



# **New Information and Intelligence Needs in the 21<sup>st</sup> Century Threat Environment**

THE HENRY L. STIMSON CENTER  
SEPTEMBER 2008

REPORT NO. 70

Copyright © 2008  
The Henry L. Stimson Center  
1111 19<sup>th</sup> Street, NW  
12<sup>th</sup> Floor  
Washington, DC 20036

Telephone: 202-223-5956  
Fax: 202-238-9604

[www.stimson.org](http://www.stimson.org)  
email: [info@stimson.org](mailto:info@stimson.org)

# TABLE OF CONTENTS

|   |           |
|---|-----------|
| Preface.....  | 3         |
| <b>CHAPTER 1: THE PROBLEM.....</b>  | <b>5</b>  |
| Traditional Intelligence Cycle .....  | 7         |
| Evolving Intelligence Cycle .....   | 8         |
| <b>CHAPTER 2: THE CURRENT SYSTEMS .....</b>   | <b>9</b>  |
| The US Perspective .....  | 9         |
| US Systems.....   | 10        |
| Chart: Information Sharing and Disease Surveillance Systems in the US .....                     | 13        |
| Chart: Natural Hazards Surveillance and Information-Sharing Systems in the US .....             | 16        |
| The EU Perspective .....  | 18        |
| EU Systems .....  | 18        |
| Chart: Information Sharing and Disease Surveillance Systems in the European Union .....         | 23        |
| Chart: Natural Hazards Surveillance and Information-Sharing Systems in the European Union ..... | 25        |
| <b>CHAPTER 3: UNDERSTANDING THREE INFORMATION CULTURES .....</b>                                | <b>27</b> |
| Shared and Disparate Challenges .....   | 27        |
| Diagram: Three Information Cultures .....   | 29        |
| Chart: Cultures – Systems, Technical Expertise, and Data Ownership.....                         | 30        |
| Chart: Public Health Cycles – Traditional and Emerging .....                                    | 34        |
| <b>CHAPTER 4: POLICYMAKERS’ NEEDS (AND WANTS).....</b>  | <b>39</b> |
| Warning in Complex Threat Environment .....   | 39        |
| All-Hazards Challenges.....   | 40        |
| Defining the Customers and Their Needs.....   | 40        |
| Culture and Secrecy.....  | 42        |
| Inter-agency Distrust .....   | 43        |
| Legal Barriers and Over-classification .....  | 43        |
| <b>CHAPTER 5: CHALLENGES AND CHOICES.....</b>   | <b>45</b> |
| Increasing Ties Across Information Cultures .....   | 46        |
| Improving Ties Between Information Cultures and Policymakers .....                              | 47        |
| Deepening Transatlantic Cooperation on All-Hazards Information and Policy Responses .....       | 48        |
| Conclusion.....   | 49        |
| <b>ENDNOTES .....</b>   | <b>50</b> |
| <b>SELECTED READINGS .....</b>  | <b>53</b> |

# PREFACE

Dear Colleague,


I am pleased to present the report *New Information and Intelligence Needs in the 21st Century Threat Environment*. This study examines some key issues about information support to policymakers that have arisen in the information age. The challenge of providing the right information to the right people has been compounded by the challenge of terrorism and shifts in governments' priorities and in governmental organization that deal with various threats to national and human security. This problem set is not unique to the United States, and the study looks at the European Union and selected EU member states as an important point of comparison, and as a critical partner for information sharing and problem solving.

The Stimson Center, in collaboration with the Swedish Emergency Management Agency (SEMA) and the Department of Homeland Security's Office of Intelligence and Analysis, embarked on a year-long exploration of three distinct information cultures – terrorism, public health, and natural hazards – to illuminate problems within and between those distinct expert communities in providing information to key decision-makers and crisis managers. We are grateful to SEMA and to DHS for their financial support, and for their expert participation in a series of workshops and conversations that contributed to this report. Several dozen people of diverse expertise, in government and out, agreed to be interviewed for this study, and we are indebted to them for the insights and information they provided.

The Stimson team included: Julie Fischer, Senior Associate and director of our work on global health security, Jesper Gronvall, former representative of the Swedish Institute for International Affairs resident at Stimson, Aditi Hate, Research Associate, Rebecca Bornstein, Scoville Fellow, summer interns Amanda Greenland and Anita Ravishankar, and Peter Roman, former Senior Associate responsible for homeland security analysis. I am grateful for their fine contributions to this study.

I hope you will find this study of use in prompting creative thinking about the enduring challenges of information sharing for homeland security as well as international security requirements.

Sincerely,



Ellen Laipson  
President and CEO



## THE PROBLEM

The twenty first century has presented us with distinctly new kinds of security challenges. From the year 2000 computer rollover (Y2K) to the terrorism attacks against major western cities since 2001, to a series of natural disasters, governments and societies are coping with a different security agenda than was the case in the 20<sup>th</sup> century, with its nearly static geopolitical threat configuration.

These new challenges have specific information components.<sup>i</sup> In some cases, the crisis is essentially about information, such as cyberattacks against government or critical private sector information systems. In others, the information needs for crisis managers are critical but do not yet enjoy a robust infrastructure. Yet others require a blending of sensitive intelligence gathered by government satellites or human agents, with complex data available in the public domain but not often integrated with secret information. Governments are adapting their practices to this world of greater interdependence and interaction, between issues such as terrorism and health, and between actors, such as government and industry. They continue to search for new ways to manage these relationships at time when the public demand for information and transparency is high.

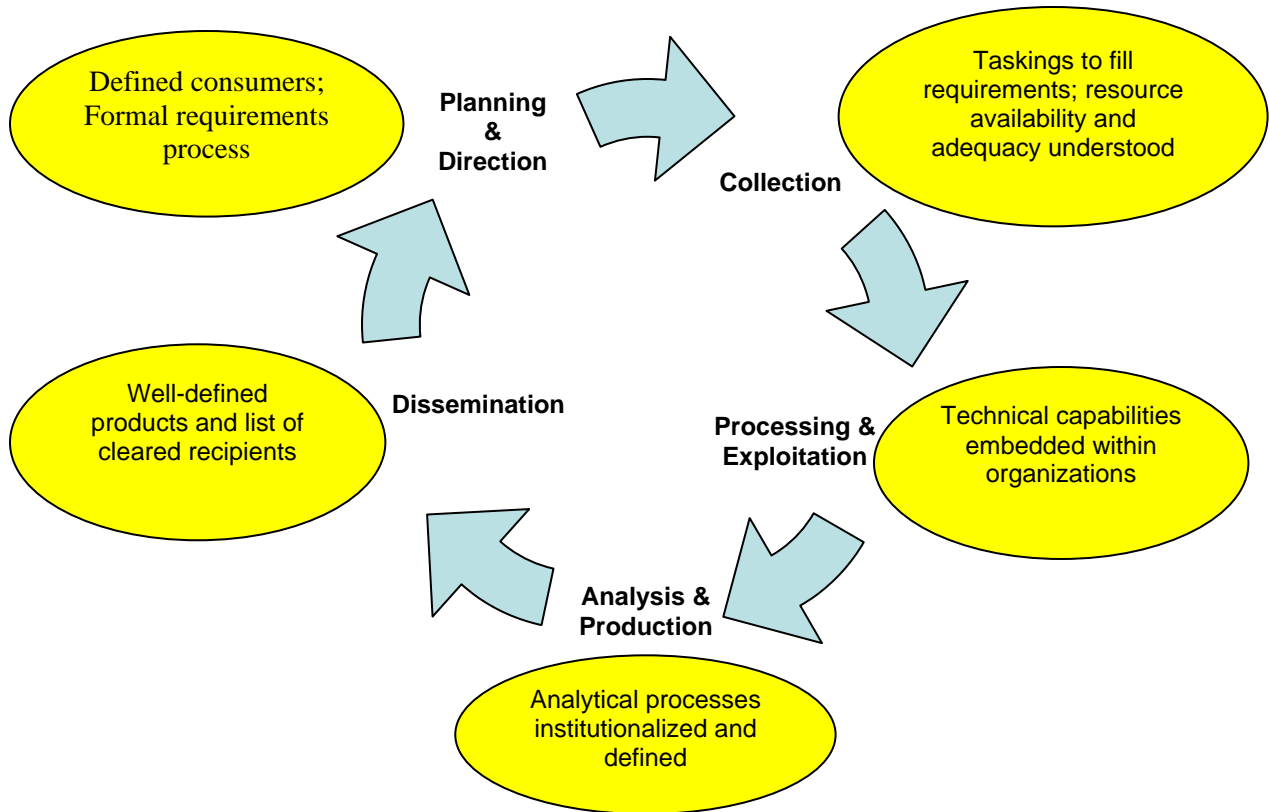
This study offers an initial look at three information cultures – terrorism, health, and natural hazards – which are intrinsically important to the homeland security mission, but are also surrogates for a wider array of topics on which there is expertise in and outside of government that needs to be channeled in reliable ways to decision-makers and crisis managers. It does not attempt to offer operational solutions to the demands for information sharing and integration of expertise; rather, it examines more broadly some of the conceptual issues within and between these information communities, and considers how policy makers use or wish to use the knowledge housed within these communities. It consciously works to identify parallels and differences between US and European perceptions and practices, and attempts to identify some policy responses that would be relevant to both. Throughout the report we try to identify areas where progress has been made in improving sharing, or other aspects of promulgating a more effective information support system for all-hazards contingencies.

---

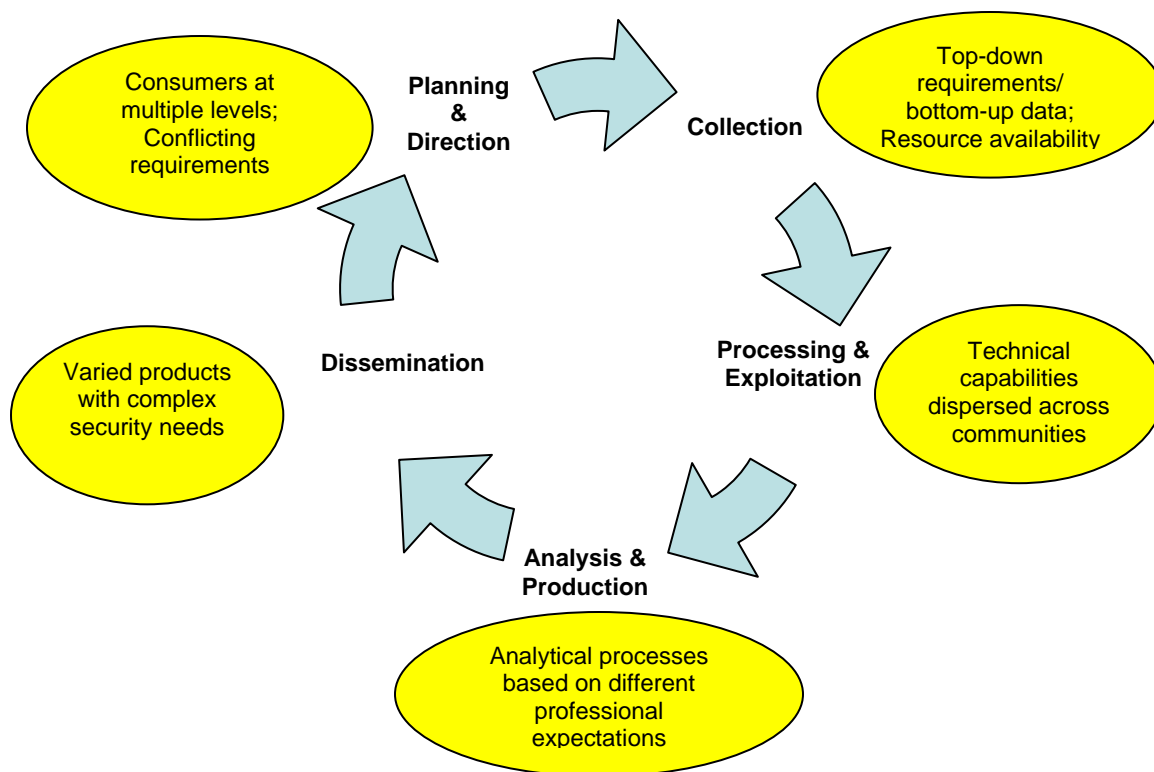
<sup>i</sup> This study is about the information needs of government decision-makers. Information includes material derived from observation, communications, reports, and technical systems. When collected clandestinely or evaluated and interpreted by intelligence analysts, information becomes intelligence or is included in intelligence products. Data is a discrete subset of information, collected according to scientific methods or based on clear and quantifiable criteria. This report will use these terms as the key actors use them, and provide context to the use of these different, overlapping terms, to the extent possible. We have intentionally avoided referring to all-hazards information as “intelligence” both because we do not think all of that information can accurately be categorized as intelligence and because of the implications of “securitizing” very open and public information systems for the experts involved.

This study is an early exploration of some of the key issues of how governments acquire and use the information from diverse communities for decisions and responses to a new threat environment. The study asks:

- How do decision-makers in homeland/societal security positions get the information they need?
- In an all-hazards environment, is information on topics as diverse as health, natural hazards and terrorism readily available and reliable?
- Do decision-makers differentiate between information and intelligence?
- Is the US experience unique or are there useful comparisons to Europe's experience?



**Traditional intelligence cycle:** A formal requirements process, with clearly defined stakeholders, a good understanding of analytical capabilities, and a process for dissemination based on predetermined security needs.



**Evolving intelligence cycle:** Diverse communities under aegis of homeland security bring differing expectations, priorities, and decision-making needs to an increasingly complex information environment.



## THE CURRENT SYSTEMS

This chapter briefly examines existing mechanisms to bring information related to terrorism, infectious diseases, and natural hazards to the attention of decision-makers and crisis managers at the local, national, and supra-national levels. It offers a glimpse of institutions, some old, some very recent, designed to cope with the information requirements of 21<sup>st</sup> century challenges. Our focus is on information support to leaders. We have attempted neither to address all the public information and citizens' awareness programs that have been promulgated in the aftermath of terrorist, health and natural hazards crises of recent years, nor to evaluate the effectiveness of any of these structures. It is clear that over the last decade, many new offices and acronyms have been created, yet uncertainties abound regarding information flows, authorities to share, and rules of the road in getting critical data and analysis to key decision-makers.

### The US Perspective

For the United States, the homeland security story begins with the September 11, 2001, attacks, and moves quickly to Hurricane Katrina in September, 2005. These twin crises exposed serious deficiencies in US intelligence and crisis management capabilities, and led to the radical restructuring of two key components of the US national security government infrastructure: the creation of the Department of Homeland Security (DHS) in 2002 from several dozen agencies and the establishment of the Office of the Director of National Intelligence (ODNI) through intelligence reform legislation in late 2004. These two new institutions, and other lesser steps such as renaming one of the US-based commands (Northcom) to include a more explicit homeland security mission, are considered the most important changes in how the US manages its domestic and national security requirements since the National Security Act of 1947 which created the National Security Council, the Central Intelligence Agency, and the Department of Defense.

Both of these new institutions are still in formation, but considerable work has been done to develop smarter and more effective ways to share information, to break down barriers that impeded smart utilization of information and intelligence that was owned, but not exploited fully, by various government bodies. The US Congress has been critical of some aspects of institutional reform, but the two institutions have not faced significant political or financial constraints as they consolidate and create new processes and business practices.

The ODNI's mission is fundamentally about information. It was not created primarily to be a producer of analysis, but to empower and facilitate the smart fusion of knowledge from all the intelligence players, and to defend and represent the intelligence function in strategic planning, funding, and management of the nation's national security requirements. DHS, by contrast, was created primarily to provide services and to implement a vast array of operational requirements. Intelligence and information support functions have had to establish their roles and make themselves players in this large department. The DHS intelligence operation was set up when terrorism was the existential threat, but has had to adapt quickly to an all-hazards threat logic.

## ***US Systems***

### ***Terrorism***

Since 2001, terrorism analysis has remained the highest priority and the largest single enterprise of the US intelligence community, commanding billions of dollars annually and enormous amounts of analytical expertise. The intelligence community, with the ODNI at its head, is the primary player with respect to information, intelligence and analysis related to terrorism. The ODNI is charged with ensuring timely and objective delivery of critical intelligence to important actors on the federal level, as well as establishing clear objectives and priorities for the collection, analysis, production and dissemination of intelligence. The ODNI, as part of the post-9/11 intelligence reforms, also sets policies for sharing critical information with state and local actors, policies that DHS and Department of Justice, in practice, implement.

In the immediate wake of the 2001 terrorist attacks, the intelligence community sought new mechanisms to improve interagency information sharing, including convening analysts from across the intelligence community to compile the daily terrorism threat matrix for senior policymakers. Over time, the core functions of this threat matrix have been absorbed into an increasingly institutionalized system of interagency information sharing.

The following is a selection of key terrorism information hubs:

- *National Counterterrorism Center*  
The National Counterterrorism Center (NCTC) organizes national counterterrorism efforts, from collection to operations, and is located in the ODNI. The CIA provides training and personnel for this hybrid arrangement, established partly to address the 9/11 Commission's concerns about information stove-pipes and ambiguities in agency responsibilities prior to 2001. NCTC provides all-source intelligence support throughout the government, including "information technology (IT) systems and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of, terrorism information."<sup>1</sup>
- *National Operations Center*  
The National Operations Center (NOC), located in DHS, harvests information on potential terrorist activities gathered by other multi-agency operations, serving as a national center for situational awareness. Since its creation after the 9/11 attacks, the NOC has steadily evolved into an all-hazards and threat center and now aggregates and disseminates all homeland security information, issuing alerts and security bulletins to stakeholders at the federal, state, and local level. It incorporates the 24/7/365 National Operations Center-Interagency Watch (NOC-Watch), which has an embedded intelligence watch and warning staff, and the Federal Emergency Management Agency's (FEMA) National Response Coordination Center, and shares responsibility for the National Infrastructure Coordination Center.
- *State and Local Fusion Centers*  
The establishment of state fusion centers across the US represents a significant reform effort to increase terrorism information-sharing across jurisdictional levels as well as

between agencies, increasing analytical and information-gathering ability and creating an avenue for disseminating information to local and state authorities. At present, there are more than 40 operational fusion centers in the US.<sup>2</sup> Fusion centers are “a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”<sup>3</sup> Although Federal support for these centers initially focused on counterterrorism, the majority of operational fusion centers describe their current missions as “all crimes” or “all-hazards.”<sup>4</sup> Law enforcement organizations form the backbone of most fusion centers; the number and breadth of other partnerships vary, with some centers focused primarily on criminal and terrorist activities and others encompassing a broader public health and safety mandate. Federal stakeholders such as DOJ, the Federal Bureau of Investigation (FBI), and the DHS Office of Intelligence and Analysis (I&A) deploy officers to fusion centers to facilitate a timely flow of classified and unclassified information, provide subject matter expertise, coordinate with local law enforcement departments and other agencies, and share information on the jurisdiction’s priorities, needs, and vulnerabilities.

- *Interagency Information Sharing Networks and Systems*

Collectively, DHS and DOJ have 17 major information-sharing networks to support their homeland security missions. Systems such as the DHS Homeland Secure Data Network (HSDN) facilitate rapid electronic information exchange, including with state and local governments. Of these 17 networks, four are classified as top secret/secret and 12 are sensitive but unclassified. Only one network is unclassified. Nine of these networks share information only within a single department; the remaining eight facilitate information-sharing among federal, state, and local government agencies. DHS and DOJ also host four web-based applications that collect, warehouse, and disseminate homeland security-related information. These applications include DHS’s Homeland Security Information Network (HSIN), the department’s main information technology system for sharing terrorism and related information, and DOJ’s Law Enforcement Online (LEO). All four system applications are considered to be sensitive but unclassified and are available for use by relevant federal, state, and local government agencies.<sup>5</sup>

### *Infectious Diseases*

The anthrax attacks of 2001, the SARS epidemic of 2003-2004 and the spread of a highly pathogenic avian influenza strain feared to have pandemic potential created a new awareness of the vulnerability of US interests to disease threats. Since 2002, the US government has dedicated billions of dollars to building state and local public health capacity for the detection and control of potentially catastrophic outbreaks.<sup>6</sup> A new international health regulatory framework implemented in 2007 raised the stakes, creating a notional obligation for all World Health Organization member states to develop capacity to detect and report significant public health emergencies in real time.<sup>7</sup>

The majority of disease surveillance activities take place at the local and state level, when clinical or laboratory findings of a reportable disease trigger an outbreak investigation by local or state health departments. Diseases that must be reported vary by state, allowing authorities to detect and track outbreaks of local significance in addition to those that states must report to the National Notifiable Diseases Surveillance System maintained by the US Centers for Disease Control and Prevention (CDC).<sup>8</sup> Disease surveillance, outbreak response, and communications capabilities vary greatly among states.

If the outbreak investigation or response requirements overwhelm local capacity, or the disease itself is suspected to be one of the “select agents” deemed to pose a significant threat to public health if released deliberately, officials can request Federal assistance. The major Federal capacity for outbreak investigations is contained within the CDC, including a cadre of experienced epidemiologists and laboratorians working in the US and overseas, and the Epidemic Intelligence Service, a 2-year postgraduate program for about 160 trainee-officers at any given time initially launched to detect covert biological attacks during the Cold War.<sup>9</sup> The recently renamed National Center for Medical Intelligence (formerly AFMIC, the Armed Forces Medical Intelligence Center), has expanded its mission from a focus on identifying health threats to military personnel only to respond to the broader homeland security biodefense mission. The new National Biosurveillance Integration Center (NBIC) at DHS has been assigned to coordinate information-sharing on disease threats, first for Federal agencies and eventually for state and local stakeholders, and to develop a “Biological Common Operating Picture.”

The CDC is currently leading development of a National Biosurveillance Strategy, including a comprehensive gap analysis and stakeholder mapping exercise to strengthen information-sharing among Federal, state, and local public health experts and clinicians. In the meantime, the current patchwork of disease surveillance information-sharing systems range from detector-based programs designed to give advance warning of a narrow spectrum of covert biological attacks to technologies aimed at combing open-source media for suggestions of unfolding disease events. The following table characterizes some of these systems briefly.

| Information Sharing and Disease Surveillance Systems in the US |  |                    |   |              |                    |   |  |
|--|--|--------------------|---|--------------|--------------------|---|--|
| Scope  | Name   | Host               | Brief Description   | Stakeholders |                    |   | Challenges                                     |
|  |  |                    |   | Int'l        | Federal            | State and Local                           |  |
| DOMESTIC SURVEILLANCE SYSTEMS                                  | BioWatch   | DHS                | Early warning system to detect airborne biological traces             |              | EPA, CDC, FBI      | Health departments                        | Limited analysis, poor coordination            |
|  | BioSense   | CDC                | Syndromic data from healthcare systems                                |              | CDC                | Healthcare facilities, health departments | Pilot phase                                    |
|  | National Bio-surveillance Integration System   | DHS                | Automated system to integrate all Federal health data in real time    |              | DHS, DHHS          | Health departments                        | Major logistical and organizational challenges |
|  | National Retail Data Monitor   | Health depts., DHS | Collects and analyzes data on pharmaceutical sales in near real-time. |              | DHHS, CDC          | Health departments                        | Limited baseline data and unclear utility      |
|  | National Electronic Disease Surveillance System  | CDC                | Software application for disease surveillance and reporting           |              | CDC                |   | Implementation still in progress               |
|  | Electronic Surveillance System for the Early Notification of Community-Based Epidemics | DoD                | Collects data from 300 military health facilities for BioSense        |              | CDC                |   | Essentially a sentinel system                  |
|  | FABIS  | USDA               | Integrates animal health/food safety data                             |              | USDA, FDA          |   | Implementation still in progress               |
|  | Project ARGUS  | Georgetown Univ.   | Seeks disease event warning information in open source media          |              | DHS, CDC, USAMRIID |   | Broad but imprecise net – still                |

|                             |  |                    |   |                       |          |                               | prototype   |
|-----------------------------|--|--------------------|---|-----------------------|----------|-------------------------------|---|
| GLOBAL SURVEILLANCE SYSTEMS | Global Outbreak Alert and Response Network (GOARN) | WHO                | A network of national networks and open source information                        | WHO, other int'l NGOs | DHS, CDC | Infectious diseases community | As reliable as input information                  |
|                             | Global Public Health Intelligence Network (GPHIN)  | WHO, Health Canada | Seeks disease event warning information in open source media                      | WHO, other int'l NGOs | DHS, CDC | Infectious disease community  | Broad but imprecise net                           |
|                             | FluNet   | WHO                | WHO's influenza surveillance network database                                     | WHO                   | DHS, CDC | Infectious disease community  | As reliable as input information                  |
|                             | ProMED   | IDSA               | Community tool for detecting and sharing disease information in open source media | WHO                   | DHS, CDC | Infectious disease community  | Asset is informed people – minimal infrastructure |

***Natural Hazards***

Although better warning systems and a greater awareness of natural hazards has decreased the loss of life associated with natural disasters in the US, the economic toll continues to mount. Hurricane Katrina alone is estimated to have caused approximately \$200 billion in damages and losses, making it the costliest disaster in history; less spectacular hazards such as floods are estimated to cost about \$6 billion (and take about 140 lives) annually in the US.<sup>10</sup>

Information and intelligence sharing within the natural hazards community consists of a loosely defined network of national weather experts, federal, state, and local emergency management officials, and the media that work together to ensure timely dissemination of catastrophic weather information to the public when a major disaster threatens a vulnerable area. Various programs within the National Oceanic and Atmospheric Administration's (NOAA) National Weather Service (NWS) and the US Geological Survey (USGS) conduct research and disseminate warnings on severe weather events and disasters such as hurricanes, tornadoes, and floods, earthquakes and tsunamis. These two organizations share broad jurisdictions and information strategies; both collaborate closely with FEMA and senior state emergency management officials to develop strategies for disaster preparedness at the state and local levels to protect critical infrastructure and vulnerable populations. The following table briefly summarizes organizations and systems involved in collecting and sharing information on natural hazards.

| Natural Hazards Surveillance and Information-Sharing Systems in the US |   |   |   |  |                       |  |  |
|--|---|---|---|--|-----------------------|--|--|
| Scope  | Category                                  | Host  | Brief Description   | Stakeholders   |                       |  | Challenges   |
|  |   |   |   | Int'l  | Federal               | State and Local  |  |
| NON-FEDERAL DOMESTIC ORGANIZATIONS                                     | Academic Institutions                     | Universities and university-Federal centers | Range in focus from basic research in hazard reduction and environmental studies to specific threats or issues  | Academic professionals interact with a range of stakeholders both formally and informally. |                       |  | Communications between scientists and policymakers |
|  | State/regional agencies and organizations | State governments and regional offices      | All states have an emergency management organization with some hazards analysis capability  |  | FEMA, DHS, NOAA/NWS   | State/local gov'ts (emergency managers, public safety)   | Funding, coordination                              |
|  | Professional organizations                | Membership organizations and societies      | Venue for information sharing among technical professionals   |  |                       | State/local gov'ts and public  | Fairly technical, resource-limited                 |
| US GOVERNMENT AGENCIES   | US Geological Survey (USGS)               | Federal Government                          | Collects and analyzes data on multiple hazards, including:<br>Global seismic networks<br>Hydrologic networks and analysis<br>Landslide hazards<br>Volcano hazards | Int'l partners   | FEMA, DHS             | State/local gov'ts (emergency managers, public safety), regional centers, NGOs, private sector, public |  |
|  | US Army Corps of Engineers (USACE)        | Federal Government                          | Responds and conducts post-disaster assessments   |  | FEMA, DHS, NOAA, USGS | State/local gov'ts (emergency managers, public safety)   |  |



|                             |   |  |   |                             |                                  |  |  |
|-----------------------------|---|--|---|-----------------------------|----------------------------------|--|--|
| GLOBAL SURVEILLANCE SYSTEMS | National Earthquake Hazards Reduction Program (NEHRP)                                   | Federal Government                     | Addresses interagency coordination shortfall to improve assessment of hazards and vulnerabilities   |                             | FEMA, NIST, NSF, USGS, OSTP, OMB | State/local gov'ts (emergency managers, public safety)   |  |
|                             | Federal Emergency Management Agency (FEMA)  | Federal Government (in DHS)            | Federal coordinator of information-sharing for emergency preparedness, protection, response, and recovery   |                             | White House, DHS                 | State/local gov'ts (emergency managers, public safety), regional centers, NGOs, private sector, public |  |
|                             | National Oceanic and Atmospheric Administration (NOAA) - National Weather Service (NWS) | Federal Government                     | Collects and analyzes weather-related information through offices including:<br>Tropical Prediction Center<br>National Hurricane Center<br>2 domestic and 2 international tsunami warning centers<br>Storm Prediction Center<br>Hydrologic Information Center | Int'l partners              | FEMA, DHS                        | State/local gov'ts (emergency managers, public safety), regional centers, NGOs, private sector, public |  |
| GLOBAL SURVEILLANCE SYSTEMS | International and Overseas Organizations  | Regional Groups and Individual Nations | Multiple US-supported regional hazards and recovery information-sharing organizations   | Nations and regional bodies |                                  |  |  |

## **The EU Perspective**

The twenty-seven member states of the European Union (EU) with its 490 million citizens have not been immune from consequences of crises and complex emergencies in recent years. Events such as massive flooding in central Europe, vast forest fires in southern Europe, terrorism bombings in Madrid and London, avian flu outbreaks across the EU, support to many thousands of EU citizens caught in the tsunami in south-east Asia and evacuating EU citizens from Lebanon during the conflict in 2006, have shaped the development of an emerging EU societal security identity (this term will be used as the EU equivalent to homeland security).

Consequential threats to our societies are not always triggered by acts of ill-will, but through structural reasons or by chance, like the SARS outbreak first reported in 2003 or large-scale industrial accidents, as demonstrated by the 1986 incident at the Chernobyl plant. The proliferation of public and private biological labs across the globe increases the risk of accidental release, as happened in 2007 with foot-and-mouth disease in the UK.

These novel and more acute threats and risks are different in character and more diffused in their potential consequences. They demand concerted strategies that differ from how governments could meet the territorial wars of the past. The ability to pick up weak, or contradictory, signals and interpret them correctly stands out as a key process for individual decision-makers and for bureaucracies. “Sense-making” has been identified as a key factor for effective decision-making.<sup>11</sup> This may be especially essential in an environment that is characterized by complexity, compressed time-lines and dwindling importance of geographical distance.

## ***EU Systems***

In Europe the questions of societal security primarily fall under the direction of national governments, but an EU role has evolved over time through an Europeanization process. When talking about EU level, it should be understood as the supranational political system based in Brussels on a set of treaties, institutions, and processes.

The bottom-line is that at present there is no common, or shared, understanding or institutional framework for societal security in the EU to match that of the federal level in the US. An unresolved issue in the EU is where responsibilities for different aspects of societal security should rest; on a national or the EU (Brussels) supranational level. Furthermore, the twenty-seven member states of the EU have idiosyncratic national institutional arrangements. In some member states, the main responsibility for this area can be found in a Ministry of Interior, or Ministry of Justice, or Ministry of Defense. That of course increases the complexity of a transatlantic discourse on homeland security matters, as there is no single clear point of contact for DHS and other homeland security actors in the US. There is furthermore no Europe-wide consensus on an EU term equivalent to the US term “homeland security.” The term homeland security is not well understood in Europe, as it does not sufficiently frame the issue of 21<sup>st</sup> century security, which cannot be established by one nation alone. Nations are dependent, and thriving, on global flows of goods, people, financial transactions and communication signals.

The heavy emphasis on terrorism is also not well understood in Europe. The first US Homeland Security Strategy issued in 2002, and the updated version in 2007, define Homeland Security as: "...a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." An emerging term in Europe is societal security, which implies that the threats and challenges of the 21st century are less about the integrity of the territory than about safeguarding critical functions of society, protecting citizens and upholding fundamental values.

### ***Terrorism***

The EU's common foreign and security policy (CFSP), a framework for considering external security matters, is relatively young and quite complex. The CFSP specifically in relation to the fight against terrorism consists of at least six formally institutionalized intelligence and counterterrorism bodies, various ad hoc groups and several operational EU-wide databases.<sup>12</sup> While the EU advocates establishing many decentralized institutions and multilateral partnerships, it is necessary that Europe's intricate system of information sharing is made easily comprehensible and accessible by all Member States for EU security initiatives to achieve their full potential.<sup>13</sup>

The EU's Counter-Terrorism Strategy and its underlying information sharing mechanisms have materialized over the past two decades in the form of two primary entities: European Police Organization (Europol), and the European Union Military Staff.<sup>14</sup> Other EU institutions assisting in the fight against terrorism include Eurojust, a body that investigates, prosecutes, and extradites criminals and terrorists acting in two or more EU Member States, and the European External Borders Agency (Frontex), which facilitates enhanced coordination between the Member States to secure and survey EU external borders.<sup>15</sup> The EU also relies on numerous less-institutionalized intelligence bodies such as SitCen, Satellite Facilities, the Club of Berne and similar ad hoc communication groups and intelligence sharing agreements, including the EU Counter-terrorism Co-ordinator, the ARGUS system (a general link between all specialized Rapid Alert Systems), and the Crisis Coordination Arrangements (CCA) within the Council framework.

- ***Europol***

Europol was established under the 1992 Maastricht Treaty as a descendant of the 1970's Trevi Group.<sup>16</sup> Foundationally similar to the Club of Berne discussed below, the Trevi Group was one of the first attempts to unify Europe around common security priorities. This intergovernmental assembly established the first secure communication network throughout the EU for more reliable cooperation on defense and intelligence related issues.<sup>17</sup> According to Europol's mandate, the organization is responsible for increasing intelligence sharing to combat terrorism, drug and human trafficking, illegal immigration, money laundering, and other serious crimes.<sup>18</sup> Europol does not directly enforce EU laws, but facilitates cooperation between Member States through European liaison officers (ELO) from each State who operate as middlemen between national and EU bodies, requesting and providing intelligence to both.<sup>19</sup>

- *Military Staff Intelligence Division*

The Military Staff's Intelligence Division does not have independent collection capabilities. It relies, like most EU intelligence bodies, on finished intelligence provided by Member States. Accordingly, it regularly coordinates with Member States' defense and intelligence units to fulfill its mandate to provide early warnings, situation assessments, and long-term strategic planning in regards to EU security concerns.
- *SitCen*

Occasionally referred to as the Joint Situation Centre, the EU's Situation Centre (SitCen) resides in the EU Council of Ministers and is responsible for intelligence coordination generally. SitCen also lacks collection capabilities, primarily due to sovereignty issues, but builds its own intelligence assessments based on intelligence products provided by Member States.<sup>20</sup> SitCen promotes dialogue between intelligence and security experts to discuss evolving threats to the EU. Before 2005, SitCen focused solely on external threats, but in the past three years has directed its attention toward threats emanating from within the EU. In doing so, SitCen has become one of the most reliable sources for EU strategic terrorism analysis. Today, SitCen regularly communicates with Europol, which further increases information sharing within the EU, and the Centre continually meets with foreign, defense and interior ministers to recommend policies and actions appropriate to counter assessed threats.<sup>21</sup>
- *Satellite Facilities*

EU imagery intelligence capabilities primarily rely on the Torrejon Satellite Center based in Spain. This center became operational in 1997 as a result of the Western European Union's push for intelligence sharing between Member States. The Center does not, however, own or operate its own satellites. Instead, it coordinates the inflow and dissemination of relevant intelligence data to and from EU members. The only satellites acquired by the EU thus far include Hélios 1 & 2, both launched in the late 1990's, and the two Horus project Satellites. Due to limited funding and support from EU members, the satellites are limited in technological ability, a hindrance to the development of independent IMINT capabilities within the EU for surveying and tracking terrorists and other dangerous criminals.<sup>22</sup>
- *Ad hoc Security Bodies and Additional Groups*

The Club of Berne is more or less an intelligence & security discussion group for the 27 EU Heads of States. However, unlike other EU security and information sharing institutions, the Berne Group operates independently of the EU, does not employ a staff for analytical purposes and cannot require Member States and EU intelligence institutions to share information. The Club's members can, however, create working groups, such as the Counter Terrorist Group (CTG) and perform threat assessments, occasionally in partnership with the United States.<sup>23</sup> Numerous less formal organizations focused on securing Europe through increased cooperation exist, facilitating increased communication among officials from all Member States. A few examples include terrorism working groups comprised of national interior ministry

officials, the foreign policy-oriented working groups on terrorism consisting of national foreign ministry officials, and the police chief's task force, composed of national law enforcement officials.<sup>24</sup> Less formal partnerships also contribute to overall EU intelligence sharing. The most noteworthy of such partnerships in the EU is the G-5 group where members Britain, France, Germany Spain and Italy often discuss counterterrorism at routine meetings.<sup>25</sup> Other similar multilateral dialogues which focus on security issues include the Benelux countries, the Salzburg group, the Baltic Sea task force and even a nascent Mediterranean initiative for collaborative law enforcement and counterterrorism efforts.<sup>26</sup>

### ***EU Health Protection***

Health protection, extensively discussed within the EU, generally falls under the purview of member states. Action at the EU level is "largely of a voluntary nature comprising information and 'best practice' sharing, networks are still loosely organized...."<sup>27</sup> Many EU structures and processes in infectious disease detection and response have been triggered by crises or near-misses, such as links between the outbreak of the mad cow disease (BSE, or bovine spongiform encephalopathy) and its human equivalent, hoaxes in Europe following the anthrax letters in the US, and the SARS outbreak.

However, the EU Commission, with DG Health and Consumer Protection in the lead, is a major partner in developing health protection policies with the member states, such as the EU Commission green paper on bio-preparedness launched in 2007 to stimulate a debate on how to reduce biological risks and enhance European preparedness and response capabilities. The critical need to put processes in place for early warning and response through effective information exchange was highlighted, and several of the report's suggestions are being addressed by a key actor in this field, the European Centre for Disease Prevention and Control (ECDC).<sup>28</sup>

The ECDC, an EU agency established in 2005, is located in Stockholm, Sweden and has a staff of about 200 people with a budget of €40.1 million for 2008.<sup>29</sup> Its mission is to work together with relevant institutions in the member states to develop and strengthen systems for disease surveillance, rapid alerts, and to build and sustain preparedness and response capabilities against epidemics. The agency serves as an expert authority that, in concert with networks in the member states, can provide timely expert advice on public health to the Commission, authorities in the member states, the public and international organizations.<sup>30</sup>

The 27 EU member states have their own surveillance systems and procedures, using different data collection methods and case definitions (which makes it difficult to compare data sets) and through divergent agencies and processes.<sup>31</sup> These collection discrepancies, along with differences in staff/technology capacity, funding and source validity, all contribute to problems of non-compatibility of EI surveillance data. In addition to the national surveillance systems, several EU-wide Dedicated Surveillance Networks (DSNs) created by networks of devoted microbiologists or epidemiologists in member states were established before the inception of ECDC. These emerged independently of each other without any holistic European plan on how to tie them together and to integrate the results. The ECDC is working with member states and DSNs to harmonize and

standardize systems and data for higher quality and validity. In 2007 ECDC approved a long-term strategy (2008-2013) for the Surveillance of Communicable Diseases in the European Union aimed at reforming both national and Union level epidemic intelligence (EI), particularly data collection methods. Towards 2013 the “ECDC will have taken over full responsibility of surveillance and can subsequently focus on developing and consolidating the highest quality systems possible for Europe.”<sup>32</sup> The following table briefly summarizes current or anticipated mechanisms for sharing disease surveillance information at the EU level.

| Information Sharing and Disease Surveillance Systems in the European Union                   |  |               |  |              |                       |                         |   |
|--|--|---------------|--|--------------|-----------------------|-------------------------|---|
| Scope  | Name   | Host          | Brief Description  | Stakeholders |                       |                         | Challenges  |
|  |  |               |  | Int'l        | National              | Sub-national            |   |
| EU Systems   | Basic Surveillance Network (BSN)                                 | ECDC          | Data on disease incidence trends in the EU Member States                                 |              | EU member states      |                         | Limited feedback and low usage  |
|  | The European Surveillance System (TESSy)                         | ECDC          | An integrated EU database that combines 15 disease-specific surveillance systems         | ECDC         | EU/EEA member states  |                         | In implementation; will have to overcome variability in data content and quality        |
|  | EU Threat Tracking Tool (TTT or 3T)                              | ECDC          | Tracks and analyzes emerging diseases affecting two or more EU/EFTA states               | ECDC         | EU/EFTA member states |                         | In process of transformation from event-based system to an Epidemic Intelligence System |
|  | Early Warning and Response System (EWRS)                         | EU Commission | Secure web-based system for sharing information on outbreaks with cross-border potential | ECDC         | EU/EEA member states  |                         | Reporting requirements for “immediate notification” still poorly defined                |
|  | RAS BICHAT (Rapid Alert System for Bio/Chem Attacks and Threats) | EU Commission | Information exchange and coordination of crisis management efforts                       | ECDC         | EU member states      |                         | Complex resource and management demands   |
|  | MediSys  | EU Commission | Seeks disease event warning information in European open source media                    |              | EU member states      | Public (limited access) | Broad but imprecise net   |
| For global surveillance systems and resources, see table in US Systems – Infectious Diseases |  |               |  |              |                       |                         |   |

***Natural Hazards***

Europe is vulnerable to natural disaster, including flooding, forest fires, heat waves, and drought.<sup>33</sup> This natural vulnerability appears exacerbated by climate change and environmental degradation. Recent disasters such as the 2004 Indian Tsunami and the 2007 European floods and forest fires prompted acute awareness of the EU's insufficient disaster response capabilities.<sup>34</sup> The European Commission's (EC) Environment Directorate-General's (DG) Civil Protection Unit<sup>35</sup> is responsible for working together with the member states to enhance the capacity for disaster prevention and response policy management. The EU-level's major contribution is to encourage the member states to improve response times by sharing timely information and preparing interoperable resources.

Recent efforts have focused on improving the 'horizontal coordination' of disaster response between the EU Commission, President and High Representative/Secretary General with relevant organizations at the national level.<sup>36</sup> The following table summarizes some of the existing resources for natural hazards information sharing in the EU.



| Natural Hazards Surveillance and Information Sharing in the European Union |   |  |  |               |   |
|--|---|--|--|---------------|---|
| Scope  | Category  | Host   | Brief Description  | Stakeholders  | Challenges  |
| EU Organizations   | European Commission Environment Directorate-General's Civil Protection Unit | European Commission Environment -Directorate-General | Encourages states to improve response times by sharing timely information and preparing interoperable resources                                    | Member States |   |
|  | Community Mechanism for Civil Protection (CM)                               | European Union                                       | Coordinates collective civil protection action between all EU member states and Iceland, Liechtenstein and Norway                                  |               |   |
| Major CM Organizations   | Monitoring and Information Center (MIC)                                     | CM   | Acts as a communication hub that facilitates information sharing between member states   |               | The EC wants the MIC to become the focal point of European operational coordination in disasters; for this to happen, the MIC needs to develop capabilities for proactive anticipation and real-time monitoring |
|  | Common Emergency Communication and Information Center (CECIC)               | CM   | Comprehensive web-based information-sharing platform which synchronizes communication between MIC and National Contact Points in each member state |               |   |
|  | CM Training Program   | CM   | Ensures the continual training of civil protection personnel; encourages discussion between experts; tests EU capabilities                         |               |   |



---

— 3 —

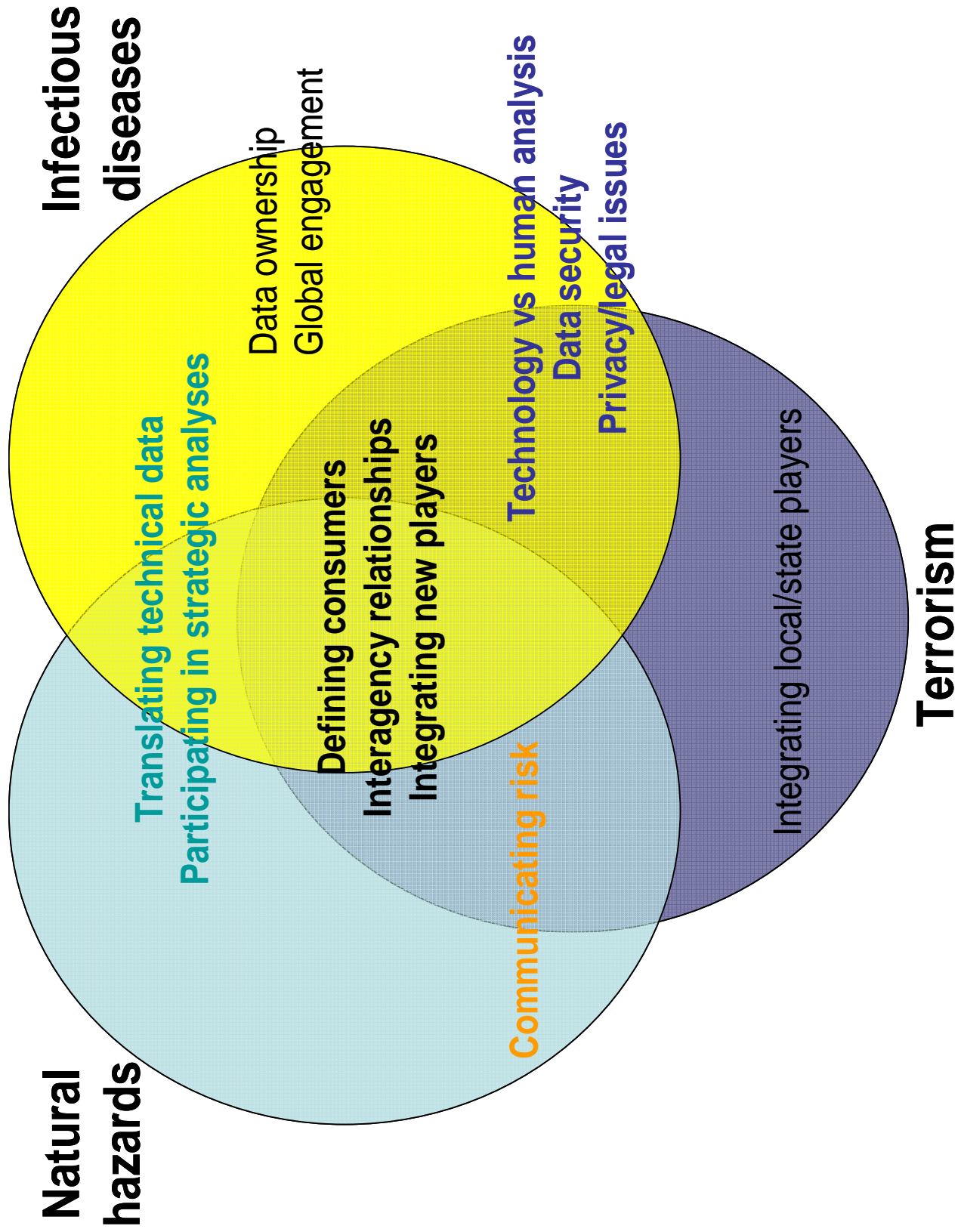
## UNDERSTANDING THREE INFORMATION CULTURES

The increasing complexity of information systems, combined with the expanded list of threats now collected under the aegis of homeland or societal security, creates an overwhelming amount of disparate and equally urgent information for decision-makers. The organizational demands alone make enfoldng multiple communities of newly relevant experts into an evolving set of government policy structures a formidable challenge. More intractable obstacles to integrating diverse expertise into this new security paradigm can be traced to deeply rooted differences inherent to the communities themselves. Overcoming these challenges will require at least a basic appreciation of the distinct professional cultures that shape the perceptions of experts who define, collect, analyze, and disseminate information to support homeland security decision making. This chapter offers an overview of information cultures in the three distinct fields of terrorism, infectious diseases, and natural hazards, and examines how differences among them might exacerbate information-sharing problems. We focused on the US experience within these three communities, characterizing each in terms of data ownership and management, analytical focus, warning and crisis capacity, and stakeholders.

### **Shared and Disparate Challenges**

The vocabularies of these three information cultures reflect the range of data control behaviors, ranging from reflexive secrecy among terrorism information analysts to deeply ingrained openness among natural hazards experts. When professionals in each of these fields refer to intelligence, information, and data, the connotations and assumptions of value assigned to each of these terms varies tremendously. Experts commonly assume that at least 95% of information called “health intelligence” derives from sources not constrained by security or classification concerns, while the inverse is true of terrorism intelligence analyses. The term “intelligence” itself, wholly unremarkable for policymakers and their advisers, can itself be divisive; for example, some public health experts explicitly reject the “disease intelligence” label as an unnecessary securitization of routine disease detection activities that could jeopardize their credibility with foreign counterparts. Although the terrorism and infectious diseases experts refer to routinely employed data-gathering activities as “surveillance,” disease surveillance bears no resemblance to electronic or physical surveillance of suspected terrorists. In the natural hazards context, storm surveillance refers to the collection of weather data through satellite imagery or heavily instrumented aircraft, a technique that adopts many of the tools and resources of traditional intelligence collection for different ends. In both public health and natural hazards information cultures, access to data is more commonly restricted by technical literacy and general conventions of scientific data integrity than by security concerns. Experts in all three disciplines generate information that can be understood as having strategic or tactical significance, but use these definitions differently (or not at all). Different types of professionals in each field generate distinct varieties of analytical products, and both the producers and consumers of the information hold different opinions about what constitutes an authoritative product. Finally, the evolution of these distinct information cultures has given rise to

very different types and expectations of access to policy making structures, and thus different abilities to influence decision-makers. The figure that follows graphically represents some of the key concerns unique to, and shared among, the three information cultures.



The table below summarizes some of the key characteristics of these three communities, followed by a closer look at the associated information cultures – the values, practices, norms, and assumptions that define the way that experts within these communities exchange information with each other and with decision-makers. System “openness” refers to a collection of attributes that include enterprise scope (for example, a self-contained agency-centered system as compared to a system with interagency or extra-governmental access), emphasis on personnel and information security, and data sources, ownership, and usage.

| Culture                    | System   | Technical Expertise and Knowledge   | Data Ownership and Management  |
|----------------------------|--|---|--|
| <b>Terrorism</b>           | Closed   | Embedded within organizations   | Security-limited at national level – increasing generation and consumption at local/state levels |
| <b>Infectious Diseases</b> | Primarily open (data secured to protect individual privacy; emerging securitization) | Dispersed across governmental and non-governmental institutions (research primarily federally funded) | Tiered data ownership at many levels; analyzed data disseminated to public (published)           |
| <b>Natural Hazards</b>     | Open   | Dispersed across governmental and non-governmental institutions (research primarily federally funded) | Data disseminated across agencies; analyzed data disseminated to public (broadcast)              |

### ***Terrorism***

The terrorism information culture incorporates most of the norms, values and practices of the traditional intelligence cycle, because much of the core technical expertise for collecting and analyzing information about potential domestic terrorist activity derived from the existing intelligence community. Terrorism information systems remain deeply intertwined in the larger intelligence community figuratively, as well as through personal and organizational links within the federal government.

**Training and professional criteria:** No specific academic credentials exist for intelligence analysts, although most have graduate level training in a social science or deep knowledge about a specific region. Terrorism analysis relies upon cross-disciplinary teams focusing on the various capabilities of terrorist organizations as quasi-military adversaries. Intelligence methods and skills are acquired primarily on the job, with analysts generally working several years in apprenticeship-like roles before assuming more independence. The professional reward structure – from peer recognition to promotion – within these systems traditionally honors analysts based not only on the quality of their work, but on whether it is incorporated into high-profile classified intelligence products for senior policymakers.

**Data control:** Data control practices in the terrorism information culture primarily reflect the intense information control systems derived from intelligence community protocols and expectations. These include the familiar system of information security characterized by levels of classification, with access to information and sources restricted to individuals with appropriate security clearances on a “need to know” basis. As has been reviewed elsewhere, intelligence collection and analysis systems established prior to the 2001 terrorist attacks revolved primarily around agency roles and missions, fostering procedural as well as philosophical barriers to information-sharing between organizations.<sup>37</sup> Recent intelligence reforms emphasize interagency collaboration and integration of information collection capabilities around missions rather than bureaucratic structures.<sup>38</sup> However, attempts to move beyond the barrier of originator-controlled information (ORCON) processes, in which the agency that collects the information controls the information, are still underway.

Intelligence agencies have historically accommodated the need to consider open-source data by creating distinct open-source programs within their organizations. Although new information technologies and data networks have dramatically increased the amount of information available in general, open-source data still tends to be perceived as inherently less valuable than clandestine intelligence, creating a cultural barrier to effective integration of the two parallel types of information.

**Analytical focus:** As in the broader intelligence community, access to analytical products on terrorism is largely pre-determined through a series of personnel classification and protection processes. The analytical focus of intelligence products is customarily defined through a formal process to establish the information requirements of the consumer. (Until recently, consumers consisted almost exclusively of senior-level policymakers). The planning process then creates directions for information collection, processing, assessment, and finally the production of intelligence products by trained analysts. This formal tasking process links specific intelligence collection and analysis missions to the organizations deemed most capable of bringing the appropriate resources and technical expertise to the problem. In this framework, the reliability of terrorism information products depends upon these conventions of traditional intelligence methods.

How the expanding set of stakeholders perceives the utility of the reports is a different matter altogether. The formal requirements process that traditionally drives intelligence collection and analysis precludes the question of whether analytical products meet the needs of the consumers. However, terrorism analytical products are being put to a much broader set of uses than informing high-level policymakers. Products now also go to state and local decision-makers, as well as into interagency processes, as the terrorism information culture struggles to redefine the requirements process appropriately. The perceived utility of reports can be reduced by warning fatigue (sometimes called the “Chicken Little Syndrome”), a particular problem as policymakers and community responders at every level struggle to set priorities for allocating scarce resources.

In response to the increasing complexity of the threat environment and information demands, the terrorism information culture is becoming even more multidisciplinary and more “joint.” One example is the collection of information through fusion centers – analytical clearinghouses

designed to improve terrorism information sharing by co-locating Federal intelligence professionals with local and state law enforcement and public safety authorities in a single location. On one hand, this increases the availability of information and the breadth of perspectives; on the other, the inclusion of more technical professionals through the fusion centers and other mechanisms for personnel exchanges within the Federal government creates whole new challenges with regard to assumptions about data ownership, stakeholders, and what constitutes an authoritative analytical product.

**Warning and crisis capacity:** Due to the political profile and potential consequences of terrorist activities, terrorism information systems generally receive high priority for government resources. Senior policymakers and policy implementers alike recognize the value of receiving adequate warning and timely intelligence about potential terrorist activities, and thus assign great value to obtaining access to appropriate analytical products. The crisis or surge capacity within the community is consequently relatively high, with the ability to produce analyses rapidly where information exists, as well as a cultural expectation that the intelligence will be integrated immediately into the decision-making process.

### ***Infectious Diseases***

Although the study of infectious diseases spans the full spectrum of clinical medicine, basic research, and traditional public health functions, infectious disease surveillance constitutes a primarily government activity. For the purposes of this and subsequent chapters, the “infectious diseases” culture refers to professionals engaged in disease surveillance activities, or the “systematic collection, analysis, interpretation and dissemination of health data” undertaken with an ultimate goal of introducing effective disease control measures.<sup>39</sup> The majority of disease surveillance activities take place at the local and state level, when clinical or laboratory findings of a reportable disease trigger an outbreak investigation by local or state health departments. In the past five years, the Federal government has taken a much larger role in strengthening state and local disease surveillance capabilities and creating systems for the exchange of real-time disease outbreak information.

**Training and professional criteria:** Disease surveillance is an inherently collaborative activity. Healthcare providers, local and state health department officials, laboratory technicians, epidemiologists, and researchers in academic and government laboratories play roles in recognizing outbreaks, spurring broader investigations, identifying the causes and sources of disease, and alerting policymakers and the public. Each of these disciplines requires specific formal academic training in a technical field. Post-graduate and continuing training are customary, often as part of professional credentialing requirements. Epidemiologists, who identify disease risks and distributions in populations, generally have a doctorate or medical degree with post-graduate technical training. The trainees of the US CDC’s Epidemic Intelligence Service, who may be embedded in local health departments or travel to investigate domestic or international disease patterns, in some sense represent counterparts to the professional intelligence analysts in state or local fusion centers, although the match is far from perfect.



**Tiered data ownership:** In this system of tiered analysis, most data is collected at the state and local level and shared with Federal investigators in the midst or at the conclusion of a locally instigated outbreak investigation. The collaborative nature of this work yields a system of tiered data ownership. The raw data may reside in databases and records maintained at the local or state health department, to which public access is controlled to protect individual privacy. Depending on the analytical capabilities of the local or state health authorities and the significance (either in terms of professional interest or public health urgency) of the outbreak, analysis may be conducted on site or carried out subsequently by Federal or academic researchers. Multiple groups of researchers or health authorities may enjoy varying degrees of access to the raw data. Although the data itself is rarely shared publicly without validation and analysis, it may be published in aggregate to alert healthcare providers through public forums such as the weekly reports on seasonal influenza incidence produced by the US CDC or its European counterparts.

Although outbreak data may be used tactically for disease control interventions and to inform decision-makers at various levels of government, there is a real expectation that the analyzed data will eventually be shared openly through publication in peer-reviewed journals or presentations at professional conferences. Such publications and presentations are critical not only to professional advancement for the outbreak investigators, but for other experts to become aware of the findings and to consider them valid. In most cases, the researchers or health authorities who elect to analyze the data and publish peer-reviewed articles on outbreaks or disease incidence manage the raw data. Tiered access to data is common even within Federal agencies such as the CDC, where the organization itself “owns” the data, but individual experts control access to protect data integrity (preventing accidental mishandling or misinterpretation by outside researchers) or to protect their own publication opportunities. Multi-authored publications are the norm, conferring recognition on all experts who contributed significantly during any phase of data collection and analysis.

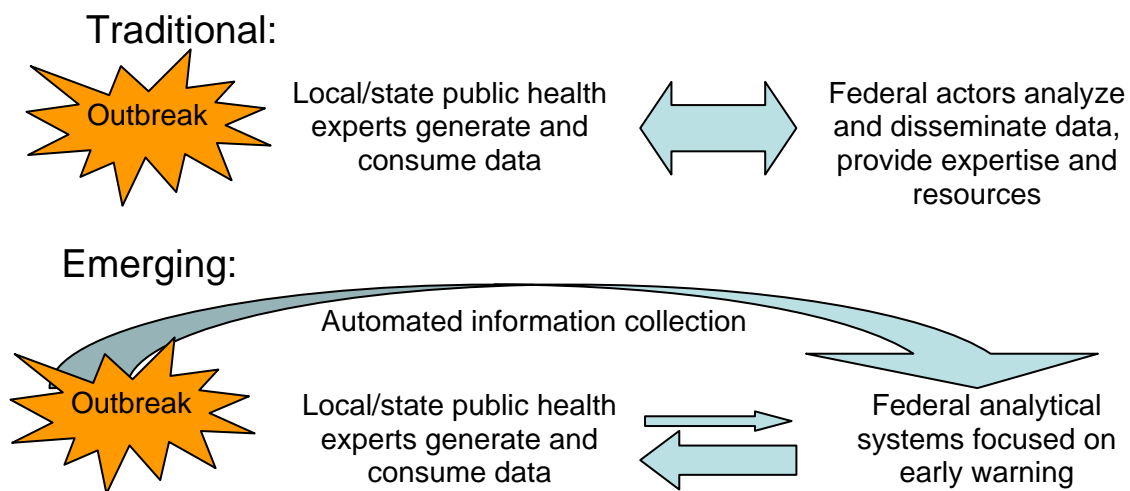
Some information about US capabilities to detect deliberate biological releases is classified, and the public health and intelligence communities continue to debate whether access to other information that might be associated with the development of or response to biological attacks should be limited. The speed with which a truly catastrophic attack is likely to unfold and the need for real-time information by clinicians, field epidemiologists, and researchers with the skills to develop diagnostic tests or countermeasures makes practical control of outbreak data problematic and potentially counterproductive. Many experts feel that the experiences during the SARS outbreak of 2003, when rapid and relatively open sharing of specimens and information allowed quick confirmation that the disease represented an emerging infection rather than a biological attack, validate the desire to keep public health information-sharing as open as possible.

**Analytical focus:** Disease outbreak investigations generally produce two types of analytical products: immediate reports that may be useful in informing policy makers, public health professionals, and the public of strategies to contain the further spread of the disease, and articles for peer-reviewed journals that are generally published weeks to months after the outbreak. Standard mechanisms for producing, sharing, and validating real-time outbreak information are still evolving. Peer-reviewed journal articles are considered highly authoritative but are rarely produced in anything approaching real time; retrospective analysis of the data generates a high degree of

confidence through confirmatory diagnostic tests and statistical evaluations that are either impractical or technically impossible to conduct immediately. These documents contain real strategic value in public health terms, including for the development of public health policy. However, the intelligence culture that traditionally advises senior policy makers on strategic threats has not yet developed mechanisms for integrating the lessons learned from previous outbreak investigations routinely into high-level decision making.

In developing global disease forecasts and other strategic reports, investigators frequently rely on disease incidence data supplied by foreign governments to the international community. The methodology for testing the reliability of these data is underdeveloped; governments may be motivated to suppress disease incidence reports to protect trade or tourism, and objective “ground truth” is rarely available in real time. The broader intelligence community tends to regard the quality of these reports with a much lower level of confidence than disease experts, reflecting the inherent political skepticism born of their training and a lack of technical health expertise that makes evaluating degrees of uncertainty (whether due to biased reporting, uneven disease detection capabilities, or simple knowledge gaps) challenging. This problem further complicates the development of strategic health intelligence products considered authoritative by both disease and intelligence professionals.

**Warning and crisis capacity:** The increasing securitization of disease threats has highlighted real tensions between public health experts in the field and those closer to policymakers and the intelligence community. Although the stakeholders in disease surveillance and response have remained relatively constant, the emphasis on who collects and first receives disease warnings has changed. Local and state experts remain primary generators and consumers of outbreak data, yet many recent programs based on the information requirements of senior policy makers have focused on mechanisms to generate early warnings through information networking and data mining, seeking to bypass the human elements in favor of a real-time data integration system.



Infectious disease experts face serious technical challenges in communicating the probable severity and timing of disease threats to policy makers. Legal, technical, and scientific data guidelines do not drive information collection; policy makers drive information collection. The infectious diseases culture has not yet developed reliable mechanisms for estimating and communicating probabilistic threats to policy makers in a way that fosters realistic contingency planning, particularly given the potentially apocalyptic nature of pandemics. Even if technical experts can describe the scope of a specific disease threat with strong certainty based on models and historical outbreak investigation data, the technological capacity to determine the timing of a catastrophic outbreak rarely exists. The Federal government has little to no capacity to forewarn state and local jurisdictions in the event of a disease outbreak or biological attack, which is a particular problem, given the extreme unevenness in jurisdictional capabilities to detect and contain such outbreaks locally.

### ***Natural Hazards***

The natural hazards community is inherently interdisciplinary, encompassing the study of phenomena associated with severe weather, seismic events, floods, and other disasters as well as the social and technical responses required to mitigate losses. Studies that involve measuring widely dispersed phenomena, such as the routine gathering of data on rivers and streams to allow accurate flood forecasting, also foster cross-jurisdictional collaborations. Most natural hazards research and detection activities in the US are supported at least in part by Federal funding, reflecting US government investment in managing and mitigating disaster risks. Many of the experts who investigate and predict severe weather and other natural hazards move relatively easily between Federal assignments and academia. Further blurring the line between academic and government natural hazards research, many of the line offices and programs under the aegis of the National Oceanic and Atmospheric Administration (NOAA)-National Weather Service and the US Geological Survey (USGS) consist of strategic research partnerships with universities. In a sense, the Federal organizations serve as boundary organizations between the natural hazards research and emergency management practitioner communities, setting priorities for basic and applied research and facilitating information-sharing. Like the terrorism information community, US government programs for natural hazards reduction experienced significant reforms and reorganizations following the creation of DHS, and in the wake of the lessons learned from Hurricane Katrina.

**Training and professional criteria:** Highly collaborative investigations at the intersection of natural hazards observation and disaster research may integrate expertise in fields as diverse as climatology, meteorology, seismology, hydrology, geology, economics, geography, law, planning, sociology, and engineering. Each of these fields requires several years of formal academic training in recognized programs, as well as specific post-graduate training or credentialing.

**Broadcasting data:** Data control principles in the natural hazards community reflect a system that assumes openness in almost every situation, from the collaborative collection of data to the public dissemination of findings through broadcast media. Because there is no adversary and public education offers real benefits in increasing community resiliency, there are few risks associated with making hazards data broadly available. In general, US policy conforms with the deeply held belief within the natural hazards community that such “data are a public good; raw data should be

openly available, and proprietary value attached only to the interpretation.”<sup>40</sup> Data controls within the natural hazards disciplines primarily involve proprietary analyses produced by insurance companies and data “retailers” who design probabilistic models by overlaying forecasts with historical data on past disasters and local geographic/structural maps to provide highly tailored risk predictions for specific industries. Most natural hazards data generated in the US lies in the public domain, largely accessible via the internet with minimal filtering beyond basic validation and occasional commercial fee requirements. Natural hazards data gathered from US satellites is routinely disseminated to researchers internationally as well as domestically. (Indeed, the openness of natural hazards data gathered from US satellites has been an issue of international trade contention, as freely available US data depresses market opportunities for other nations to offset the costs of their space programs by selling data.)

Routine updates on weather conditions are obviously accessible to communities in the US through forecasts and real-time monitoring adapted for broadcast by commercial news outlets. During severe storms, floods, and other disasters, all available relevant data is disseminated through a variety of warning systems designed to reach decision-makers at every level of government as well as the public, combining notification systems that rely on information technologies with broadcast media capabilities.

**Analytical focus:** The majority of analysis produced within the natural hazards community – encompassing data on hurricanes, tornadoes, floods, droughts, earthquakes, tsunamis, and volcanic activity – consists of academic literature produced for peer-reviewed journals and presentations for professional conferences. As in other scientific disciplines, peer recognition and professional advancement, including tenure-track promotions, primarily depend on accumulating a solid record of scientific publications and institutional leadership positions.

The reliability of natural hazards analytical products within the field depends on the traditions of scientific peer review, in which other experts evaluate the openly described methodologies and results prior to and after publication. New access to continually refined modeling techniques built on a growing body of historical data has increased the availability of authoritative products that predict natural hazards risks and behaviors, facilitating long-term strategic planning to prevent the worst impact of disasters (through evacuation plans, building codes, etc.). On the other hand, the science behind strategic macro-scale forecasting (such as estimating the likely number of hurricanes in the upcoming season) remains in development, yielding highly predictive products of generally low value to experts in the field. During severe storms and other natural disasters, the natural hazards community generates a range of generally authoritative tactical products, such as predictions of hurricane or severe storm paths.

The supply of knowledge within the natural hazards community is not always integrated with the demand for knowledge among decision-makers and their advisers. For example, decision-makers rarely have to be convinced of the value of natural hazards data and models in advance of a rapidly approaching severe storm, or when rivers are obviously rising to flood stage. However, strategic models that offer real potential for reducing disasters losses, many of which result predictably from a combination of foreseeable hazards, the social and demographic characteristics of communities,

and the physical infrastructure or “built environment,” are often neglected or even rejected by decision-makers between disasters for various political and behavioral reasons.<sup>41</sup> Because of this, ordinary events that ought to be anticipated elicit different amounts of attention from equally vulnerable communities, a particular concern given the global development of large urban centers that depend on relatively fragile lifelines.

Differences in how technical experts and decision-makers perceive the authoritativeness and utility of these strategic products stems from multiple issues. The first is simply cross-cultural communications techniques and assumptions: scientific training emphasizes detail and tends to foster the belief that a critical mass of data speaks for itself, while public officials tend to look at the “big picture” and balance scientific evidence against socioeconomic and political concerns, frequently with the optimistic view that as-yet unrealized protective technologies will emerge before the disaster occurs. The natural hazards community, based both on scientific conventions and concerns about its collective credibility, tends to be quite conservative in recommending changes in practices, models, methods, or assumptions. Technical experts frequently face challenges in communicating complex risk models in a manner that is both accurate and accessible to non-technical experts. This is complicated even further when interdisciplinary teams working on multi-faceted problems, such as assessments of community vulnerability to severe storms, introduce cross-disciplinary differences into already intractable problems with a high degree of uncertainty. Building on experiences such as those of the post-Hurricane Katrina Interagency Performance Evaluation Task Force, natural hazards experts have recognized the need to resolve conflicting technical assessments and reduce jargon in real time, so that reports can be used strategically even in draft form rather than waiting for final editing, but this is a labor-intensive and new process.

**Warning and crisis capacity:** Incremental advances in natural hazards analytical capabilities continually change the definition of “real-time” warning for various hazards. For example, increasingly sensitive detection and tracking methods have allowed major strides in hurricane forecasting, providing several days’ worth of warning to implement disaster preparedness plans, although less progress has been made in predicting the precise point of landfall. As storms approach, the news media propagate warnings issued by the USGS or National Weather Service, essentially allowing the public access to the same information available to public officials. In the case of seismic activity, information technologies can compensate for the lack of warning: although current technologies offer only a few seconds of warning for earthquakes, that interval is long enough to trigger a series of automated alerts at the local level, allowing responders to focus resources immediately on the most vulnerable systems and structures.

Information-sharing during a disaster tends to be unrestricted, but the data available from sensor networks embedded at the local and state levels may be incomplete, causing confusion about data reliability. In addition, natural hazards data released in real time during a catastrophe may lack some of the quality assurance and analytical interpretation normally available. The value of information during a catastrophic event increases dramatically exactly at the moment that systems to deliver it are most likely to be impaired. Natural hazards warning and information-sharing systems are rarely tested at the surge level of demand they are likely to experience during a

disaster; a tremendous amount of information on river levels is available on any given day, but is rarely of interest to policymakers and the public until floods begin to threaten.

Much of the investment in natural hazards warning systems has focused on the technical and logistical demands of specific announcement systems and strategies, rather than on social issues and the acceptability of the messages themselves. The perception of the urgency of natural hazards threats lies almost entirely in how decision-makers and the general public are acculturated to receive the information and act on it, not in the severity of the events themselves. Although the US and Europe annually incur billions of dollars in economic losses as well as loss of lives due to natural disasters and severe weather, information on natural hazards tends to be valued at an inherently lower level by the intelligence professionals who closely advise senior policy makers on homeland or societal security risks. Thus, while the natural hazards community comprises evidence-based and relatively robust warning capabilities, it collectively enjoys a much lower expectation of influence in the policy making process than counterparts in traditional intelligence analysis.

First, the very openness of the data precludes ownership, and may falsely suggest that the breadth of its dissemination will automatically spur necessary policy decisions. Second, the natural hazards community's profile in preventing loss of lives and damage to critical infrastructure in the purview of security has been raised only recently. Many agencies and organizations contribute to natural hazards information collection and sharing, including local governments, academic institutions, and the private sector, and no clear agency leadership has been cultivated to represent the community routinely to senior level policymakers. This perpetuates an imbalance of systems, structures, and resources for sharing information on natural hazards in a strategic fashion, within fusion centers and other local and state decision-making structures as well as at the top government levels.

---

— 4 —

## POLICYMAKERS' NEEDS (AND WANTS)

This chapter considers basic problems in how information flows to policymakers, in theory and in practice, and identifies concerns of government officials in the US and Europe regarding the enduring problems of creating reliable and predictable information flows. It also considers the dilemma for information providers regarding wants vs. needs: who decides what information is most relevant and necessary for different levels of government action? In times of crisis, it is virtually impossible to tell a decisionmaker who may face media or parliamentary scrutiny that he or she should remain strategic in focus and not get too involved in operational details or try to master a complex and scientific topic. Government intelligence and information systems spend a lot of time paring back large volumes of empirical data into short, digestible forms, gleaning the strategic message for the most senior government officials, and gauging the absorptive capacity of information users at different levels of government. Aligning the mutual expectations and interactions between information experts and decision-makers remains an elusive goal.

### *Warning in Complex Threat Environment*

Each of the three kinds of information needs we focus on – terrorism, health and natural hazards – represents bad things that can happen quickly and require fast government responses. Each also represents strategic challenges that need to be studied over time for patterns and explanations to enhance strategic planning, reduce vulnerabilities and mitigate consequences of. But for the busy all-hazards government actors, warning of pending disaster is the fundamental and essential information need.

It is useful to reflect on how the concept of warning has changed, in the transition from a world of a peer adversary in a potentially existential geopolitical contestation to a world of unlimited dangers from multiple causes, but few of an existential scale that would help order and organize information collection and analysis.

In the age of globalization challenges, from disease to climate change to extremist non-state actors, the art of warning is no longer managed through the lens of military organization and threat assessment. Warning is part of three different analytic approaches:

- Warning as a byproduct of daily activity and analysis by experts
- Persistent surveillance for a specific outcome/event with routine reporting
- Strategic reconnaissance – looking for early signs of threat and opportunity

These three categories also generate different kinds of warning products. Some are the natural and habitual byproduct of daily intelligence analysis (including the President's Daily Brief), which are only provided so that the decision-maker is able to react to fast-breaking or current situations. Consumers are all too often overly interested in this type of product. A second type relates to

specific regions or subject areas that are continually monitored (including persistent surveillance on India/Pakistan), and creates a strategic warning – this is the most traditional notion of warning. A third category is strategic reconnaissance, which considers the emerging security environment, looking for very early signs and threat indicators to allow for proactive policies rather than reacting to crises. It may not be fair to ask intelligence analysts to cover all three types of warnings, as the skill sets required for each technique are so unique.

One solution would be to separate the warning mechanism from the Intelligence Community for anything other than current, tactical, day-to-day surveillance and warning. Since they are not trained to deal with uncertainty and complex issues, current intelligence analysts should not be relied upon for strategic warning, which could engage non-government experts in a more sustainable fashion than current practice.

### ***All-Hazards Challenges***

Policymakers are also aware that the fast shift from traditional threats to the new “all-hazards” approach has generated new bureaucratic and cultural tensions. The different information cultures and worlds do not know each other or fully understand each others’ research methodologies, and have little or no experience working together. The all-hazards world requires agility and ability to work in cross-disciplinary teams. Policymakers also feel the pressure from a public that is more sophisticated due to information technology, and, in the aftermath of Hurricane Katrina in the US and catastrophic floods and terrorist incidents in Europe, demands more competent government responses. Prosperous societies are more risk-averse, in part because they have more personal property to protect, and in part because governments create an expectation that risk can be reduced to negligible levels.

The organizational changes in both US and EU systems relied at the outset on intelligence community experts and management, who lack expertise in environment and health fields and do not have established relationships with those communities. DHS wants to break out of its terrorism-centric mindset and focus on all-hazards; however, national intelligence is not yet to this point. Europeans face the same difficulties fusing terrorism, natural hazards and infectious disease information sharing and crisis management, compounded by the fact that it is officially mandated to the Member States but inherently part of the EU itself due to integration. The Union organizes by sector, but the States do not, and this creates a problem of alignment.

### ***Defining the Customers and their Needs***

The customer base for all-hazards information is quite diverse, and this creates challenges for information and intelligence experts in designing collection strategies and developing useful products. While state and local entities desire tactical, actionable intelligence that pertains to their specific regions, factors such as data classification and a lack of understanding of the true needs of first responders hinder the ability of the federal government to provide them with this information. There are also costs, in terms of time and resources, in developing distinct information products for customers at different levels of government, and with different functions, such as homeland security and law enforcement.



Both the US and EU face similar challenges in adapting what had previously been a closed, secret system of national security intelligence for a limited set of customers, to a more open system that enables first responders as well as national policymakers to access useful information and data in times of crisis. Collaboration among information systems, integration of classified and unclassified information, and authorities to share with officials at different levels of government are common problems. It is also clear that providers of information and users may hold distinctly different views about how authoritative and useful is the information provided.

Intelligence products must reflect the needs of the consumer, but those customers include both policy level and operations personnel, those working at the tactical as well as strategic levels, etc. Some officials straddle both sides of these divides, especially at the state level. Until recently, the intelligence community tended to define its customers for information as high level officials with relevant federal intelligence agencies. Creating intelligence products for state and local jurisdictions was considered to be much less important. There has been a recent push within DHS I&A to create a customer-oriented approach to information dissemination for customers at the state and local levels. The fusion centers help towards achieving this goal. Yet, DHS I&A and other related agencies still struggle in terms of determining what kinds of analytic products to create for these communities and more importantly, how to disseminate them without releasing more information than needed. The information also flows in both directions: one of the National Operation Center's biggest challenges is also how to fuse information coming in from the state and local level with federal-level intelligence products without comprising national security.

Some decision-makers do not make a careful enough distinction between their wants and needs: policy-makers require knowledge, often at an aggregated level, with which to make decisions and implement policy, whereas those responsible for implementing decisions may well need more tactical, fine grained data. With the pressure of public scrutiny and press attention, many senior officials believe they need to master the deeper level of detail. This can create friction or misunderstanding with information providers, who are attempting to meet requirements for different levels of government.

Both the EU and US find that they have an alignment problem between customers at various levels of government, and the organizational structures for information. In the US, for example, state and local entities are geographically organized, while the federal government is arranged by sector or field. Federal level intelligence officers often do not know how to engage with people at the state or local level, and those who are responsible for acting in the event of a crisis are rarely integrated into the new fusion centers and operations centers where intelligence is available.

In Europe, there are issues about the responsibilities of the member states versus Brussels, with a need to find an acceptable balance between what the national level and Union levels are responsible for handling. Member states are strengthening their infrastructures and coordination to support EU information sharing requirements, but Union-level warning systems appear to be overly complex. Some members, including Sweden, are bypassing Brussels and coordinating directly with each other. At the same time, Member States such as Sweden are not opposed to increased coordination

with the EU level. In addition, Europeans find an alignment problem when they try to identify their counterparts in the US system.

Within the three information cultures we studied, there are also specific issues that arise in engaging with this expanding customer base.

- The health professionals feel that the center of gravity is shifting. Data collected at the local level was transmitted to appropriate federal entities; now, with greater reliance on technical systems to disseminate data, those local public health officials feel their role has diminished, as federal actors pull the information they need, bypassing the deep knowledge and expertise of local officials.
- Health experts also recognize that their reliance on proven scientific methodologies for analyzing disease patterns needs to be enhanced with methods used by the intelligence community that would provide quicker findings and enable the health community to engage more effectively with federal and state officials, should a disease outbreak occur.
- The terrorism community acknowledges that it has yet to develop comfortable new protocols for engaging with state and local officials. But in major urban centers, such as New York, law enforcement has successfully recruited retired intelligence officers with deep terrorism experience, and these human connections can facilitate new relationships.
- Building more mutual understanding and stronger relationships could be achieved with more revolving-door career patterns. Weather experts appear to move the most easily between academia and government, and terrorism experts move the least easily. Equally important is for information experts within government to have opportunities to serve on rotations in policy offices. Such experiences bring great value over time to these essential relationships, across the policy/intelligence divide, and across the government/academic divide.

### ***Culture and Secrecy***

The culture of information sharing has evolved as new threats have entered the homeland security paradigm. Terrorism, a primary security concern, comes with a culture that emphasizes the classification of intelligence, and has occupied the forefront of the national dialogue on homeland security. Threats such as natural hazards and infectious disease come with cultures that focus more on information sharing than classification, and are frequently perceived as less important than terrorism.

Some estimate that within the intelligence community (IC), 95% of valued information has been collected clandestinely, and the other 5% from open sources. In the public health community, these percentages are reversed. During crisis simulations involving traditional intelligence analysts, analysts performed well on terrorism scenarios but failed the exercise on pandemic emergency, due

to the fact that they would not seek information from the CDC because CDC employees did not hold security clearances, even though the analysts were merely tasked to gather information, not to protect or share anything of their own.

Information sharing is often seen as existing within a “power culture,” in which classified intelligence commands respect, and open-source data is frequently disregarded, no matter its value. In our exploration of the three information cultures, it was clear that the terrorism community has the most power, and weather experts the least. In the former case, it is assumed that most information is classified and available only to those who need to have access, whereas in the latter case, information from weather satellites is instantly available to anyone with internet access, and is often taken for granted as a public good.

It is important to not view information as a commodity; a better analogy would be that intelligence provides a nourishing meal, but open source information is the air that analysts breathe.

### ***Inter-agency Distrust***

Obstacles to effective information sharing between various emergency response organizations as well as homeland security agencies tend to be cultural in nature. Even today, information sharing tends to be dependent largely on personal relationships and trust between members of various organizations, generally within the same discipline. There are historic cultural barriers that impede effective collaboration between different emergency response communities that ideally should work together. For example, pandemic disease is public health, homeland security, as well as law enforcement concern. However, these communities are yet to find an effective way to facilitate a smooth process of information sharing for this issue in terms of planning, preparedness, as well as response activities.

### ***Legal Barriers and Over-classification***

There are also legal considerations that sometimes impede effective inter-agency information sharing. Some federal, state, and local agencies tend to have more robust information sharing rules and laws to prevent mismanagement of information than others. For instance, if agency X has stricter information sharing rules than agency Y, then agency X will not wish to share information with agency Y because agency Y may share agency X’s information and data with third parties not approved by agency X.

Information sharing is frequently impeded by classification of data or analytical products considered to be sensitive for national security purposes. Emergency response organizations at the state and local levels often are denied access to information that would be useful in helping them achieve their homeland security missions. Security clearances are provided to only select members of these organizations; however these members are restricted from sharing sensitive information with their counterparts in their agencies. DHS officials justify restrictive security clearances for state and local officials as allowing these officials an appropriate level of access to all information that they have a need to know about. They also claim that DHS already is sharing all relevant information with state and local agencies and is not engaged in restricting access to necessary information. State and local personnel suggest that DHS should expand its clearance issuances to

more members of the state and local emergency response community to more fully include officials that need to access such information.

## CHALLENGES AND CHOICES

This study offers an early examination of the challenges of information support to “all-hazards” decision-makers and crisis managers in the world of 21<sup>st</sup> century threats. It provides some broad ways to think about how to integrate information and intelligence, to create more productive relationships across diverse expert communities, and to increase the satisfaction and effectiveness of the users of this information, at different levels of government in the United States and Europe. It also identifies opportunities for deepening and improving transatlantic cooperation on information sharing.

Much of the research, based on public documents and dozens of interviews with people in government and in non-government expert communities, identified even more problem areas or possible solutions than are mentioned here. Many in the homeland security community are action-oriented, and they move quickly from information needs to actual response requirements. This study focuses more on the information needs, before and at the beginning of a crisis, rather than on the entire life cycle of a crisis response. The information/intelligence input is most important and valued most in these early phases of a crisis; once the response begins, actors get in a rhythm of information input/decision and action output. The information problems discussed here pertain mostly to the early, and often chaotic, stages of a crisis and government response, as well as the strategic challenge of warning and information inputs long before a crisis erupts.

We found a high level of awareness of the need to improve information sharing, and a remarkable number of new initiatives, organizational changes and efforts at reform that have taken place in the past eight years. On the US side, the creation of fusion centers outside of Washington is an important achievement in a system that usually pulls information and power to the center, whereas in Europe, the achievement has been to build more capacity at the EU level, and to attempt to clarify boundaries and protocols for Member-Union authorities and relationships. But all of these efforts are works in progress, and this report does not attempt to evaluate their quality or effectiveness to date. It is clear that personnel in the large, complex bureaucracies are not yet fully familiar with these new arrangements, and relationships of trust will take time.

Several of the structures and processes that have emerged on the EU level are in response to a crisis or a near-miss. Many examples can be found in the establishment of early-warning systems in various sectors, one is the Rapid Alert System for Biological and Chemical Attacks and Threats (RAS-BICHAT). Another is the establishment of a Community mechanism for civil protection in October 2001 that can facilitate resources and information between member states. It points to a reactive event-driven environment where evidence of weakness in the system must be experienced to be acted upon. Thorough analysis of the EU's strategic environment and future risks need to be performed on what societal security tasks are better performed at the EU-level.

We also note that the interactions between information providers and government users are best thought of as an ongoing process, not a one-dimensional transmission of information to the

customer. In the highly evolved government structures of western democracies, government users can influence and shape the information support systems through dialogue over requirements, which in turn drive how information and intelligence systems set priorities and allocate resources. We found in our comparisons of the three information cultures that terrorism was the most sensitive to this symbiotic relationship between customer and provider, while natural hazards experts were driven more by their own investigative methods, and the health culture was in the middle.

### ***Increasing Ties Across Information Cultures***

Our examination of terrorism, health and natural hazards as distinct information cultures suggests that they have different professional reward systems and different attitudes about the relationship of their knowledge to government decisions and actions. The three represent a spectrum, with terrorism as a closed information world with inherently governmental purpose and application, health is both official and scientific, and natural hazards, while linked to government, is an information system that relates naturally and automatically to wider societal users, not exclusively government.

Due to the severity of the early 21<sup>st</sup> century terrorism and natural hazards crises, these different communities are becoming more accustomed to working together in hybrid teams. In the United States, for example, the worlds of terrorism and health sciences are now linked through the shared concerns about bioterrorism, the possibility of terrorists using biological agents as weapons, or inducing a disease in a target population as an act of war. In humanitarian crises caused by natural disasters, health workers are a core part of a governmental response, and they bring disease surveillance techniques with them that provide important knowledge about the effects of natural disasters that are critical to government action and priority-setting.

But back in capitals, large communities of experts tend to work in their respective lanes, with a very small percentage of analysts working in cross disciplinary teams or settings. It is also clear that the three issues we considered, both on their own merits and as surrogates for a wider set of issues, have distinct rewards systems with respect to collaboration with non-government or non-national networks. For terrorism experts, such collaboration is often circumscribed by security rules, or is conducted in formal liaison channels. For health and natural hazards experts, there are larger more porous academic and scientific networks where collaboration across borders and between government and non-government experts is natural and non-controversial.

Government officials engaged in promulgating a new “all-hazards” way of thinking stress the need for the public health community to start looking at international threats and developing a better understanding of the intelligence component of health security as national security. In the US, it could well take at least a decade to achieve insightful health and intelligence leadership that can facilitate peaceful coexistence and even active collaboration between the communities. This will include developing new methodologies to warn and acquire more quickly useful knowledge about disease trends and forecasts; it will also require sensitivity and understanding regarding the use of the word “security” to define the value and mission of the health information world. This community, like the weather community, serves society and does not necessarily see its mission as serving a national or homeland security purpose.

We offer some modest suggestions for improving ties between information communities that can be accomplished with strong leadership, and would not require legislative remedies or structural change:

- Create informal networks, such as monthly discussions of all-hazards information experts, to share knowledge and create more familiarity with the substance and the players.
- Ensure that there are clear counterparts at the expert or first-line manager level among the different all-hazards topics (terrorism, health, environment, weather, etc.).
- Make sure that weather and environment are represented in all-hazards homeland security threat assessments; they need a seat at the table to be treated as peers.
- Offer training several times a year for both experts and for policymakers, to ensure that people understand the existing systems and their capacities.
- Inculcate new values and rewards for a new generation of analysts who are more adept at working in a hybrid classified/unclassified information environment. Allow them to operate in a less restricted security culture so that a true fusion of all available information, across disciplines and sources, is permitted.

### ***Improving Ties between Information Cultures and Policymakers***

Communicating effectively to decision-makers is an enduring challenge for intelligence and information providers in government; it is not unique to the homeland security mission, but that mission has, in the US case in particular, a special burden since the threat menu keeps expanding, and the level of public and political scrutiny is high.

At the federal or EU level, the issues of complexity and access to power are paramount. Both the US and EU systems keep adding components to address discrete requirements, but busy decision-makers lose track of with whom or where the authoritative all-source information resides. Access to power is also a key issue, and systems, such as the Crisis Management Secretariat in the Swedish Prime Minister's office and the National Security Council, create units that are coordinators, rather than producers, of key information. There is a question, but no easy answer, as to whether these information intermediaries are an effective alternative to having intelligence professionals available 24/7 to brief policymakers. Experts also believe that agencies, such as the Department of Homeland Security, can play a direct role, rather than having a duplicative structure of a Homeland Security Council in the White House, which creates a power struggle with senior DHS officials who see their role as briefing White House principals.

A second set of issues relates to vertical and horizontal flows of information, determining who has a need to know, security protocols for sharing below the national or federal level, and setting rules for the hand-off of information from fusion center monitors to real first-responders. There are problems of trust between career intelligence and other disciplines, and it is not clear how much priority or value is assigned to the fusion of intelligence and open-source material. Overall, the creation of new systems below the federal level, such as the US fusion centers (several dozen have been established to date, less than half of the total plan), is well intended and appears to be solving

some of the underlying problems of bringing appropriate information to the state and local levels, but more data gathering and assessment of their utility to various customers is needed.

In the EU system, the problem of vertical flows is different. Member states are accustomed to sharing with each other on discrete topics, but less familiar with sending material to Brussels, to offices and entities of recent vintage that do not have well established track records or even a core mission to use the information for shared purpose. (This may be comparable to the feeling in the established intelligence agencies in the US regarding the new Office of the Director of National Intelligence; the agencies seem to feel they give more than they get from ODNI. Information or resource sharing has not yet proven to be mutually beneficial.)

### ***Deepening Transatlantic Cooperation on All-Hazards Information and Policy Responses***

2009 represents a great opportunity for a new look at US-EU cooperation on all-hazards information sharing and crisis management. A new US administration will be making some decisions about the homeland security mission as part of its internal review and setting of spending priorities. The EU, under Sweden's presidency (July-December 2009), is likely to set an ambitious agenda for US-EU cooperation, and homeland or societal security issues could be a promising area for new action.

The EU Lisbon Treaty, which was to come into force on January 1<sup>st</sup> 2009 if ratified by all member states, is currently in limbo. It would have provided several key components to achieve a groundbreaking framework in the area of EU societal security. Three noteworthy components are the introduction of a Solidarity Clause, inclusion of an article on civil protection, and a new standing committee on internal security under the EU Council.<sup>1</sup> These pieces would have the effect of shifting influence on many issues areas in the societal security arena from being primarily an area under the control of the member states to the EU level. In areas such as border patrol and immigration issues, judicial and police operations, critical infrastructure protection, visa and passport procedures, counterterrorism efforts and the fight against organized crime, issues would be decided with majority vote rather than unanimity. The Commission will be able to put forward initiatives in a more forceful way than before. The European Parliament would as well become a significant partner in the area. Should the treaty's prospects improve, this would create new momentum and a more favorable alignment for US-EU collaboration and cooperation.

Each member state is responsible for managing crises and catastrophic events. It should be remembered that the EU was not constructed to be a fast-paced crisis management machine. It was designed to slowly remove barriers and integrate separate European nations to a peaceful and prosperous whole. But as experience has shown, and a little creative thinking can illuminate, it is not a stretch to imagine that crises of the future will have far-reaching consequences that can potentially overwhelm even the most resource rich and prepared nation. Current and future realities may prove to be too challenging for nations to manage in isolation.

The institutional design of government, however, is slow to adapt to a changing environment. There is an historical legacy of separating agencies and departments operating in either the domestic or the international sphere. Failing to address jurisdictional, organizational, and even mental barriers



for national and international organizational cooperation will be at our peril, for example organized crime and terrorists maneuver in the transborder sphere that causes challenges for “old” organizational structures. Exploring new ways to cooperate in planning, information exchange, training and response is critical for the future.

As the Homeland Security policy area is slowly maturing in the US and is embryonic in the EU, the time is ripe for an informed and inclusive transatlantic dialogue on shared challenges and opportunities. While it is not necessary for the same institutional and strategic concepts to be embraced on both sides of the Atlantic, it is important that the respective efforts reinforce, and not undermine, the hard work being done to improve homeland/societal security.

### ***Conclusion***

This exploration of three information cultures for all-hazards government responses demonstrates the daunting challenge of creating an easy fusion of knowledge across different disciplines and cultures. The professional cadres in the health, natural hazards and terrorism fields have developed by different methods, and have evolved different incentives and rewards for achievement. Each sees its relation to government action differently, but parts of these three communities are actively engaged in adapting their respective field to the new twenty-first century security environment. We found considerable receptivity to further enhancing the ability of US and EU experts to communicate with government, in order to inform and improve government responses to all-hazards contingencies.

Progress will not be quick; the iron laws of bureaucracy, to use the memorable phrase of the 2005 Commission on Intelligence Capabilities, suggest that large organizations are self-reinforcing, risk averse, and not prone to accepting outside advice.<sup>42</sup> The slowness of institutional change is coupled with the challenge of introducing new incentives and rewards for serious professionals whose achievement and career success is measured by long-established methods and metrics. Many experts in the fields of health, natural hazards and terrorism may not be motivated to rethink their approach to their work and its impact on the lives of fellow citizens. But this study suggests that there are bridge-builders who see the connectedness of the all-hazards issues and are stimulated by the challenge of creating new knowledge across established fields and achieving more impact by working together.

The US and European Union can benefit from more robust exchanges about all-hazards early warning and response. The US brings to the table its experience in building such a large and complex intelligence infrastructure that is now adapting to new reforms; the EU brings deep experience in building its response systems for “societal” security that could help shape ideas for more effective integration of effort at all levels of government. The differences in approach and in priority do not diminish the deep sense of shared values and common purpose across the Atlantic. The twenty-first century will continue to generate its surprises and security challenges that will require creative and agile information systems; sharing knowledge about the specific threats and establishing productive government-to-government interactions about our respective responses will be a worthy contribution to a safer world.

1 For more information, see the NCTC's statement of purpose ([http://www.nctc.gov/about\\_us/what\\_we\\_do.html](http://www.nctc.gov/about_us/what_we_do.html))

2 Government Accountability Office, GAO 08-636T. Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers. Statement of Eileen R. Larence, April 17, 2008.

3 Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, August 2006, 2, available from [[http://it.ojp.gov/documents/fusion\\_center\\_guidelines\\_law\\_enforcement.pdf](http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)], accessed on January 20, 2008.

4 GAO 08-636T, Statement of Eileen R. Larence.

5 Government Accountability Office. GAO-07-455. Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information Sharing Initiatives. April 2007. [www.gao.gov/cgi-bin/getrpt?GAO-07-455](http://www.gao.gov/cgi-bin/getrpt?GAO-07-455).

6 Crystal Franco. "Billions for biodefense: Federal agency biodefense funding, FY 2008-2009." *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 2008; 6(2):131-146.

7 World Health Organization, International Health Regulations (2005), <http://www.who.int/csr/ihr/en/>

8 General Accounting Office, Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts. Washington, DC, 2004.

9 US Centers for Disease Control and Prevention, Epidemic Intelligence Service Fact Sheet, accessed online at <http://www.cdc.gov/eis/about/factsheet.htm> in August 2008.

10 USGS Fact Sheet: Flood Hazards--a National Threat, <http://pubs.usgs.gov/fs/2006/3026/> .

11 Arjen Boin, Paul 't Hart, Eric Stern, and Bengt Sundelius (2006) *The Politics of Crisis Management: Public Leadership Under Pressure*. Cambridge University Press

12 The EU maintains a number of collective databases, including:

#### *TECS*

The European computer system is maintained by Europol and collated by Member State's ELOs. TECS is organized into two categories of intelligence. First, the European information system is a catalog of indicted and suspected criminals and terrorists including personal information, group characteristics, connections with other groups or individuals, details of committed crimes and any future suspicions. The second system consists of intelligence work files detailing specific criminal and terrorist incidents, which are drafted by various ELOs and Europol employees. (Walsh, J. I. (2006, September). *Intelligence-Sharing in the European Union: Institutions Are Not Enough*. *Journal of Common Market Studies*, 44(3), 625-643. Retrieved from Social Science Research Network database. Pages 632-633 cited here. )

#### *Eurodac, Schengen Information System & Visa Information System*

These databases contain information on individuals immigrating throughout the EU in order to locate illegal individuals who may wish to disrupt EU security. More specifically, Eurodac focuses on asylum seekers, the Schengen Information System (SIS) tracks individuals moving into and out of the Schengen region (including France, Germany, Belgium, Luxembourg and the Netherlands (For more information about SIS please see: <http://europa.eu/scadplus/leg/en/lvb/l33020.htm>) ). and the Visa Information System (VIS) ensures that common visa standards prevent visa fraud and other criminal immigration attempts in order to ensure internal EU security (For more information about VIS please see: <http://europa.eu/scadplus/leg/en/lvb/l14517.htm>) (Keohane, D. (2005, May). *The EU and counter-terrorism (Working Paper)*. Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Page 30 cited here)

#### *EU Watch List*

Continuously discussed and updated by Member States' intelligence professionals, the EU Watch list contains information of the most pertinent threats to EU security, such as individuals suspected or confirmed as terrorists. The List is maintained by the Production branch (and in partnership with the Policy branch) of the EU Military Staff's Intelligence Division and in coordination with the EU Commission. (Antunes, J.

---

N. J. V., Maj. Gen. (2005). Developing an Intelligence Capability: The European Union. Studies in Intelligence: Unclassified Edition, 49(4). Retrieved from CIA Center for the Study of Intelligence Web site: [https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/Intelligence%20Capability\\_6.htm](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/Intelligence%20Capability_6.htm)).

#### *Emergency Response Capability Databases*

In the aftermath of the 2004 Madrid Bombings, EU governments agreed to increase collaboration for emergency response. A database housing details of emergency response capabilities for all Member States was created to supplement the existing EU Commission's environmental directorate's response centre. Established along with this database was the custom of an open dialogue between members for peer review of current emergency response capabilities as well as recommendations for future improvements. (Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site:

[http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Pages 32-33 cited here.)

13 Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Page 22 cited here.

14 Walsh, J. I. (2006, September). Intelligence-Sharing in the European Union: Institutions Are Not Enough. Journal of Common Market Studies, 44(3), 625-643. Retrieved from Social Science Research Network database. Pages 225-226 cited here.

15 Additional information on both agencies available at <http://europa.eu/scadplus/leg/en/lvb/l33188.htm> and <http://europa.eu/scadplus/leg/en/lvb/l33216.htm> respectively.

16 <http://www.europol.europa.eu/index.asp?page=facts>

17 Walsh, J. I. (2006, September). Intelligence-Sharing in the European Union: Institutions Are Not Enough. Journal of Common Market Studies, 44(3), 625-643. Retrieved from Social Science Research Network database. Page 632 cited here.

18 <http://www.europol.europa.eu/index.asp?page=facts>

19 Walsh, J. I. (2006, September). Intelligence-Sharing in the European Union: Institutions Are Not Enough. Journal of Common Market Studies, 44(3), 625-643. Retrieved from Social Science Research Network database. Page 631-632 cited here.

20 Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Page 15 cited here.

21 Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Page 31 cited here.

22 Villadsen, O. R. (2000, Summer). Prospects for a European Common Intelligence Policy. Studies in Intelligence UNCLASSIFIED EDITION, 9, intelligence today & tomorrow. Retrieved from Central Intelligence Agency Web site: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art07.html>

23 Walsh, J. I. (2006, September). Intelligence-Sharing in the European Union: Institutions Are Not Enough. Journal of Common Market Studies, 44(3), 625-643. Retrieved from Social Science Research Network database. Page 631 cited here. Also utilized 2004 Swiss fedpol press release retrieved from [http://www.ejpd.admin.ch/ejpd/en/home/dokumentation/mi/2004/ref\\_2004-04-28.html](http://www.ejpd.admin.ch/ejpd/en/home/dokumentation/mi/2004/ref_2004-04-28.html) Pages 625-626 cited here.

24 Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Page 19 cited here.

25 It should be noted that the Interior Ministers are responsible for these and other multilateral partnerships throughout Europe which focus on terrorism, while NATO counterterrorism strategies are developed by the Foreign and Defense Ministers of European states. This is one inconsistency that must be overcome in order to facilitate increased collaboration in the European Union for security purposes. For source, see the following endnote.

- 26 Keohane, D. (2005, May). The EU and counter-terrorism (Working Paper). Retrieved from Center for European Reform Web site: [http://www.cer.org.uk/pdf/wp629\\_terrorism\\_counter\\_keohane.pdf](http://www.cer.org.uk/pdf/wp629_terrorism_counter_keohane.pdf) Pages 14-22 cited here.
- 27 Matzén, N. (2007) An Ascending Sector: The European Union's Role in Health Protection, in *Protecting the European Union – Policies, Sectors and Institutional Solutions*". Swedish National Defence College.
- 28 GREEN PAPER ON BIO-PREPAREDNESS, (presented by the Commission, Brussels, 11.7.2007. COM(2007) 399 final. [http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007\\_0399en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0399en01.pdf)
- 29 Annual Report of the Director (2007) European Centre for Disease Prevention and Control. Page 15. [http://ecdc.europa.eu/pdf/Director\\_annual\\_report\\_2007.pdf](http://ecdc.europa.eu/pdf/Director_annual_report_2007.pdf)
- 30 Surveillance of communicable diseases in the European Union. A long-term strategy | 2008–2013. European Centre for Disease Prevention and Control. [http://ecdc.europa.eu/documents/pdf/Surveillance\\_of\\_CD\\_EU.pdf](http://ecdc.europa.eu/documents/pdf/Surveillance_of_CD_EU.pdf)
- 31 Kaiser R, Coulombier D. Different approaches to gathering epidemic intelligence in Europe. *Euro Surveillance*. 2006;11(17):pii=2948. Available online: <http://www.eurosurveillance.org/ViewArticle.aspx?ArticleId=2948>
- 32 Surveillance of communicable diseases in the European Union. A long-term strategy | 2008–2013. European Centre for Disease Prevention and Control, page 4. [http://ecdc.europa.eu/documents/pdf/Surveillance\\_of\\_CD\\_EU.pdf](http://ecdc.europa.eu/documents/pdf/Surveillance_of_CD_EU.pdf)
- 33 For an overview of natural disasters recently effecting Europe and other implications of climate change, please refer to the EU's 2006 Joint Public Hearing Natural disasters - How should Europe respond? Assessable at [http://www.europarl.europa.eu/comparl/envi/hearings/natural\\_disasters/speeches\\_en.htm](http://www.europarl.europa.eu/comparl/envi/hearings/natural_disasters/speeches_en.htm)
- 34 Communication From the Commission to the European Parliament and the Council on Reinforcing the Union's Disaster Response Capacity (COM(2008)130 final). (2008, May 3). Retrieved from the European Commission Web site: [http://ec.europa.eu/commission\\_barroso/president/pdf/COM2008\\_130\\_en.pdf](http://ec.europa.eu/commission_barroso/president/pdf/COM2008_130_en.pdf) Page 2 cited here.
- 35 Official website of the European Commission's Environment Directorate-General's Civil Protection Unit: <http://ec.europa.eu/environment/civil/index.htm>
- 36 A list of national civil protection and disaster response authorities is available at: [http://ec.europa.eu/environment/civil/prote/cp10\\_en.htm](http://ec.europa.eu/environment/civil/prote/cp10_en.htm)
- 37 9/11 Commission Report . Washington, DC: 2004, accessed online at <http://govinfo.library.unt.edu/911/report/index.htm> in August 2008; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report to the President. Washington, DC, :2005, accessed online at. [http://www.wmd.gov/report/wmd\\_report.pdf](http://www.wmd.gov/report/wmd_report.pdf) in August 2008.
- 38 Office of the Director of National Intelligence, Intelligence Community Information Sharing Strategy Washington, DC, 2008. Accessed online at [http://www.dni.gov/reports/IC\\_Information\\_Sharing\\_Strategy.pdf](http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf) in August 2008.
- 39 World Health Organization. Report on global surveillance of epidemic-prone infectious diseases. Geneva, Switzerland: WHO, 2000.
- 40 Timothy A. Cohn, Kathleen K. Gohn, and William H. Hooke, eds. *Lessons from PPP2000: Living with Earth's Extremes*. Tampa, FL: Institute for Business and Home Safety, 2001.
- 41 Denis Mileti, *Disasters by Design: A Reassessment of Natural Hazards in the United States*. Washington, DC: Joseph Henry Press, 1999.
- 42 The Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction, March 31, 2005, p. 6. Full text can be found at [www.wmd.gov](http://www.wmd.gov).

---

## Selected Readings

- Allen, Charles, E, Under-Secretary for Intelligence and Analysis. Testimony before the Senate Committee on Homeland Security and Governmental Affairs. *Information Sharing at the Federal, State and Local Levels*. 2008.
- Boin, A., Hart 't, P., Stern, E., Sundelius, B. The Politics of Crisis Management: Public Leadership Under Pressure. Cambridge: Cambridge University Press. 2005.
- Cecchine, Gary and Melinda Moore. *Infectious Disease and National Security Strategic Information Needs*. RAND Corporation. Arlington, VA. 2006.
- European Centre for Disease Prevention and Control (ECDC). *Meeting Report: Epidemic Intelligence in the EU*. Stockholm: 18-19 January 2006.
- Government Accountability Office. *Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts*. Report GAO-04-877. Washington, DC: GAO, 2004.
- Homeland Security Council. *National Strategy for Pandemic Influenza*. Washington, DC, November 2005.
- Informal High Level Advisory Group on the Future of European Home Affairs Policy (Report of "The Future Group"). *Freedom, Security, Privacy -European Home Affairs in an open world*. June 2008.
- Müller-Wille, Bjorn. For Our Eyes Only? Shaping an Intelligence Community within the EU. EU Institute for Security Studies. 2004.
- Müller-Wille, B. *The Effect of International Terrorism on EU Intelligence Co-operation*. Journal of Common Market Studies, Vol. 46, Issue 1, pp. 49-73, January 2008.
- Pawlak, P. *From Hierarchy to Networks: Transatlantic Governance of Homeland Security*. Journal of Global Change and Governance, Volume 1, Number 1, Winter 2007.
- Protecting the European Union: Policies, Sectors and Institutional Solutions. Eds. Boin, A., Ekengren, M., Rhinard, M. Swedish National Defence College. 2007.
- Protecting the Homeland: European Approaches to Societal Security - Implications for the United States. Eds. Hamilton, D., Sundelius, B., Grönvall, J. Washington, DC: Center for Transatlantic Relations. 2007.
- Rollins, John. CRS Report for Congress. *Fusion Centers: Issues and Options for Congress*. 2008.
- Security in Transition: Towards a New Paradigm for the European Union. Eds. Boin, A., Ekengren, M., Rhinard, M. Swedish National Defence College. 2008.

---

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. 2005.

The 9/11 Commission. *Final Report of the National Commission on Terrorist Attacks upon the United States*. 2004.

Transforming Homeland Security: U.S. and European Approaches. Ed. Esther Brimmer. Washington, DC: Center for Transatlantic Relations. 2006.

Vision 2015 - A Globally Networked and Integrated Intelligence Enterprise. DNI  
[http://www.dni.gov/Vision\\_2015.pdf](http://www.dni.gov/Vision_2015.pdf)

White House Katrina Report. <http://www.whitehouse.gov/reports/katrina-lessons-learned/>. 2006.