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

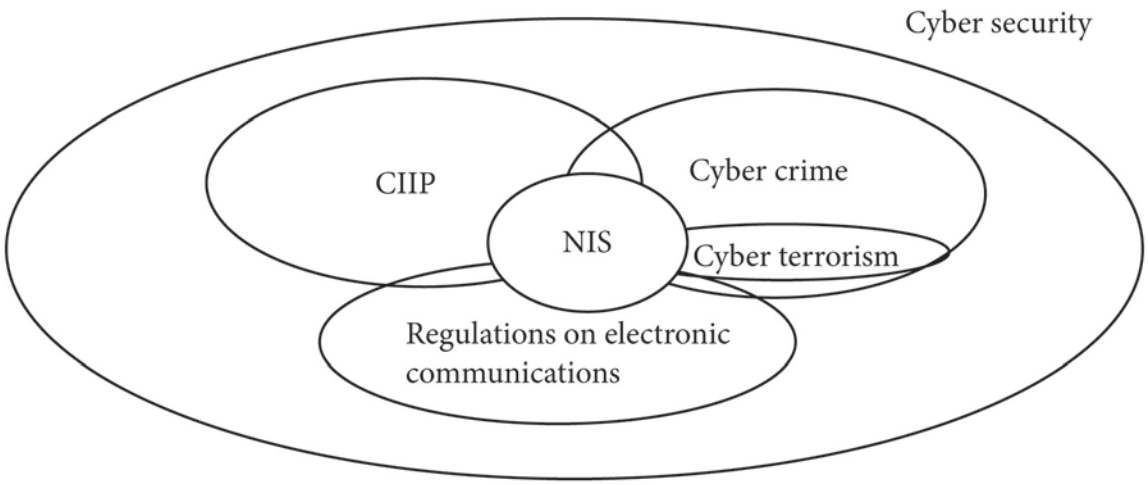
Document	Main Cyber References	Defintions	Expectations
A Secure Europe in a Better World: European Security Strategy (2003)	[…] European dependence on an interconnected infrastructure […] in information […]	//	//
	[…] terrorist movements are well-resourced, connected by electronic networks	//	//
Report 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.

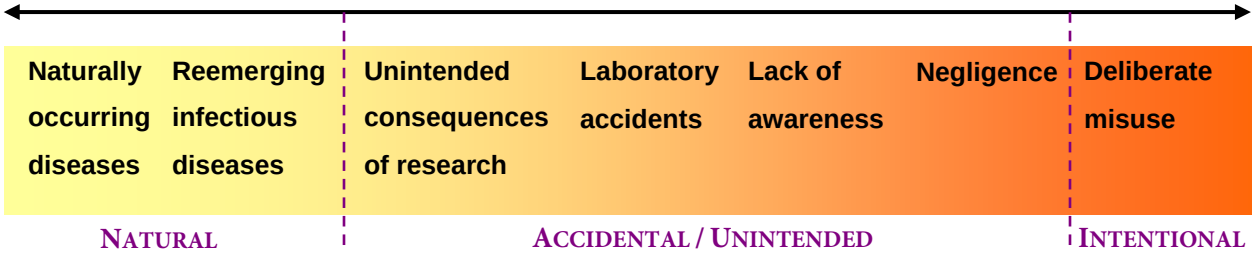
Reducing the risks can be achieved through a full range of options, such as adopting national legislation and regulations, strengthening the Biological and Toxins Weapons Convention and promoting UN Security Council Resolution 1540 (2004), engaging in outreach and cooperation activities, or providing 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.