.htm]
[70] Mark Rhinard and Arjen Boin, "Relief effort reveals some uncomfortable truths", *European Voice,* 28 January 2010. See also, Bruno Waterfield, "Lady Ashton under fire over "EU visibility", *The Telegraph*, 22 January 2010.
[71] EU fact sheets on Haiti, 28 January 2010 [http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/22&format=HTML&aged=0&language=EN&guiLanguage=en#footnote-8].
[72] [72] European Commission, Europe Aid Developments and Cooperation, "Haiti Earth Quake" [http://ec.europa.eu/echo/aid/caribbean_pacific/haiti_earthquake_en.htm].
[73] This sum comprises the pledges of 18 member states, the Commission and the European Investment Bank. Out of this money the European Commission pledged €460 million.
[74] EU Focus newsletter: EU Emergency Assistance: Humanitarian Aid and Disaster Response, May 2010 [http://www.eurunion.org/eu/images/eufocus-humaid-may2010.pdf].
[75] European Commission, Humanitarian Aid and Civil Protection, "Preparatory Action on an EU rapid response capability - 2008" [http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/haiti_2010.pdf].
[76] Wiharta, Sharon et al. *The Effectiveness of Foreign Military Assets in Natural Disaster Response*, (Solna: SIPRI, 2008), 21.
[77] Response to the Humanitarian Crisis In Haiti: Achievements, Challenges and Lessons To Be Learned, Inter-Agency Standing Committee.
[78] See Mark Rhinard and Bengt Sundelius, "Crisis Management in an Age of Globalisation," E2010
[79] "Enhanced Practical Cooperation in the Field of International Disaster Relief," Fact Sheet, Euro-Atlantic Disaster Response Coordination Centre [http://www.nato.int/eadrcc/fact.htm].
[80] Martin N. Murphy, "Solving Somalia", *Proceedings*, United States Naval Institute, July 2010, 30-35.
[81] See piracy map of the International Chamber of Commerce [http://www.icc-ccs.org]
[82] United Nations Security Council, *Report of the Secretary-General pursuant to Security Council resolution 1846 (2008)*, S/2009/146, 16 March 2009, p.2.
[83] Peter Chalk (RAND Corporation) "Piracy Off the Horn of Africa: Scope, Dimensions, Causes and Responses" *Brown Journal of World Affairs,* Spring/Summer 2010, Volume XVI, Issue II, 91-92, [http://www.relooney.info/0_New_7595.pdf].
[84] United Nations Security Council, *Report of the Secretary-General pursuant to Security Council resolution 1853 (2008)*, S/2010/91, 10 March 2010, 39.
[85] Peter Chalk (RAND Corporation) "Piracy Off the Horn of Africa: Scope, Dimensions, Causes and Responses" *Brown Journal of World Affairs,* Spring/Summer 2010, Volume XVI, Issue II [http://www.relooney.info/0_New_7595.pdf].

[86] United Nations Security Council, *Report of the Monitoring Group on Somalia pursuant to Security Council resolution 1811 (2008)*, S/2008/769, 10 December 2008, p.31 [http://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/2008/769&Lang=E&Area=UNDOC].
[87] Peter Chalk, (RAND Corporation) "Piracy Off the Horn of Africa: Scope, Dimensions, Causes and Responses" *Brown Journal of World Affairs,* Spring/Summer 2010, Volume XVI, Issue II, 95, [http://www.relooney.info/0_New_7595.pdf].
[88] Peter Chalk, (RAND Corporation) "Piracy Off the Horn of Africa: Scope, Dimensions, Causes and Responses" *Brown Journal of World Affairs,* Spring/Summer 2010, Volume XVI, Issue II [http://www.relooney.info/0_New_7595.pdf].
[89] Osler D, The Long way around, *Lloyd's List*, 26 November 2008, quoted in United Nations Conference On Trade And Development, *Review of Maritime Transport, 2009*, Report by the UNCTAD secretariat, pp. 10-11 [http://www.unctad.org/en/docs/rmt2009_en.pdf].
[90] Prof. Gustaaf de Monie, Policy Research Corporation (PRC), Economic consequences of piracy and Armed Robbery on Shipping, European Commission Seminar Piracy And Armed Robbery Against Shipping, Brussels 21 January 2009 [http://ec.europa.eu/transport/maritime/events/doc/2009_01_21_piracy/critical_demonie.pdf].
[91] ibid.
[92] Commodore Per Bigum Christensen Royal Danish Navy, *Task Force 150 anti-piracy operations*, 2009 MARLO Maritime Conference, Dubai, 25 January 2009 [http://www.cusnc.navy.mil/marlo/Events/MARLO-2009%20DubaiConference.htm].
[93] Clive Schoefield, "Floating Treasure," *Professional Yachtsmen Association News*, n°17, 2009-2010, p.12 [http://www.pya.org/wp-includes/pdf/pya-news-17.pdf] See also Scott Baladauf, "Piracy Raises Pressure for New International Tack on Somalia," *Christian Science Monitor,* 6 January 2009, [http://www.csmonitor.com/World/Africa/2009/0106/p12s01-woaf.html].
[94] Julie Cohn, *Somalia: Terrorism Heaven*, Backgrounder, Council for Foreign Relations, update 10 June 2010 [http://www.cfr.org/publication/9366/terrorism_havens.html].
[95] Nick Wadhams, "Somali Pirates vs. Islamists: A Dispute Over Business", *Time/CNN, May. 07, 2010,* [http://www.time.com/time/world/article/0,8599,1987855,00.html].
[96] The text of all these resolutions as well as key EU text are available on the website of the European Council: [http://www.consilium.europa.eu/showpage.aspx?id=1519&lang=EN].
[97] *Contact Group on Piracy off the Coast of Somalia*, New York, January 14, 2009 [http://www.marad.dot.gov/documents/Establishment_of_CGPCS_1-14-2009.pdf].
[98] Djibouti Code of Conduct, Record of the Meeting, 29 January 2009, [http://www.fco.gov.uk/resources/en/pdf/pdf9/piracy-djibouti-meeting].
[99] Combined Maritime Forces, Combined Task Force (CTF) 150 [http://www.cusnc.navy.mil/cmf/150/index.html].
[100] Véronique Sartini, "Entretien avec le vice-amiral Gérard Valin, commandant des forces maritimes françaises de l'océan Indien (Alindien)", *DSI* n°39, juillet-août 2008, p.73.
[101] Council Joint Action 2008-851-CFSP of 10 November 2008 on a European Union military operation to contribute to the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:301:0033:0037:EN:PDF].
[102] Council of the European Union, *EU naval operation against piracy (EUNAVFOR Somalia - Operation ATALANTA) Fact Sheet*, Updated July 2010, [http://www.consilium.europa.eu/uedocs/cms_data/docs/missionPress/files/100713%20Factsheet%].
[103] Cmdr. James Kraska and Capt. Brian Wilson, "Fighting piracy, International coordination is key to countering modern-day freebooters", *Armed Forces Jounal*, February 2009, [http://www.armedforcesjournal.com/2009/02/3928962].
[104] Capt Tom Tulloch (CAN N), Maritime Command Northwood, Current Operations Briefing to NMIOTC Annual Conference, 30 June 2010, [http://www.hellenicnavy.gr/nmiotc/files/AnnualConference2010/Presentations/2/Current%20Operations%20(Capt%20Tom%20Tulloch%20CC%20MAR%20NORTHWOOD).ppt].

[105] Fact Sheet – Counter-Piracy: Operation Ocean Shield, Public Diplomacy Division, NATO HQ Brussels, January 2010, [http://www.nato.int/nato_static/assets/pdf/pdf_2010_01/20100204_20100128-Fact_Sheet_Counterpiracy.pdf].
[106] Loren Ploch et alii, *Piracy off the Horn of Africa*, Congressional Research Service, April 19th 2010, p.30, [http://fpc.state.gov/documents/organization/142669.pdf].
[107] Capt McGuire, RAN, Director Plans Combined Maritime Force*, Combined Maritime Forces, Who We Are and Wider Military Counter Piracy Update*, MARLO Conference, 13 December 2009, [http://www.cusnc.navy.mil/marlo/Events/DEC-MARLO-DubaiConference_files-2009/CAPT%20McGuire.ppt].
[108] *Ibid*.
[109] Paul Ridgway, "NATO chairs counter piracy meeting in Bahrain", *Ports & Ships Maritime News*, June 3, 2010, [http://ports.co.za/news/article_2010_06_2_1103.html].
[110] Cdr Alastair Clark RN CMF ACOS (OPS), *Combined Maritime Forces (CMF) Operations Counter Piracy Operations, Challenges, Shortfalls and Lessons Learned*, Presentation, 4 June 2009 [http://www.nato.int/structur/AC/141/pdf/PS-M/Combined%20Maritime%20Forces%20Ops.pdf].
[111] Devirupa Mitra, "EU asks India to co-chair anti-piracy group", *Headlines India*, July 13, 2010, [http://headlinesindia.mapsofindia.com/india-and-world/european-union/eu-asks-india-to-cochair-antipiracy-group-55987.html].
[112] Capt Richard Farrington, RN, *EU NAVFOR Mission Brief and Operational Update*, Presentation, 19 May 2009, [http://www.powershow.com/view/264d54-ZDIwM/EUNAVFOR].
[113] Background NATO Shipping Centre, July 2009 http://www.shipping.nato.int/NATOShippi/1233054946
[114] UKMTO Dubai of the MSCHOA website: [http://www.mschoa.org/Links/Pages/UKMTO.aspx].
[115] For EU data of this section, see EU Council Secretariat Factsheet , *EU Engagement in Somalia*, April 2010, [http://www.consilium.europa.eu/uedocs/cms_data/docs/missionPress/files/100407%20FACTSHEET%20EU%20ENGAGEMENT%20SOMALIA%20-%20version%208_EN01.pdf].
[116] For U.S. data of this section, see Department of State, Congressional Budget Justification, Foreign Operations, FY 2011, Annex: Regional Perspectives, [http://www.usaid.gov/policy/budget/cbj2011/2011_CBJ_Annex.pdf].
[117] See United Nations Security Council, S/2008/769, *op cit*.
[118] U.S. Department of Transportation, Economic Impact of Piracy in the Gulf of Aden on Global Trade, December 2008, [http://www.marad.dot.gov/documents/HOA_Economic%20Impact%20of%20Piracy.pdf].
[119] United Nations Conference On Trade And Development, *Review of Maritime Transport, 2009*, op cit, p.100
[120] Ibid., Table 12, p.53.
[121] Basil Germond and Michael E. Smith, "Re-Thinking European Security Interests and the ESDP: Explaining the EU's Anti-Piracy Operation," *Contemporary Security Policy* 30, no. 3 (2009), p. 573–93.
[122] Frank Hagemann, *Strategic Planning for Comprehensive Security in the European Union's Military Operations: EUFOR RD Congo, EUFOR Tchad/RCA, and EUNAVFOR Somalia*, Master's Thesis, Naval Postgraduate School, June 2010, p. 59-66 [http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA524653].
[123] Lars Erselv Andersen, "Piracy in the Gulf of Aden, Reflections on the Concepts of Piracy and Order", in Danish Insitute for International Studies, *Danish Foreign Policy Yearbook 2009*, 80 [http://www.diis.dk/graphics/Publications/Books2009/Yearbook2009/Yearbook_2009_web_Erslev_Andersen.pdf].
[124] AP, "German frigate begins anti-piracy patrols in Somalia", GMA News TV, 31/12/2008, [http://www.gmanews.tv/story/140902/German-frigate-begins-anti-piracy-patrols-in-Somalia].
[125] *Annual report from the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament on the main aspects and basic choices of the CFSP – 2009*, 46, [http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/EN_PESC%202009_web.pdf].
[126] Interview with Navy Press Officer Christoph Kohlmorgen, "Germany steps up battle against piracy in Gulf of Aden", *Deutsche Welle*, 13.01.2010, [http://www.dw-world.de/dw/article/0,,5122313,00.html].
[127] Bjoern H. Seibert, "When great powers compete, the pirates win", *The Argument Blog*, March 30, 2009, [http://experts.foreignpolicy.com/posts/2009/03/30/when_great_powers_compete_the_pirates_win].

[128] United States National Security Council, *Countering Piracy Off The Horn of Africa – Partnership Action Plan*, December 2008, 6 [http://www.marad.dot.gov/documents/Countering_Piracy_Off_The_Horn_of_Africa_-_Partnership__Action_Plan.pdf].
[129] Hillary Rodham Clinton, Secretary of State, *Announcement of Counter-Piracy Initiatives*, Washington, DC, April 15, 2009, [http://www.state.gov/secretary/rm/2009a/04/121758.htm].
[130] Jonathan Stevenson, "Jihad and Piracy in Somalia," *Survival,* vol. 52, no. 1, February–March 2010, 31.
[131] Adam Entous, "U.S. Admiral: military ships can't stop Somali Piracy", *Reuters* April 16, 2010
[132] ADM Gary Roughead, GEN James T. Conway, ADM Thad W. Allen, *Naval Operations Concept 2010, Implementing the Maritime Strategy*, p.97, [www.navy.mil/maritime/noc/NOC2010.pdf].
[133] VADM William Gortney, *Global Maritime Partnership*, Brief to the Middle East Naval Commanders Conference, 30 March 2010, [http://www.rusiqatar.org/attach/VADM%20WILLIAM%20GORTNEY_Global%20Maritime%20Partnership_ENGLISH.pdf].
[134] 469 Sixth Plenary Meeting of the Contact Group On Piracy Off The Coast of Somalia, 14 June 2010, [http://www.icpat.org/index.php/events-archive-mainmenu-81/469-sixth-plenary-meeting-of-the-contact-group-on-piracy-off-the-coast-of-somalia].
[135] Capt McGuire, RAN, Director Plans Combined Maritime Force*, Combined Maritime Forces, Who We Are and Wider Military Counter Piracy Update*, MARLO Conference, 13 December 2009, [http://www.cusnc.navy.mil/marlo/Events/DEC-MARLO-DubaiConference_files-2009/CAPT%20McGuire.ppt].
[136] "Article 105, Seizure of a pirate ship or aircraft", *United Nations Convention on the Law of the Sea of 10 December 1982*, [http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf].
[137] M. Christian Ménard, *Rapport d'information déposé par la commission de la défense nationale et des forces armées sur la piraterie maritime*, n° 1670, 13 mai 2009, pp. 36-38, or Anonymous, *Prosecution of acts of piracy off Somalia by German prosecution authorities*, May 2009, [http://www.iflos.org/media/34039/brandt%20statement%20piracy%20maritime%20talks%202009.pdf] or Oliver Hawkins, "What to do with a captured pirate", *BBC News*, 2009/03/10 [http://news.bbc.co.uk/go/pr/fr/-/2/hi/in_depth/7932205.stm].
[138] United Nations Security Council, *S/2010/394*, 26 July 2010, p.14, [http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Somalia%20S2010%20394.pdf].
[139] "Kenya To Stop Prosecuting Somali Pirates Captured", *RTT News*, 1 April 2010, [http://www.rttnews.com/Content/GeneralNews.aspx?Id=1259094&SM=1].
[140] United Nations Office on Drugs and Crime, *Counter Piracy Programme*, November 2009, [http://www.unodc.org/documents/easternafrica//piracy/UNODC_Counter_Piracy_Programme.pdf].
[141] Sixth Plenary Meeting of the Contact Group On Piracy Off The Coast of Somalia, 14 June 2010, [http://www.icpat.org/index.php/events-archive-mainmenu-81/469-sixth-plenary-meeting-of-the-contact-group-on-piracy-off-the-coast-of-somalia].
[142] Nicolas Gros-Verheyde, « Bilan des opérations anti-piraterie (EUNAVFOR *Atalanta*, CTF, Otan, Russie). Exclusif », *Bruxelles2 blog*, [http://www.bruxelles2.eu/bilan-des-operations-anti-piraterie-eunavfor-atalanta-ctf-otan-russie-exclusif].
[143] United Nations Security Council, S/2010/394, 26 July 2010, [http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Somalia%20S2010%20394.pdf].
[144] United Nations Security Council, *Security Council Stresses Long-Term Solution Needed to Problem of Prosecuting, Imprisoning Pirates Operating off Somalia Coast, Welcomes Report on Issue, Secretary-General Presents Report with 7 Legal Options; Range from Enhanced UN Assistance for Ongoing State Efforts, to Establishment of International Tribunal*, SC 10014, 25 August 2010, [http://www.un.org/News/Press/docs/2010/sc10014.doc.htm].
[145] Cmdr John Patch (USN, Ret), "How Does this End", *Proceedings*, United States Naval Institute, July 2010, pp. 16-17 , See also Lesley Anne Warner, "Pieces of Eight, An Appraisal of U.S. Counterpiracy Options in the Horn

of Africa", *Naval War College Review*, Spring 2010, Vol. 63, No. 2, 61-87, [http://www.usnwc.edu/getattachment/7eaf3023-526f-4d34-ae81-5233dc8694b1/Pieces-of-Eight--An-Appraisal-of-U-S--Counterpirac].

[146] Christopher Spearin, A Private Security Solution to Somali Piracy: The U.S. Call for Private Security Engagement and the Implications for Canada, *Naval War College Review*, Autumn 2010, Vol. 63, No. 4, pp 56-71, [http://www.usnwc.edu/getattachment/c6f939ef-5695-4ed8-bf0a-14fd1ebe29f6/A-Private-Security-Solution-to-Somali-Piracy--The-].

[147] See *La piraterie maritime : menace stratégique ou épiphénomène ?*, Journée d'étude du lundi 7 décembre 2009, acte de colloque, Fondation pour la recherche stratégique, 40, 82, [http://www.frstrategie.org/barreFRS/publications/colloques/20091207.pdf].

[148] Cmdr John Patch (USN, Ret), "Send the Warship Home", *Armed Forces Journal*, April 2010, [http://www.armedforcesjournal.com/2010/04/4537286].

[149] Milan Vego, *Counter-Piracy: An Operational Perspective*, Reprinted from *Tidskrift i Sjöväsendet* Issue 3 2009, 169-180, [http://www.koms.se/ul_pdf/382_Vego.pdf].

[150]Camilla Hall, Gates Calls for Action Against Somali Pirates (Update1), *Bloomberg*, Dec 13, 2008 [http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1m817na3YFo].

[151] Elizabeth Dickinson, "The secret Somalia anti-piracy force", *The Argument blog*, 2 December 2010, [http://blog.foreignpolicy.com/posts/2010/12/02/the_secret_somalia_anti_piracy_force].

[152] Peter Chalk (RAND Corporation) *op cit*.

[153] Lesley Anne Warner, op cit., 77-78.

[154] Martin N. Murphy, "Solving Somalia" U.S. Naval Institute, *Proceedings Magazine* - Vol. 136 (July 2010): p. 1, 289. [http://www.usni.org/magazines/proceedings/2010-07/solving-somalia].

[155] Stig Jarle Hansen, P*iracy in the greater Gulf of Aden. Myths, Misconceptions and Remedies*, Norwegian Institute for Urban and Regional Research, October 2009, 56-57, [http://www.nibr.no/uploads/publications/26b0226ad4177819779c2805e91c670d.pdf].

[156] Katharine Houreld, "1,000-man militia being trained in north Somalia", *The Associated Press*, 1 December 2010 [http://www.washingtonpost.com/wp-dyn/content/article/2010/12/01/AR2010120103290_pf.html] and "Somalia: Puntland pres meets Kuwait emir, defends anti-piracy force", *Garowe Online*, December 3 2010, [http://www.garoweonline.com/artman2/publish/Somalia_27/Somalia_Puntland_pres_meets_Kuwait_emir_defends_anti-piracy_force.shtml].

[157] Also Lesley Anne Warner, *op cit*.

[158] United Nations Security Council, S/2010/91, p.6 [http://www.un.org/ga/search/view_doc.asp?symbol=S/2010/91].

[159] See anti-piracy operations page of the Indian Navy: [http://indiannavy.nic.in/AntiPiracy.htm].

RESEARCH TEAM

Istituto Affari Internazionali

Riccardo Alcaro, Valerio Briani, Jean-Pierre Darnis, Federica Di Camillo, Ettore Greco, Alessandro Marrone, Sandra Mezzadri, Valérie Miranda, Nicolò Sartori, Stefano Silvestri, Anna Veclani

Swedish Institute of International Affairs

Jan Joel Andersson, Erik Brattberg, Mark Rhinard, Bengt Sundelius

Fondation pour la Recherche Stratégique

Yves Boyer, Jean-François Daguzan, Philippe Gros, Camille Grand, Hélène Masson, Lucia Marta, Elisande Nexon

Center for Strategic and International Studies

Guy Ben-Ari, David Berteau, Ben Bodurian, Michael Cass-Anthony, T.J. Cipoletti, Heather Conley, Stephen Flanagan, Priscilla Hermann, Manuel Lafont-Rapnouil, Rick "Ozzie" Nelson, Amanda Tuninetti