THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

MAY 2013
VOLUME 11 NUMBER 11

INTERNATIONAL CIP

EDITORIAL STAFF

EDITORS
Kendal Smith

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Melanie Gutmann

Click here to subscribe. Visit us online for this and other issues at
http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

In this month's issue of *The CIP Report* we present our annual review of international topics in critical infrastructure.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, Assistant Secretary for Infrastructure Protection Caitlin Durkovich describes U.S. efforts to enhance critical infrastructure resilience around the globe. Next, Intellium CEO Matthew Holt discusses infrastructure protection in the European Union, and Professor Damien Serre presents a method for modelling network interdependencies to assist with urban reslience design. Then, Thomas Haeberlen and Rossella Mattioli explain the European Network Security Agency's endeavor to map the Internet in Europe. Dr. Amit Kumar next examines international efforts to counter the financing of terrorism. Finally, Drs. Pamela Collins, Alessandro Lazari, and Ryan Baggett describe a new research initiative focusing on international education programs in critical infrastucture protection.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Working Together to Enhance Critical Infrastructure Resilience Around the Globe

by Caitlin Durkovich, Assistant Secretary,
DHS Office of Infrastructure Protection

Introduction

The United States benefits from and depends upon a global network of infrastructure systems that underpin the Nation's way of life. The safety and security of those systems, however, requires the concerted effort of public and private sector partners around the world. Within the Department of Homeland Security (DHS), the Office of Infrastructure Protection works to enhance critical infrastructure resilience by promoting cross-border and multilateral collaboration and information sharing so all can benefit from the exchange of best practices, expertise, and lessons learned. DHS also works with international partners to expand global awareness regarding the importance of critical infrastructure protection and resilience in today's interconnected and interdependent world.

Recent incidents, from hurricanes and earthquakes to volcanic ash spread into the atmosphere, illustrate that impacts from events in one country can have cascading effects worldwide. Therefore, it is important for countries to develop programs and work with partners at all levels to secure both critical infrastructure and the supply chains upon which they rely, to enhance global resilience.

Critical infrastructure resilience–the ability to prepare for and adapt to changing conditions, and withstand and rapidly recover from disruptions–is recognized by governments, critical infrastructure owners and operators, and the community as key to sustaining our way of life. But infrastructure resilience is not only about building protective barriers or delivering goods during an event. It is also about building relationships to minimize global impacts from disruptive incidents. DHS engages international partners to ensure that all infrastructure critical to the United States, regardless of location, benefits from the collective experience and expertise of the global infrastructure security community.

Enhancing cross-border resilience—working multilaterally, and sharing existing tools, products, and materials—is integral to enhanced global resilience and the cornerstones of the Department's international efforts. Information exchanged through each of these engagements grows the knowledge base of all partners, provides a strong foundation for continued dialogue, and offers opportunities to leverage existing work to benefit all. Specific areas of mutual interest include approaches to public-private partnerships, voluntary and regulatory critical infrastructure protection practices, assessment and risk methodologies and tools, and information sharing practices and policies.

Cross-Border Resilience Efforts

The northern border of the United States consists of 5,500 miles of shared border, encompassing many physical and virtual shared assets with Canada. Recognizing that the interconnected nature of critical infrastructure requires coordination and collaboration, the United States and Canada developed the Canada-U.S. Action Plan for Critical Infrastructure. Released in July 2010, the action plan's purpose is to strengthen the safety, security, and resiliency of Canada and the United States. The action plan focuses on three broad elements for engagement—information sharing, partnership building, and risk management.

Under this action plan, the United States and Canada have conducted joint projects and programs to enhance cross-border resilience. For example, the countries are executing the first-ever cross-border Regional Resiliency Assessment Program (RRAP) for the Maine-New Brunswick region. The RRAP evaluates critical infrastructure "clusters," regions, and systems to reduce vulnerability to all-hazard threats

(Continued on Page 3)

(Continued from Page 2)

by coordinating efforts to enhance critical infrastructure resiliency and security across geographic regions.

The Maine-New Brunswick RRAP has expanded information sharing, broadened partnerships, and promoted risk management—all key elements of resilience. Through the RRAP, the United States and Canada engaged state and provincial partners, gaining insights and building up the knowledge base for understanding unique characteristics of, and implications for, enhanced cross-border resilience. To support risk management, possible resilience enhancement options have been identified for consideration.

In addition, the two governments have established the Canada-US Virtual Risk Analysis Cell (VRAC). Both countries already have in place staff analyzing critical infrastructure issues. The concept behind the effort is simple—to work jointly, rather than separately, on critical infrastructure topics of mutual interest. Through the VRAC, both countries can conduct joint analysis of critical infrastructure. The VRAC has already been used to draft a joint report on a waterway that links the United States and Canada, which includes economic impact data and possible mitigation efforts. Not only do the reports enhance cross-border understanding of critical issues, but the process can be applied during an incident, enabling both countries to work together and identify key issues and challenges to be addressed.

Further, the RRAP and VRAC are being leveraged to support two key U.S.-Canada initiatives—the Action Plan and the December 2011 President-Prime Minister "Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness" — both of which call for enhanced cross-border coordination and collaboration.

Multilateral Engagement

Beyond our immediate borders, maintaining dialogues with other nations on critical infrastructure is an essential element to the United States' approach to protection and resilience. Multilateral forums provide a means to work together and share information, best practices, and lessons learned with numerous countries on issues of common interest. For example, over several years, DHS has worked with European Union (EU) and Canadian partners to bring together government experts in the field of critical infrastructure. The initial EU-US-Canada Expert Meeting on Critical Infrastructure focused on exchanging information about approaches to critical infrastructure protection and resilience – how critical infrastructure is defined, identified, and the role of information sharing and public-private partnerships.

In only two years, dialogue has moved from basic concepts to more complex subjects: technology and human behavior in critical infrastructure failure; crisis management during critical infrastructure disruptions; knowledge sharing; high-likeliness/low-likeliness events and critical infrastructure planning; and cyber attacks as part of critical infrastructure exercises. Building on these exchanges between experts, this year's meeting focused on innovative and forward-looking subjects – climate change, the interdependence of physical and cyber critical infrastructure, and aging infrastructure. Sharing experiences, knowledge, best practices, and lessons learned in addressing these topics serves an important role in evolving dialogue and taking action to advance global infrastructure security.

The yearly international discussions introduced the concept of developing a mechanism to promote this sharing and dialogue between countries committed to building robust infrastructure security (to include protection and resilience) programs. This initial concept now has become a reality – a secure platform that can be accessed only by vetted Federal government partners and officials from Canada, the European Union, and the European Commission is up and running, and the partner countries have all contributed materials. The underlying goal of this effort is to enhance the knowledge base amongst partners and promote global infrastructure protection and resilience.

These efforts are important because the world is more interconnected than ever before, and threats from natural disasters and cyber attacks do not know or respect international boundaries. However, by working together and continuing an open dialogue, the United States and our international partners can enhance the security and resilience of the critical infrastructure we depend on every day, wherever we may call home. ❖

Critical Infrastructure Protection in the European Union

by Matthew W. Holt, CEO, Intellium*

On 12 December 2006, as one of the elements of the overall European Programme for Critical Infrastructure Protection (EPCIP), the European Commission put forward a Proposal for a Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. Political agreement on the Directive was reached in June 2008, and the Directive was formally adopted by the Council on 8 December 2008. The Directive was accompanied by guidelines for implementation (containing the sectoral and cross-cutting criteria needed to identify European Critical Infrastructure), which were also endorsed by the Council.

The Directive establishes a common procedure for the identification and designation of European Critical Infrastructure (ECI), defined as critical infrastructure located in the EU Member States, the disruption or destruction of which would have a significant impact on at least two Member States of the EU. The identification and designation process takes place through a cooperative effort between the relevant Member States and the Commission. The basic obligations of the Directive include:

- Each Member State takes forward and participates in the identification and designation of relevant ECI;

- Owners/operators of designated ECI must implement an Operator Security Plan (or equivalent) and designate a Security Liaison Officer;

- Member States perform threat assessments concerning specific subsectors in which ECI have been identified on their territory;

- Member States report to the Commission on the types of threats, vulnerabilities and risks identified in each subsector in which ECI have been identified on their territory;

- Each Member State designates a formal European Critical Infrastructure Protection Contact Point;

- Based on the information gathered through the ECI process, the Commission and the Member States shall assess whether further protection measures should be considered for ECIs.

Overall, the Directive has been implemented in the Energy and Transportation sectors by almost all Member States. This includes all aspects of transposing the Directive into necessary national policy, as well as the implementation of the Identification, Designation, Protection, and Reporting aspects as required in the Directive. However, it should be noted that although the Directive aims to promote the development of national CIP strategies, the level of integration is not equivalent across all Member States. While some Member States have made great strides in the development of their national programmes, others have simply translated the Directive and ratified it into legislation, without actually developing the supporting activities needed to effectively implement this legislation.

As the European Commission considers how to improve its CIP policy going forward, there are three strategic challenges that will most likely need to be addressed with most ECI stakeholders in order to achieve buy-in for an efficient and effective ECI process:

- Illustration of Benefits to the Sectors in Scope

- Support for the "European Infrastructure" Perspective / Approach

- Validation of EPCIP Programme Assumptions, Objectives, and Framework

Illustration of Benefits to the Sectors in Scope

(Continued on Page 5)

(Continued from Page 4)

The primary objective of the Directive is to improve the protection level of European Critical Infrastructure through permanent and graduated security measures. Any measurement of the success of the Directive, as well as any discussion about potential expansion to other sectors, should be evaluated based on actual improvements in protection levels in the Energy and Transportation sectors.

The majority perception among relevant stakeholders across Europe is that the increase of protection level of critical infrastructure across Europe has been minimal, if at all, as a result of the Directive. Even in the cases where core proponents argue that European CIP protection has improved, there is not sufficient evidence for making this case to their peers. Solid evidence of improvement will be essential for the Commission to maintain support for the current Directive or to gain support for expansion of scope of the Directive to include new sectors.

Support for the "European Infrastructure" Perspective / Approach

Part of this perception of limited improvement in protection levels could be based on the fact that most of the designated ECI were already designated National Critical Infrastructure (NCI) in the relevant Member States, and that nothing really new had been identified as a result of implementing the ECI process. By not comprehensively identifying all potential ECI, protection would not have been increased of infrastructure that might have been overlooked.

Although there has been no specific challenge to the bottom-up approach of starting from a list of NCI, many feel the identification process could also benefit from an additional top-down approach that includes some sort of EU-level perspective to help identify potential ECI that are not included in Member State NCI lists. The intention would be for this additional component of the process to leverage existing knowledge in various EU-level organizations (e.g. sectoral DGs, industry associations, etc.) that already focus on supranational issues that affect Europe as a whole (e.g. Eurocontrol, Galileo, etc.), rather than having a primary focus on any individual Member State. In this light, the objective would be to identify "European" infrastructure (e.g. not owned/managed by any individual Member State) that could then be evaluated as potential ECI. Such an end-to-end service-based approach also provides a perspective which is significantly different to that from a Member State-only perspective.

Many stakeholders feel that the lack of this component in the process will continue to make it difficult for the Directive to focus efforts on improving security levels in the types of infrastructure its originators probably had in mind.

Validation of EPCIP Programme Assumptions, Objectives, and Framework

Any efforts to improve the tool chosen ("the Directive") to implement the EPCIP objective cannot be successful without reviewing the underlying logic and reasoning that was used to select the tool in the first place.

The establishment of the EPCIP programme was to a large extent influenced by the prevailing global situation at the time in the aftermath of a number of high-profile terrorism incidents in the United States and in EU Member States. The decision to launch the EPCIP, and the resulting design of the programme itself, was inevitably based on a number of fundamental assumptions. Some of these initial assumptions presumably included, but were not limited to:

1. There is such a thing as "European Infrastructure."

2. Some of these infrastructures are critical to European society.

3. The level of security of these infrastructures needs to be increased.

These assumptions would have influenced the decision that the Directive is an effective tool, within the framework of the programme, to help achieve the programme objectives.

With the passage of time, the various initiatives that have already been implemented, and changes in geo-political situations worldwide, it is fundamental to revalidate the underlying assumptions, objectives, and approach of the whole EPCIP programme and not just the Directive as a legal instrument.

Policy makers in non-EU countries would do well to pay close at-

(Continued on Page 6)

(Continued from Page 5)

tention to these challenges faced by the European Commission in implementing its international CIP programme. While it is fair to say that the EU approach is notably lacking some important elements (e.g., interdependencies, cross-sector threats, etc.), the discussion does include 27 countries that, by having agreed to join the EU, acknowledge a shared interest in national security and economic development based on the protection of critical infrastructure. In other words, it is already a "friendly environment." Even so, the ability to mandate specific activities to public and private stakeholders in Member States is somewhat limited. This presents a rich source of lessons learned for policy makers looking to build bridges to other countries in order to protect their own. ❖

** Matthew W. Holt, MBA, CISSP, CISM, is the CEO of Intellium LTD, a cyber security consulting firm based in London. Mr. Holt has extensive international experience in cyber security across government and private sectors, including the U.S. Department of Defense, national and multi-national government bodies in Europe and the Middle East, and multiple Fortune 500 companies worldwide.*

The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks

Budapest, Hungary
June 24, 2013

A resilient system is a system that can, in the face of unknown, large-scale events, recover from the failures and maintain its functions. It is known that many systems, such as biological systems, the human mind, social systems, and dependable engineering systems exhibit this property. However, it is not clear how we should identify general "resilience" properties or strategies applicable to systems in many different domains. The purpose of this workshop is to bring the insights from various fields of resilient systems and explore common research challenges and design principles in the new discipline of "systems resilience."

Information and registration at: HTTP://2013.DSN.ORG/

Modelling Critical Infrastructure Network Interdependencies: A Preliminary Step to Designing Urban Resilience

by Damien Serre, Université Paris-Est, EIVP, Paris, France*

Rationale, Concept, and Objectives

Critical Infrastructure Network

Infrastructure systems facilitate economic growth and social cohesion (Fig. 1, left).[1] Infrastructure networks (energy, transport, water, waste, telecommunication) have evolved from being largely unconnected into being highly coupled 'systems of systems' (Fig. 1, right). These interdependent networks support the flow of goods and services and maintain the essential services for the functioning of society. The continuing occurrence of extreme and devastating natural and technological hazards has highlighted urban vulnerability to disruption of these critical functions and the profound impacts that can cascade through our society and economy.[2] There is no doubt that extreme climate related events will continue to occur, and climate science suggests this will be with increasing severity and frequency; the question is how can society be better prepared and more resilient. The "urban resilience" research axe lead by Damien Serre at EIVP understands that infrastructure is a network where interdependence reflects the reciprocal relationship that exists between several entities.[3] Understanding the mutual dependence between network components, and the potential

(Continued on Page 8)

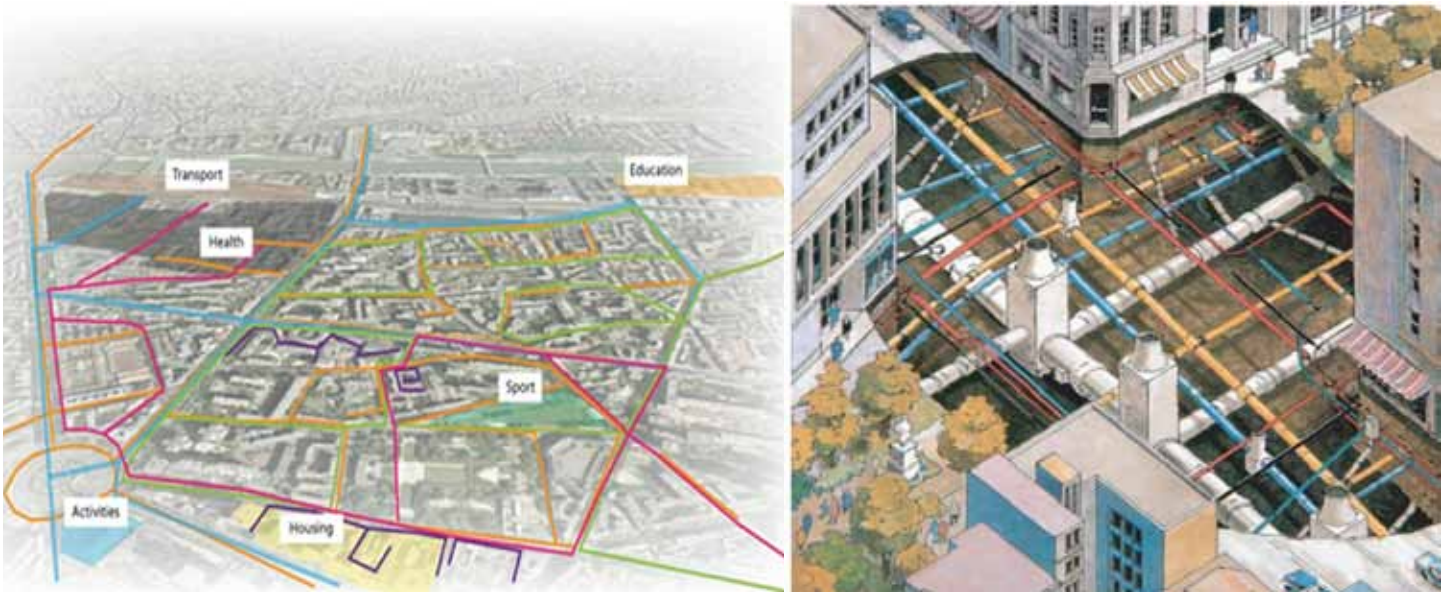

Figure 1. Critical infrastrucutre network as a support of urban life

[1] Sayers, P. Improving Resilience to Extreme Natural Hazards in Europe: IRENE, Collaborative Project: Capacity project, Co-ordinator: Paul Sayers, Sayers and Partners LLP. EU FP7 Proposal, TOPIC SEC-2013.2.1.2, Impact of extreme weather on critical infrastructure, 54 p.

[2] Toubin M., Serre D., Diab Y., Laganier R., (2012). An auto-diagnosis to highlight interdependencies between urban systems, *Nat. Hazards Earth Syst. Sci.*, 12, 2219–2224, 2012, www.nat-hazards-earth-syst-sci.net/12/2219/2012/, doi:10.5194/nhess-12-2219-2012, 6 p.

[3] Serre D., Barroca B., Llasat M-C., 2013. Natural hazard resilient cities, *Nat. Hazards Earth Syst. Sci.*, an Open Access Journal of the European Geosciences Union, Co-Editors of this Special Issue; Hémond, Y.; Robert, B. (2012). Evaluation of State of Resilience for a Critical Infrastructure in a Context of Interdependencies, *International Journal of Critical Infrastructures*. Vol. 8, Nos. 2/3, 2012.

(Continued from Page 7)

for events to disrupt these relationships (and propagate impacts across the infrastructure network and inside the urban environment) is at the heart of our research. This understanding will allow us to identify 'weak links' and effectively build resilience and mitigate risks. Our research aims to provide practical insights and evidence that can help secure infrastructure networks today and provide a framework to be taken forward into policy making, planning, and response.

Resilience Concept

Derived from ecology, the concept of resilience was first defined as "the measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables."[4] Now this concept is used in many other disciplines (physics, psychology, economics, environment, ect.). But for risk management this concept is relatively new, especially concerning natural hazards. We studied a number of other disciplines in order to comprehensively understand the resilience concept and to define it in relation to urban risk management. It appears that resilience is usually used in the continuity of existing terms in these various disciplines. The abundance of definitions of disaster resilience and the fact that this concept is shared by many disciplines makes it difficult to have a common definition. Disaster management has typically focused on analyzing the hazard. Yet, climate related risks have been increasing in frequency and severity, so researchers and some decision makers recognize the need to not only analyze the hazard, but also to try to prepare a plan B—something the concept of resilience can bring. That is why disaster management has been moving away from solely emergency response, initiated during and after an event, toward mitigation and preparedness, initiated before an event, in order to reduce impacts more effectively. Thus, in the current discussion on flood resilient cities, a strong emphasis is placed on improving the flood performance of buildings. Yet, the city has to be considered as an entity with different systems and vital functions and not merely as a set of concrete buildings if we want to design fully resilient cities.

Objectives

Here, there is a huge issue because a city is a complex object. Cities are regarded and studied like complex systems. Such systems are not fully predictable, due to the inherent uncertainty in how they evolve. As illustrated in the literature, a city appears as a set of components interconnected by networks with various critical infrastructures.[5]

Evaluating critical infrastructure network interdependencies for potential vulnerabilities is an important component of strategic planning, particularly in the context of managing and mitigating service disruptions. Yet, multiple networks that innervate cities are particularly sensitive to risks, through their structures and geographic constraints. There is a need to understand how networked systems are resilient because societal functions are highly dependent on networked systems and the operability of these systems can be vulnerable to disasters.

Methods: The DS3 Model

In our research, the concept of resilience is defined as *"the ability of a system to absorb a disturbance and recover its functions following the disturbance."*[6] Indeed, in the resilience concept, the object studied is a system. Assuming that the city can be considered as a system, the resilience definition can be transposed to the urban context as: *"the ability of a city to operate in a degraded mode and recover its functions while some urban components remain disrupted."*[7] According to this urban resilience definition, we have developed a conceptual model to analyze the resilience of urban networks: the DS3 (Spatial Decision Support System) model.[8] In this model,

(Continued on Page 9)

[4] Holling, C. S. (1973) Resilience and stability of ecological systems. *Annual Review of ecology and systematics*, vol. 4, 23 p.
[5] Serre D. (2011) Flood resilient city - Assessment methods and tools. Thesis for the obtention of the Habilitation to Lead Researches, Université Paris-Est, 173 p.
[6] Lhomme S., Serre D., Diab Y., Laganier R. 2010, GIS development for urban resilience, *Sustainable City 2010*, 14-16 April, La Coruña, Spain, 11 p.
[7] Ibid.
[8] Serre D. (2011) Flood resilient city - Assessment methods and tools. Thesis for the obtention of the Habilitation to Lead Researches, Université Paris-Est, 173 p.

(Contined from Page 8)

three capacities have been defined as essential for the study of urban network resilience: resistance, absorption and recovery (Fig. 2). This approach is based on the performance of the urban interconnected systems analysis at the city level and focuses on a physical urban dimension, particularly on technical aspects.[8]

The resistance capacity of a system begins with a system damage analysis. Resistance capacity is considered as the starting point for any resilience analysis. It is necessary to know the potential damages which the system must be able to absorb and from which it needs to recover. On the other hand, the absorption capacity is a function that involves the assimilation of a disturbance that needs to accommodate the disturbance rather than oppose it, thereby introducing the disturbance in the system's performance. The study of the absorption capacity refers to the alternatives that can be offered by the system following the failure of one or more of its components.[9] This requires studying its redundancy properties. Indeed, the redundancy is defined as one of the properties characterizing the resilience of different systems.[10]

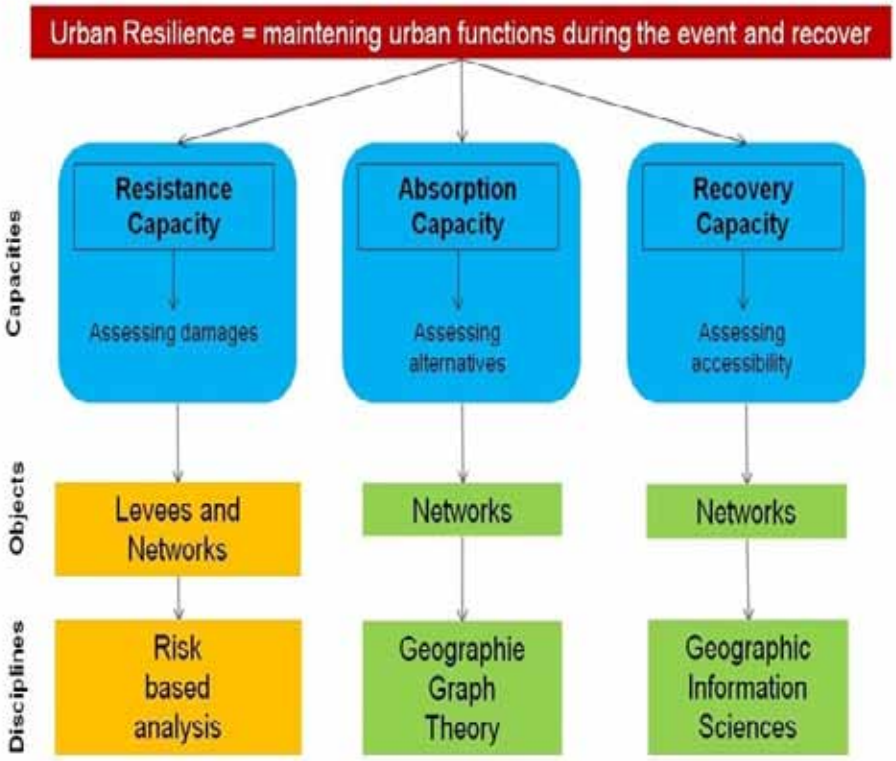

Figure 2. DS3 model representation, including urban resilience objectives and associated disciplines

Usually, if a component of a system ceases to work (it does not achieve its function), a redundant system can mitigate this failure with an alternative.[11] Finally, the recovery capacity is the most representative of the resilience concept.[12]

Recovery does not mean returning to a previous state, but rather a functional recovery of the system. The recovery leads the system to recover a state, structure, or

(Continued on Page 10)

[9] Balsells M., Barroca B., Amdal J., Diab Y., Becue V., Serre D., 2013, Application of the DS3 model to the stormwater sewerage system at the neighborhood level, 8è Conférence Internationale Novatech, Lyon, 23 - 27 juin 2013.
[10] Lhomme, S.; Serre D. ; Diab Y. ; Laganier R. (2011). A methodology to produce interdependent networks disturbance scenarios. In *Vulnerability and Risk Analysis and Management*, ed. A. S. o. C. Engineers, pp. 724-731, Hyattsville, MD, USA.
[11] Ahern, J. 2011. From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world. Landscape and Urban Planning, In Press, Corrected Proof; Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. T. Tierney, W. A. Wallace & D. Von Winterfeldt. 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, 19, pp. 733-752; Clarke, K. R. & R. M. Warwick. 1998. Quantifying structural redundancy in ecological communities. *Oecologia*, 113, 278-289.
[12] Ibid.

(Continued from Page 9)

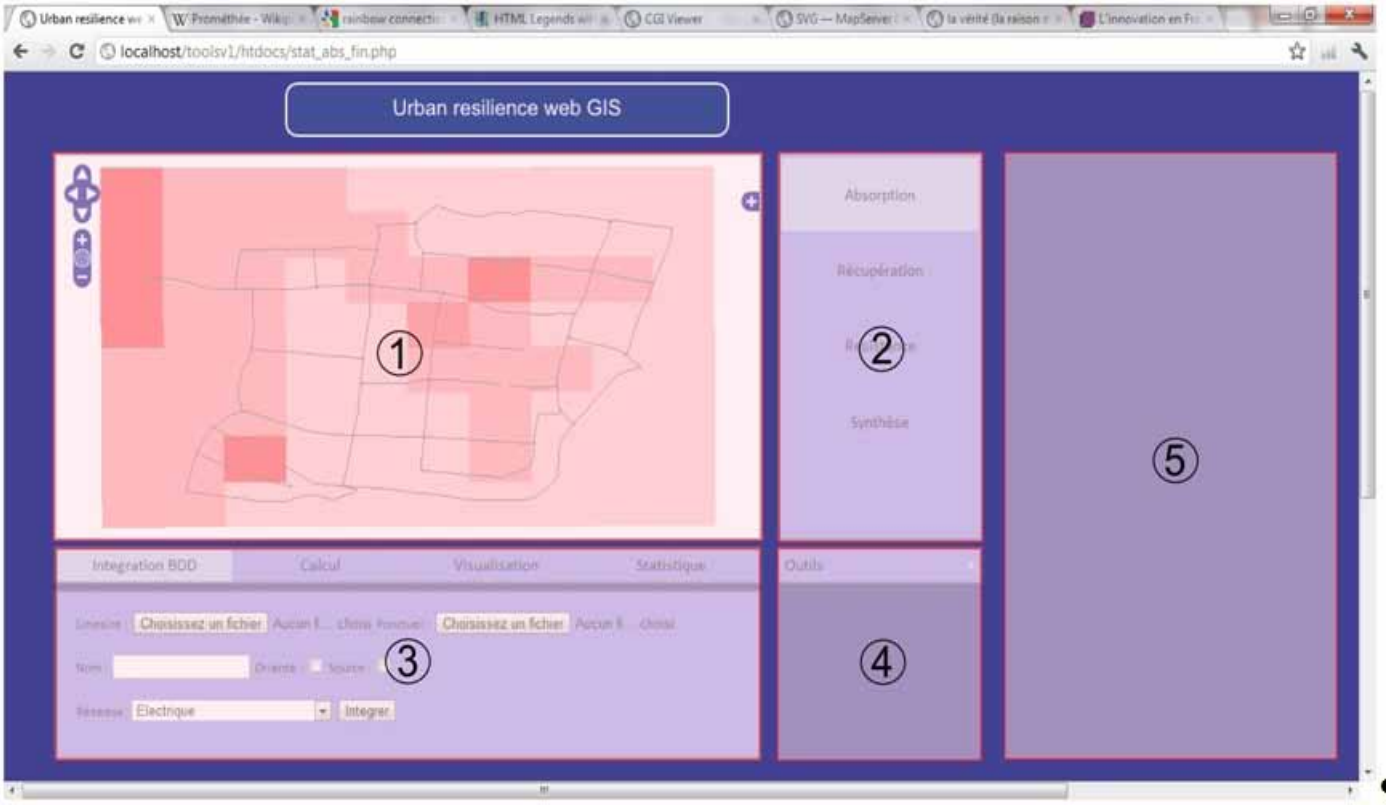

Figure 3. Results: a Spatial Decision Support System to anticipate urban operating during a crisis

The methodology presented above allows for producing network failure scenarios taking into account network interdependencies. In our research, information about housing, companies, infrastructures, hazards, and networks are needed (location, condition, exposure, ect.) This type of information is referred to as spatial information, and when visualized, we can see relationships, patterns, and trends that may not otherwise be apparent. It is well known that Geographic Information Systems (GIS) can be used to recover the spatial component of risk and it is clear that risk assessments have an important spatial component. For instance, to better respond to post disaster activities, GIS technology provides a logical tool for integrating the necessary information and contributing to preparedness, rescue, relief, recovery and reconstruction efforts. GIS is seen as a necessary tool in the area of emergency response. But resilience requires looking beyond emergency response in order to optimize recovery after a flood event, thanks to preparedness and resilience assessment. That is why a GIS prototype has been created in order to implement the developed methods and the three capacities relevant for a future urban resilient conception design (Fig. 3).

The architecture of the DS3 model is based on four main components:[13] a database storing the data required for calculations (like the network, and major issues); a web server to deliver web content; a map server for mapping application; and a user interface displaying results. Interface is composed by 5 different modules in respect to the web-GIS user methodology and strategy for assessing networks resiliency: (1) the

(Continued on Page 11)

[13] Lhomme S., Serre D., Diab Y., Laganier R., 2013, Assessing the resilience of the urban networks: a preliminary step towards more flood resilient cities, *Nat. Hazards Earth Syst. Sci.*, 13, pp. 221–230. www.nat-hazards-earth-syst-sci.net/13/221/2013/ doi:10.5194/nhess-13-221-2013.

(Continued from Page 10)

map, (2) the menu, (3) options for each menu, (4) different tools, and (5) information interface. Thus, the interface menu proposes a four step analysis: first, the absorption capacity analysis; second, the resistance capacity analysis; third, the recovery capacity analysis; and fourth, a synthesis of the different results with the introduction of critical infrastructures location analysis.

Conclusions

As a preliminary conclusion, we have highlighted the network interdependencies and the propagation of the effect of failures in this linked system. This approach allows evaluating the capacity of network resistance, one of the capacities we consider to design resilient cities. Then, we have used graph theories to assess the redundancy of the urban networks. This approach allows finally assessing another capacity we take into account in our urban resilience assessment method: the capacity of absorption, or the capacity of the city to operate in a degraded mode. We have linked the results of our models with GIS to produce spatial decision support systems to enable the managers of these infrastructures to improve their management to make cities more resilient through the capacity of recovery. This step is ongoing and we are testing the results on several cities.

Simultaneously, we are now focusing on organizational resilience to improve the governance for resilient city design.[14] This consists of identifying the multiple actors in charge of urban services and building together a new way of thinking to improve the management of these services by integrating the cascading effects highlighted in our research on critical infrastructure network analysis. Also, to date, the DS3 model has been applied to studying and assessing the resilience of urban networks only. Using the model we aim to analyze how different urban design actions can contribute to improved resistance, absorption or recovery capacities, and consequently urban resilience to risks. The idea is to develop resilience criteria to guide a neighborhood's design by integrating resilience.[15] ❖

* *Damien Serre is Associate Professor in the School of Engineering (EIVP) at the Université Paris-Est, where he heads the urban reslience research initiative. He can be reached at damien.serre@eivp-paris.fr.*

[14] Toubin M., Serre D., Diab Y., Laganier R., (2012). An auto-diagnosis to highlight interdependencies between urban systems, *Nat. Hazards Earth Syst. Sci.*, 12, 2219–2224, 2012, www.nat-hazards-earth-syst-sci.net/12/2219/2012/, doi:10.5194/nhess-12-2219-2012, 6 p.
[15] Balsells M., Barroca B., Amdal J., Diab Y., Becue V., Serre D., 2013, Application of the DS3 model to the stormwater sewerage system at the neighborhood level, 8è Conférence Internationale Novatech, Lyon, 23 - 27 juin 2013.

No Maps of These Territories …Yet.

by Thomas Haeberlen and Rossella Mattioli, ENISA

No Maps for These Territories[1] is the title of a documentary about William Gibson, the father of cyberpunk and the one who first coined the term cyberspace. But while cyberspace is a common and sometimes important part of our everyday life we cannot say that we have maps for these territories yet. Every day, our reliance on information and communication technology (ICT) systems grows greater. Via this undefined fabric of cables and interconnections, we are building the future information society and putting our most critical services at stake without even knowing where all these interconnections actually lie. Every day, we learn about research or malware tools which allow vulnerable computers around the world to be targeted, or attacks launched that aim to harm the secure usage of Internet networks.

This shows the gap between the actual usage of the Internet and the availability of a global view of the infrastructure that enables our online life. Many critical services are increasingly dependent on network connectivity. This dependency is going to grow even more with the increasing use of services like cloud computing. Apart from "known critical" services, there are others, such as social networks that may become critical in the event of a large-scale incident affecting other traditional means of communication. An example of this is the 2011 earthquake and tsunami in Japan, where voice communication broke down, but data communication was still possible[2] with people using Twitter or Facebook to communicate where they were and what they needed.[3]

The ARPANET itself, which was the predecessor of the Internet, was conceived with the explicit goal of being able to survive large-scale disruptions. The past has shown that in general, the Internet as a whole is quite resilient, although there have been a number of notable incidents where the connectivity of certain networks was severely impacted, or where whole parts of the Internet became effectively separated. Although there is a great deal of published and on-going research on the topic of the stability or resilience aspects of routing infrastructure in general, this is still not fully understood on many levels.

Governments in several European Union (EU) Member States have questioned how the Internet in their country would be affected by large-scale events or attacks,[4] e.g. a large-scale disturbance in the global Border Gateway Protocol (BGP) routing infrastructure[5] or a Distributed Denial of Service (DDoS) attack affecting a large part of the infrastructure in a particular country, such as the 2007 attacks on Estonia.[6] Governments also ask what should be done to ensure that certain critical services still remain functional in the case of such events. The usually assumed availability of everyday connectivity is not yet matched by a comprehensive and structured framework which allows predicting the domino effect at the physical and network layer of natural disasters or everyday more

(Continued on Page 13)

[1] No Maps for These Territories (2000).
[2] James Cowie, Japan Quake (2011) http://www.renesys.com/blog/2011/03/japan-quake.shtml.
[3] The 3.11 Japan Quake: Looking Back at News and Crowdsourcing on Media Coverage Map. http://emergencyjournalism.net/the-3-11-japan-quake-looking-back-at-news-and-crowdsourcing-on-media-coverage-map/.
[4] Wählisch, Matthias, Sebastian Meiling, and Thomas C. Schmidt. "A framework for nation-centric classification and observation of the internet." In Proceedings of the ACM CoNEXT Student Workshop, p. 15. ACM, 2010.
[5] RIPE, (2008). YouTube Hijacking: A RIPE NCC RIS case study, 2008, https://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.
[6] Joshua Davis, Hackers Take Down the Most Wired Country in Europe (2007) http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

(Continued from Page 12)

frequent cyber security incidents. Examples like the outages following Sandy,[7] the recent news regarding the huge DDoS attack that could have harmed part of the Internet,[8] the discovery of three divers trying to cut a submarine cable in Egypt,[9] and the recent Internet disruptions in Syria, Bangladesh, Senegal,[10] Egypt, Saudi Arabia, Pakistan, and India[11] underline how it is necessary to start mapping the interdependencies between cyber and physical territories in order to protect the Internet as we know it and the resilience of the emerging information society.

These questions cannot be answered without a good knowledge of how the different networks within a country (or any other suitably defined geographical region) are interconnected. The European Network Security Agency (ENISA) began working on the security and resilience of the Internet in 2010, and in 2013 will focus on mapping the Internet in Europe.

Internet mapping vs. Internet scanning

There are several ways to investigate the structure of the Internet, and various approaches will have to be combined to get a global understanding of network interconnections. The "node" point of view allows enumerating or scanning all the nodes in one or more networks. The "network" perspective allows investigators to look both at the physical level (cables)[12] and network layer as BGP routing tables,[13] Autonomous Systems Numbers (ASNs) allocation and related networks.[14]

For example, mapping one national Internet infrastructure from the network perspective enables first a comprehensive view of all the connection providers involved. It allows the underlining of the physical paths of the information highways and also provides a clear view of all possible points of failure. Moreover, it gives the ability to run scenarios and resilience exercises both from a technical and emergency preparedness point of view.

The node approach forms the basics of all penetration testing and produces a node point of view, but it is very problematic when it comes to large-scale or Internet-wide networks due to its legal implications. Lately it has been used by researchers to scan large portions of the Internet, with the use of various tools and approaches which range from port scanning techniques[15] to the adoption of a botnet-like methodology.[16] The technique allows the identification of nodes and addresses connected to the Internet but also vulnerable to specific exploitations techniques. Due to the various concerns regarding privacy and permissibility of remote scanning of arbitrary nodes, ENISA will focus on the Internet mapping and network perspective and not perform any active scanning.

As the history of cartography shows us, the ability to map territories brings humanity the ability both to visualize the present, and also to foresee the future. It also has two main levels: one is the strategic, which enables the mapping of the real Internet "world" and allows the planning of the next steps. The second level is more short-term and tactical, and can be used to face an emergency or to quickly respond to large-scale outages caused by natural disaster or malicious activity.

(Continued on Page 14)

[7] Doug Madory, Hurricane Sandy: Global Impacts http://www.renesys.com/blog/2012/11/sandys-global-impacts.shtml.
[8] ENISA, Flash Note: Can Recent Attacks Really Threaten Internet Availability? (2013) http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-Internet-availability.
[9] Alexandra Chang, Why Undersea Internet Cables Are More Vulnerable Than You Think http://www.wired.com/gadgetlab/2013/04/how-vulnerable-are-undersea-Internet-cables/.
[10] Akamai, The State of the Internet, Volume 5, Number 4, 4th Quarter, 2012 Report, Section 8: Internet Disruptions (2013) http://www.akamai.com/stateoftheInternet/.
[11] Doug Madory, Intrigue Surrounds SMW4 Cut (2013) http://www.renesys.com/blog/2013/03/intrigue-surrounds-smw4-cut.shtml.
[12] Wisconsin Advanced Internet Laboratory, Internet Atlas (2013) http://atlas-test.wail.wisc.edu/InternetAtlasLimited/; University of Adelaide, The Internet Topology Zoo (2013) http://www.topology-zoo.org/contact.html.
[13] RIPE, RIPE Atlas(2013) https://atlas.ripe.net/.
[14] CAIDA, AS Rank: AS Ranking (2013) http://as-rank.caida.org/.
[15] HD Moore, The Wild West (2012) https://speakerdeck.com/hdm/derbycon-2012-the-wild-west.
[16] Unknown, Internet Census 2012 (2012) http://Internetcensus2012.bitbucket.org/paper.html.

(Continued from Page 13)

The Policy and Organizational Component

As is becoming every day more evident, technology is just one aspect of the cyber security topic. While solutions for technology issues may work on the global scale, there are also organizational and policy issues which need to be addressed in order to achieve a comprehensive solution. The main point regards the ability to collect all possible information about the legal frameworks concerning the relationship between telecommunications regulators and Internet Service Providers (ISPs) involved in each of the examined countries. Collecting information to map the Internet structure of one nation not only concerns the collection of data but also requires proper security to be maintained for those data sets which cover critical infrastructures. A mapping of the Internet infrastructure must consider the framing of the legal aspects to be as important as the technological ones. This is primarily because of: the risks of this kind of information becoming available to malicious actors; issues over the management of these resources by telecommunications regulators and businesses; and the potential enhancement of coordination that can emerge from this information becoming available. Moreover, there are several implications at cross-border levels due to the interconnected nature of the Internet and the consequential transnational legal frameworks that can be applied to underground

or submarine infrastructures. For example, maritime laws or mechanisms for resolving border issues may need to be considered when dealing with incidents related to submarine cables.

Mapping "European Internets"

ENISA has studied the resilience of network infrastructures and the mechanisms for emergency communications that are in place in EU Member States since 2010, paying the same attention to both the technical and organizational components. The aim is to provide Member States with frameworks and resources to better secure and ensure the resilience of their networks. In this regard the "Inter-X: Resilience of the Internet Interconnection Ecosystem" study was the first step ENISA took towards studying this area. The study focuses on the resilience of the system of interconnections between Internet networks. The project looked not only at the actual interconnections, but also at the arrangements, agreements, contracts, and incentives that underpin them. In 2011, it was followed up with a study assessing technical (e.g. logical, physical, application layers, replication, and diversity of services and data, data centres), peering, and transit (e.g. Service Level Agreements (SLAs)), as well as market, policy, and regulatory issues. In 2013 the goal is to provide insight into the "structure of the Internet" at the physical and network layers within each of the European countries. The scope in this case will not be the global properties of the Internet, but the properties of those parts of the Internet that could be said to "belong" to a particular country (hence the term "European Internets"). This could be used by governments or policymakers to develop a strategy to ensure that critical services still remain functional even if network performance or connectivity in general is broken. The second goal is to enable competent authorities in European Member

(Continued on Page 15

*Image courtesy of sheelamohan/FreeDigitalPhotos.net

(Continued from Page 14

States to enhance their knowledge of the structure of the electronic communications infrastructure within their country, to identify gaps, and if necessary find ways to work together with the relevant stakeholders. For example, these could include ISPs and/or their associations in order to improve the resilience of certain critical services. The information and insights from the study could be used by regulators, policymakers, ISP associations, or communities to develop appropriate measures to improve the resilience of the Internet-based communications infrastructure within their respective areas of responsibility. The idea is to map the "European Internet" and continue the work started in 2010 but also set the baseline for future studies. As stated at the beginning, there are several implications of a disruption or a security incident and several variables to take into consideration concerning policy and legal issues, criticality of the data, and development of a framework that will allow contributions from different stakeholders.

Conclusion

Defining a map of the Internet is as difficult as it is to draw a line between our online and offline life. Where are the cables? What are the routes that one packet takes to go from our computer to the server where the information we are looking for is stored? These packets can be social network updates regarding our position during a natural disaster because the phone network is jammed, or any other everyday communication which is broadly wrongly assumed will never be disrupted. For these reasons and to build a more secure and better resilient information society, there is the need to develop a comprehensive view of the structure of the Internet and to visualize the interdependencies between cyberspace and physical space. ❖

8th Annual Homeland Security Law Institute

When
June 19 - 21, 2013

Where
Capital Hilton Hotel
1001 16th St NW
Washington, DC 20036-5794
United States of America

Sponsored by the ABA Section of Administrative Law and Regulatory Practice

To Register Click Here

To View the Program Click Here

International Efforts in Countering the Financing of Terrorism: A Status Check

by Amit Kumar, Ph.D., Center for National Policy; Georgetown University; George Mason University*

Introduction

This piece delves into the current state of international efforts in Countering the Financing of Terrorism (CFT). Key issues relating to these efforts are discussed at length. Furthermore, several trends in terrorist financing as well as strategies in place to deal with these trends are explored.

The Convergence of Crime and Terrorist Financing

With terrorists using criminal methods to raise, store, move, launder, and deploy funds over the past several years thanks to their collusion with criminals, both organized and petty, and the clamp down on terrorist financing through charities by authorities dedicated to CFT efforts, the convergence of crime and terrorist financing has become a hard reality. No wonder that the genesis of the CFT efforts began by extending the Anti-Money Laundering (AML) tools and techniques to CFT efforts right after the tragic attacks of September 11, 2001. And terrorists themselves do engage in laundering activities with aplomb, thus appropriating the classic criminal endeavor of money laundering as manifest in the case of Hezbollah's notorious Lebanese Canadian Bank case. Or following a different tack, terrorist organizations may rely on criminal syndicates to launder money for them ala Lashkar-e-Tayibba's (LeT's) arrangement with the D-Company. As the U.S. Government's recent investigation into HSBC's activities has shown, the funds used by terrorists are eventually placed into the internal banking system thus vindicating the earlier CFT strategy of extending AML methods to CFT measures. Recognizing the intersection of the AML and CFT worlds, the Financial Action Task Force (FATF) has over the course of the past year combined the erstwhile disparate AML and CFT 40 + 9 standards into 40 standards. In keeping with the convergence of Money Laundering and Terrorist Financing, there is an ever-greater move among countries to declare terrorist financing as a predicate offense to money laundering.

The Move towards a Risk-Based Approach to AML/CFT

The paucity of financial resources exacerbated by the global economic slowdown has brought the issues of risk-based AML/CFT measures as well as risk-based assessments to the center stage of the discussion. There has been a realization and recognition that throwing precious resources aimlessly at tackling money laundering and terrorist financing is not doing the trick, hence there is a dire need to allocate funds for AML/CFT based on risk assessments emanating out of vulnerability and threat assessments relating to money laundering/terrorist financing. The proverbial one-sized fits all rule-based approach has apparently not worked—hence the move by FATF and the international AML/CFT community to take the vulnerability assessments that are a function of a financial institutions geography, nature of business, size, customer profile, location, state of AML/CFT readiness, etc. into consideration alongside the threat information that is a function of the nature of terrorist and criminal threats infesting a certain geographical and demographic domain. Mapping vulnerabilities against threats leads to risk assessments.

The Targeted versus Systemic Approach

The impetus for a risk-based approach runs into a classic choice that the AML/CFT world runs into on a perennial basis—whether to adopt systemic (preventive) measures to abort the threat of money laundering and terrorist financing and to protect financial systems from abuse by any one of these evils or to design, devise, develop, and implement targeted approaches to specific money laundering and terrorist financing offenses or activity—namely sanctions, enforcement actions, investigations, prosecutions, and convictions. While the application of systemic approaches entails

(Continued on Page 1)7

(Continued from Page 16)

heavy financial manpower and regulatory costs, there is often a debate as to their success in curbing money laundering/terrorist financing activity. This is evidenced by the continued misuse of banking channels by terrorist organizations like Hezbollah, and the Columbian drug cartels, as well as the sloppiness in establishing and implementing sound AML/CFT controls by the likes of HSBC, Riggs, Wachovia, and the Lebanese Canadian Bank—most of whom had varying shades of AML/CFT controls to begin with. Interestingly and ironically enough, the detection of lack of AML/CFT controls has led to enforcement actions against these and other financial institutions. Whether or not these enforcement actions have forced these and other financial institutions to establish sound AML/CFT systemic measures to prevent terrorist financing/money laundering activity—only time will tell. In the meantime, both targeted and systemic measures will happily co-exist, hopefully collectively curtailing threats arising out of money laundering/terrorist financing. Also, it is only to be expected that the reputational, market, and business risks relating to enforcement actions are expected to drive banks to address any shortfalls in systemic AML/CFT controls.

The Effectiveness of AML/CFT Implementation Measures

The aforementioned severe international resource crunch has necessitated a move towards assessment of the implementation of AML/CFT measures. Key metrics like prosecutions, arrests, convictions, seizures, confiscations, etc. are gaining prominence in the lexicon of the AML/CFT world like never before. 'To do' checklists of measures enacted or laws passed are giving way to the need to assess the impact of such measures. For example, the effect of targeted sanctions on reducing terrorist financing by listed entities is now an important dynamic that has entered the AML/CFT debate. Changes in the FATF methodology that bring an effectiveness criteria to the fore in AML/CFT assessments will kick off the 4th round of Mutual Evaluations (compliance with FATF standards) at the end of the year and is emblematic of this stress on efficiency and impact. Further resource allocation for AML/CFT measures may then be made on the basis of such effectiveness metrics.

(Continued on Page 18)

(Continued from Page 17)

The Development of Terrorist, Criminal, and PEP Networks, and Greater Awareness of AML/CFT

The interlocking financial interests of terrorist organizations, criminal syndicates, and Politically Exposed Persons (PEPs) across national boundaries have made nation states more aware of the dire need for international collaborative law enforcement, intelligence, and financial information-sharing measures. The periodic increase in FATF membership and attempts at compliance with FATF standards; the urgency to enact and implement money laundering and terrorist financing laws; the growth in the number of Financial Intelligence Units (FIUs) and attendant Suspicious Activity Reports (SARs) compliance initiatives; efforts at improving investigatory and prosecutorial capacity; and the institution and development of assets freeze sanctions measures are some of the more important highlights of the moves witnessed in the AML/CFT arena internationally.

Global Targeted Sanctions versus National Sanctions

The proliferation of targeted sanctions tools against stateless actors (terrorists primarily) has brought about procedural due process concerns in regional and national courts that hit at the very rationale for global compliance of these measures. In addition, the absence of plausible effectiveness and impact metrics for these targeted assets have raised the need for national sanctions lists under United Nations Security Council Resolution (UNSCR) 1373. This in turn coupled with a greater imperative for international cooperation and transnational prosecutions, and seizing and confiscation measures—given the inherent transnational nature of terrorist financing—have brought about the urgent quest for such national and/or supranational sanctions measures as the more lethal choice to contain terrorist financing/money laundering. This is not to say that targeted sanctions measures against state actors, PEPs, and state entities have been totally ineffective. The sanctions instituted against Iran, North Korea, Libya, etc., have been effective in crippling the illicit economies of these states. Yet they have not deterred some of these states in pursuing Weapons of Mass Destruction (WMD) or in shutting off their spigots of financial support to terrorist organizations.

Lack of CFT Capacity versus Lack of Political Will

The CFT capacity deficits identified by the FATF and other international assessment mechanisms can be attributed to the lack of political will and an acute paucity of financial resources and technical expertise in countries that are subjected to these assessments. The lack of political will is not surprising given the involvement of PEPs in laundering and terrorist financing activity and their role as critical nodes in the criminal and terrorist networks mentioned earlier. The power of lucre and corruption is the hallmark of such state actors—it is this evil that leads to heightened money laundering and terrorist financing risks in states that these individuals/persons govern. It is impossible for such corrupt state actors to establish and enforce compliance with international AML/CFT measures. Unless there is political will within jurisdictions to adopt and implement the FATF AML/CFT standards, no amount of technical assistance to bridge the CFT capacity shortfalls will help.

Conclusion

This piece has touched at some length on crucial and salient issues that confront AML/CFT practitioners today. It is apparent that the future of CFT efforts rests on how artfully and smartly the international community is able to negotiate these issues. CFT internationally is a work in progress and the fight to stamp out terrorist financing remains a nascent endeavor with a lot more to be done. ❖

Dr. Amit Kumar is the Fellow for Homeland Security and Counterterrorism at the Center for National Policy; Adjunct Associate Professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service; and Adjunct Senior Fellow at the George Mason University School of Law's Center for Infrastructure Protection and Homeland Security.

International Critical Infrastructure Protection Courses and Degree Programs

by Pamela Collins, Ed.D., Alessandro Lazari, Ph.D., & Ryan Baggett, Ed.D.*

Overview

The following article will highlight ongoing research that is currently being conducted by the authors. Specifically, the research is intended to add to the existing body of knowledge on international efforts in infrastructure protection. This task will be accomplished by describing the current state of infrastructure protection and resilience, both domestically and internationally, with regards to professional core competencies as evidenced by both legislation and academic programs. The end product for the research will be an international infrastructure protection and resilience curriculum suitable for graduate level instruction and an outline for a text on international critical infrastructure protection.

Background

When examining the most recent information on international critical infrastructure, the European Programme for Critical Infrastructure Protection (EPCIP) is commonly identified. The EPCIP refers to the specific programs created as a result of the European Commission's 2006 communication, EU COM 786.[1] Additionally, research identifies a 2006 Congressional Research Service report on European Approaches to Homeland Security and Counterterrorism.[2] However, a dearth of information exists that provides the latest knowledge on international infrastructure protection.

From a domestic perspective, the majority of academic work to date has been conducted by George Mason University's (GMU) Center for Infrastructure Protection and Homeland Security, (CIP/HS).[3] There have been other assessments of infrastructure protection courses, and based upon an extensive study by the Center for Defense and Homeland Security of "Colleges and Universities Offering Homeland Security Programs," there appear to be no programs in the United States that offer a certificate program in CIP or a course on International CIP.[4]

Purpose

The primary focus of this research will be the development of knowledge on international efforts in infrastructure protection. The results of this research will have a myriad of uses to include, but not limited to: publications, conference proceedings, textbook development, and curriculum development. The curriculum would support courses that would likely serve as electives to various graduate programs or programs with concentrations in critical infrastructure protection. Additionally, efforts will be undertaken to market this course to international programs that offer degrees, certificates, or programs in CIP related disciplines. Last, an additional product of the research will be a report on the quantity and types of infrastructure protection programs being offered by accredited international universities.

Methodology

The study will employ a blended manifest and latent content analysis that uses both quantitative and qualitative approaches. While most of the data will be qualitative, the analysis will lend itself to a quantitative analysis through tracking numbers of items such as course descriptions and common terms. Based upon these quantitative elements, inferences will be made by comparing and investigating patterns and trends. The content analysis strategy will include a

(Continued on Page 20)

[1] http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.
[2] http://www.fas.org/sgp/crs/homesec/RL33573.pdf.
[3] GMU has developed a series of model CIP courses that can be adopted and tailored by individual instructors. Course syllabi can be found at http://cip.gmu.edu/index.php/courses.
[4] http://www.chds.us/?partners/institutions.

(Continued from Page 19)

multi-layered approach with a sampling process that initially includes data from the following sources: Council of International Schools, the Directory of Universities, Colleges and Schools in the Provinces and Territories of Canada, the U.S. Department of Education, and university course catalogs.

In addition to the data collection on existing programs described above, a comprehensive literature review will be undertaken initially to identify the necessary components of a graduate course as well as the information that is produced from the GMU review committee on the development of a certificate program in infrastructure protection. The literature review will include the identification, analysis, and synthesis of critical legislative domestic and international mandates.

Legislative Mandates

In an effort to effectively convey the importance and progression of both domestic and international critical infrastructure legislative mandates to curriculum users, the researchers will collect and synthesize key domestic and international legislation. Despite other initiatives that have outlined pieces of this information in the past, the researchers will emphasize the importance of comparison between domestic and international mandates. The comparison will provide students a better understanding of differing environments which govern and protect the world's critical infrastructure. Additionally, the analysis will encourage critical thinking regarding potential gaps that may exist in both domestic and international policies.

From a domestic perspective, dating back to the bombing of the Alfred P. Murrah Federal Building in April of 1995 and the subsequent passing of Executive Order 13010 in 1996, there have been several key pieces of legislation in the United States that have taken over the last 17 years. Over time, these important mandates have served to advance critical infrastructure protection and resilience. Emphasis on domestic critical infrastructure legislation will include, but are not limited to: Presidential Decision Directive 63 (1998), USA PATRIOT ACT of 2001, Homeland Security Presidential Directive 7 (2003), National Strategy for the Protection of Critical Infrastructure and Key Assets (2003), National Infrastructure Protection Plan (NIPP) (2006/2009), National Response Framework (CI/KR Support Annex) (2008), and the implications of Presidential Policy Directive/PPD-21 (2013) on current initiatives.

From an international perspective, many legislative mandates in the European Union (EU) regarding critical infrastructure protection followed the events of September 11, 2001. Starting in 2004, the European Council called for a strategy mainly focused on the prevention of and the fight against terrorism. The original focus was then reoriented in 2005 and 2006, with the "green paper" and the "EPCIP", so as to establish European Policies for Critical Infrastructure Protection and with an all-hazard approach. All these activities led to the promulgation of the Council Directive 2008/114/EC of 8 December 2008 on the "identification and designation of European critical infrastructures and the assessment of the need to improve their protection"[5] which requested the EU's Member States to engage bilateral/multilateral discussions in order to identify, designate, and enhance the protection of the "European critical infrastructure (ECI)" or those infrastructures located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States.

Preliminary Analysis/Findings – Academic Programs / Research

When assessing the current international programs dedicated to infrastructure protection, research indicates that Carleton University in Ottawa, ON Canada offers the only Master's Degree program in infrastructure protection and international security. However, there are a number of related degree programs that touch upon critical infrastructure protection and include:

- Masters in Emergency Management- Disaster Preparedness and Response- Ben-Gurion University of the Negev, Israel
- Masters in Infrastructure Planning- The University of

(Continued on Page 21)

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

(Continued from Page 20)

Stuttgart, Germany

- School of Built Environment, Centre for Sustainable Urban and Regional Futures (SURF)- University of Salford, Manchester England
- Masters in Homeland Security- Systems, Methodologies and Tools for Security and Crisis Management- University "Campus Bio Medico", Rome, Italy.

There are also a number of post graduate and combined research programs that offer degree programs in areas such as sustainability and resilience. While these programs do not specifically use the terms critical infrastructure they do contain information on topics such as risk, security, and society and spatial and temporal dimensions of hazards. While this study is preliminary, the researchers are finding a number of unique degree programs that touch upon elements of critical infrastructure protection. Additionally, the analysis of the data also suggests that there are quite a few specific courses on the subject of infrastructure protection.

With discussing higher education, another important area to evaluate is the research areas of key faculty within the university. The degree to which faculty are conducting research on infrastructure protection often suggests that this research will most likely find its way into lectures, courses, and finally curriculum. This in turn can lead to concentrations, certificate programs, options, and ultimately complete programs. Ultimately, the research exposes students to practical issues related to infrastructure protection and helps promulgate information and understanding of critical infrastructure to future engineers, city planners, and security professionals and so on. Preliminary research has identified over 50 international faculty members who are researching some facet of infrastructure protection. Additionally, a key indicator of the interest and resiliency of a discipline is to measure the extent to which it appears in conferences, and where there is a call for papers for topics related to CIP provide insights into the interest and examination of the field. The research will also analyze the frequency of these information sharing opportunities.

The preliminary data analysis is positive and would suggest that critical infrastructure protection is on the radar of many international universities and colleges and students are being exposed to the complex topic of protecting the critical infrastructure of a community, city, state, or country.

Summary

Preliminary research indicates that as a discipline, critical infrastructure protection is growing as the body of knowledge continues to expand. There are a variety of ongoing research projects being conducted at numerous international universities and the national progression of this research indicates that it will influence curriculum, lead to an increasing number of courses on the subject, and as these find their way into existing degree programs they often develop into options for certificate programs. In time it is predicted that as these programs grow in popularity with students, the creation of full degree programs at both the undergraduate and graduate levels as well as post graduate programs will grow as well. ❖

The researchers, who began this study in January of 2013, anticipate a final report with more details and information on the types of courses and programs that exist internationally on critical infrastructure protection by the fall of 2013. Those interested in contributing to the information in this research are encouraged to contact Dr. Pamela Collins at Pam.Collins@eku.edu.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1