THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY
VOLUME 10 NUMBER 11

MAY 2012

INTERNATIONAL CIP

European Commission.................2
Montréal.....................................3
Social Media................................7
Global Supply Chain....................9
Legal Insights.............................10
Resiliency DC............................11

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

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

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

This month in *The CIP Report* we present our yearly issue on international topics in critical infrastructure.

The European Traceability Institute starts us off with a look at the traceability of the supply chain in regards to the fishing industry. Then, we examine Montreal's critical infrastructure and its interdependencies. The Risk Management Group from the United Kingdom discusses the risks of social media and the following article discusses global supply chain security.

This month's *Legal Insights* compares the U.S. strategy for cybersecurtiy with various international perspectives on cybersecurity and advocates for a global, unified approach to protecting cyber space.

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

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

Integration of Standards for Traceability and Sale of Seafood Products: FishBizz

by Miodrag Mitic, Managing Partner, European Traceability Institute

Sustainability is at the heart of the proposed reform of the European Union Common Fisheries Policy (CFP). Fishing sustainably means fishing at levels that do not endanger the reproduction of stocks and managing the volume of fish taken out of the sea through fishing. To enforce the CFP rules, a control system is designed to ensure that fish products can be traced back throughout the supply chain. At every point along the chain, for every consignment of fish, information must be provided that proves that it was caught legally. Checks are carried out at every point in the chain from the boat to the retailer: in ports where fish land or are transshipped, during transport, in factories that process fish, and at markets where fish are sold.

To achieve traceability throughout the supply chain, various tracing methodologies and technologies must be integrated into the operational business processes carried out by the different actors along the full length of the chain. As a result, traceability systems must have the ability to exchange information with each other and to use the information that has been exchanged. They must be interoperable to guarantee fast, accurate, and cost-effective exchange of information. Standardization is a common approach towards achieving interoperability. There is also a wide range of technologies and solutions, which can support a standard.

The wonderful thing about standards is that there are so many of them to choose from, and the challenge lies in the fact that more than one is used by the various actors in the supply chain. Some standards have a narrow point-to-point profile aimed at achieving the so called "one-up/one-down" traceability with immediate trade partners. Other standards are focused on establishing a "chain-of-custody" system via a central repository maintained by a third party and on "traceability networks" that are based on registries that enable traceability data search along the supply chain.

The European Committee for Standardization (CEN) is a business facilitator in Europe, removing trade barriers for European industry and consumers. Its mission is to foster the European economy in global trading, the welfare of European citizens, and the environment. Through its services, it provides a platform for the development of European Standards and other technical specifications. A CEN Workshop Agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment. They have a short development time, and their development is extended to any interested party, with low participation costs and no geographical restrictions.

The aim of the CEN FishBizz Workshop is to leverage multiple complementary standards rather than picking one isolated standard that may be strong in some areas, but weak in others. This will enable broader, more integrated traceability functionalities and enable lower cost implementations. Seafood businesses, associations, solution providers, and public agencies participate in the project.

The project team is reviewing various CEN, International Organization for Standardization (ISO), United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), Organization for the Advancement of Structured Information Standards (OASIS), and GS1/Electronic Product Code (EPC) standards used for electronic commerce in the seafood sector. These range from standards data at the component level and standards aimed at general principles for designing a traceability system, trough standards specifying how electronic transactions should be executed, and standards for business collaboration, including end-to-end

(Continued on Page 13)

Modeling and Coordinating Interdependent Critical Infrastructures in Montréal

by Professor Benoît Robert, Luciano Morabito, and Irène Cloutier
Centre Risque & Performance, Department of Mathematics and Industrial Engineering
École Polytechnique de Montréal (Québec, Canada)*

The analysis and modeling of all known and unknown interdependencies between the critical infrastructure (CI) of a given city, region, or country is a complex task. Furthermore, the collaboration and information sharing needed between the numerous public and private stakeholders and operators of critical systems (CSs) still remains an important challenge. Nevertheless, this task is necessary and ultimately aims at creating a more resilient nation and has become indispensable for most developed countries.[1]

In Montréal (Québec, Canada), an original approach has been developed in the last ten years and has now started to produce some interesting results; it has increased understanding of the interdependent links in a city or region and opened up new perspectives for the future.

This bottom-up approach was initiated by owners and operators of seven critical systems (CSs) in Montréal and public safety representatives of the city. These representatives mandated the Centre Risque & Performance (CRP) of the École Polytechnique de Montréal to develop an operational and economically feasible approach of analysis, modeling, and mapping of physical and geographical interdependencies among the CI in a city or region.

The CRP approach has led to the development of a modeling and mapping tool, DOMINO. There are few known tools enabling users to identify the interdependencies among the CI and anticipate the domino effects they can generate. Developed by the CRP and its partners, DOMINO is a decision and planning assistance tool that makes it possible to respond to this set of problems.

Approach and Concepts

DOMINO is a prototype of a system for managing interdependencies and analyzing domino effects; it comprises a database linked to a geographic information system. The tool's functioning relies on a consequence-based risk management approach[2] that aims to assess the propagation over time of the consequences for CSs of a situation that may trigger domino effects without a priori, dwelling on the causes that led to this situation. Given that civil security officers are responsible for managing these consequences, both for populations and for key infrastructures, the tool's results become a true aid for decision-making in a crisis management situation. The anticipation of the propagation of failures and the resulting consequences enable users to implement specific, appropriate mitigation measures to ensure public safety.

Confidentiality of Information

Confidentiality agreements with partners ensure that DOMINO preserves the confidentiality of data. For one thing, it is divided into two separate modules: a private data module for each system and a shared analysis module for all

(Continued on Page 4)

[1] United Nations, *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters,* United Nations, World Conference on Disaster Reduction, Kobe, Hyogo, Japan, (January 18-22, 2005).

[2] B. Robert, L. Morabito, and O. Quenneville, “The Preventive Approach to Risks Related to Interdependent Infrastructures,” *International Journal of Emergency Management,* Vol. 4, No. 2, (2007), 166–182; B. Robert and L. Morabito, “The Operational Tools for Managing Physical Interdependencies among Critical Infrastructures,” *International Journal of Critical Infrastructures,* Vol. 4, No. 4, (2008), 353–367; and B. Robert, R. de Calan, and L. Morabito, “Modelling Interdependencies among Critical Infrastructures,” *International Journal of Critical Infrastructures,* Vol. 4, No. 4, (2008), 392–408.

Montréal *(Cont. from 3)*

systems. A flexible cartography approach[3] has also been developed to avoid certain problems related to the cartographic representation of information and results.

DOMINO: A Modular Tool

DOMINO includes several modules that allow for use by CSs managers and civil security officers alike. It handles functional interdependencies by analyzing the customer-supplier relationships that exist among CIs.

It compiles data related to infrastructures, their location (precise or flexible), and the resources they use. For each infrastructure that plays a direct role in the accomplishment of a CS's mission, a supply zone is defined (a zone that will be deprived of the resource if the infrastructure fails). This information makes it possible to identify the infrastructures that depend on this resource and, in light of these functional dependency relations, to simulate potential domino effects.

Flexible Cartography

A major challenge to be met concerns the confidentiality of georeferenced information about the key infrastructures of each CS. In this context, DOMINO uses a flexible cartography approach to locate system infrastructures and simulate domino effects. It allows a system to locate its infrastructures on an ad hoc basis (by means of an address or coordinates) or more flexibly for infrastructures considered to be critical or sensitive. In this case, they can be located by using sectors whose size can range from one to several square kilometers.[4] In such a context, a point does not necessarily indicate

(Continued on Page 5)

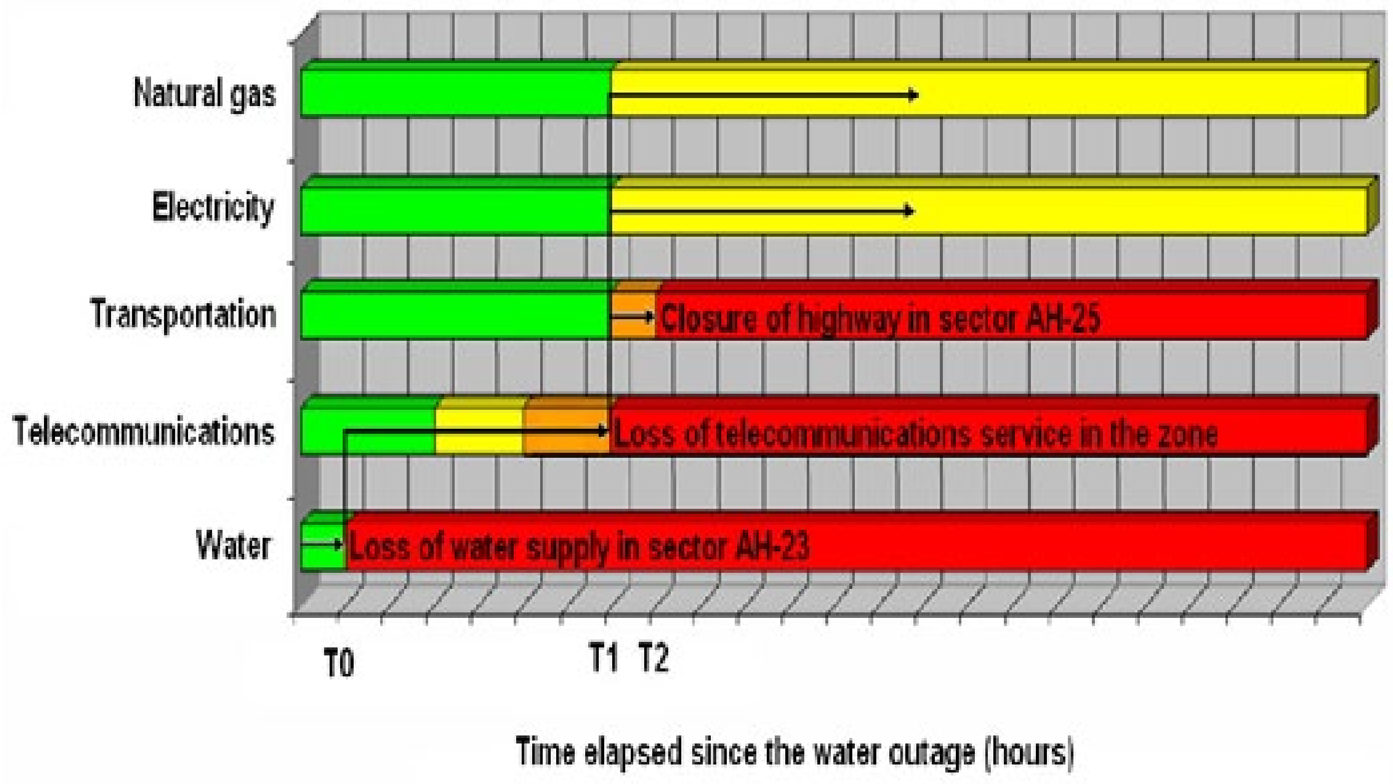


Figure 1: Example of Domino Effect Curves.[5]

[3] B. Robert and L. Morabito, "An Approach to Identifying Geographic Interdependencies among Critical Infrastructures," *International Journal of Critical Infrastructures*, Vol. 6, No. 1, (2010), 17–30.

[4] B. Robert and L. Morabito, "The Operational Tools for Managing Physical Interdependencies among Critical Infrastructures," *International Journal of Critical Infrastructures*, Vol. 4, No. 4, (2008), 353–367; and B. Robert and L. Morabito, "An Approach to Identifying Geographic Interdependencies among Critical Infrastructures," *International Journal of Critical Infrastructures*, Vol. 6, No. 1, (2010), 17–30.

[5] B. Robert and L. Morabito, "The Operational Tools for Managing Physical Interdependencies among Critical Infrastructures," *International Journal of Critical Infrastructures*, Vol. 4, No. 4, (2008), 353–367.

Montréal *(Cont. from 4)*

the exact position of an infrastructure but simply shows in which sector(s) it is located.

Data Module

The data module is reserved for CS managers, all of whom have protected access to the information on their own systems. All CS managers are also free to enter the data they consider appropriate into the system, based on the degree of confidentiality they wish to apply to their information. System owners are thus the only people likely to be able to judge the information that can be found in DOMINO.

Analysis Module

DOMINO offers numerous analyses. First, it enables users to characterize a territory in terms of dependency on a resource considered to be critical. For a given territory, maps of dependencies on these resources present all the equipment and infrastructures that use them, with turnaround times. In addition, analyses of the protective mechanisms in place are presented, such as the calculation of the volume of gasoline needed to supply generators in case of an electrical outage.

Overall, however, DOMINO is dedicated to the simulation of domino effects. This module allows users to simulate the domino effects triggered by a resource outage in a geographic sector. The results of this simulation are represented graphically in domino effect curves (see Figure 1 on Page 4).

Analysis reports are also provided. They present all the equipment and infrastructures affected, the planned protective measures, and a list of people to contact for each CS concerned. These reports allow managers to better understand the situation and potential changes in domino effects and thus help them make relevant, coherent decisions. These analyses of domino effects are complemented by a cartographic module that displays the propagation of failures over time and space.

Cartographic Module

Once the data have been compiled, the tool is able to simulate the domino effects generated by an outage of a resource in a sector. Figure 2 (Page 6) shows an example of propagation of a domino effect. For confidentiality reasons, none of the infrastructures affected by the outages are presented. Nevertheless, the diagrams do allow one to see the number and the status of these infrastructures for each CS.

A Crisis Management Tool

The cartographic results presented above mean that DOMINO can be an operational crisis management tool, given its capacity to simulate and anticipate what might happen in the first hours after a resource becomes unavailable. CSs' managers and civil security officers can then adapt their management decisions as a function of actual intervention conditions, such as a snowstorm, rush hour, a major sport, cultural, or political event, etc. They can adapt their messages to the public, plan protective measures, decide on the best time to evacuate buildings, etc.

Of course, these results allow users to adapt policies for prioritizing the recovery of certain resources to try to avoid the domino effects identified.

A Planning Tool

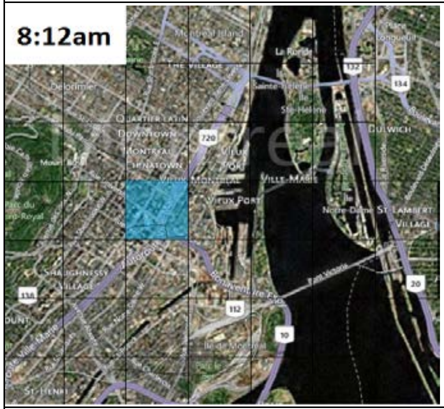
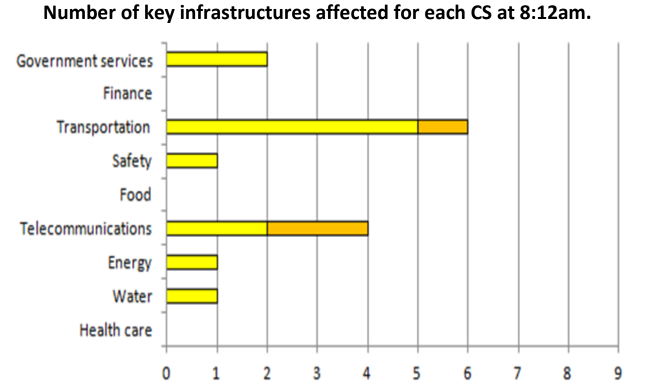
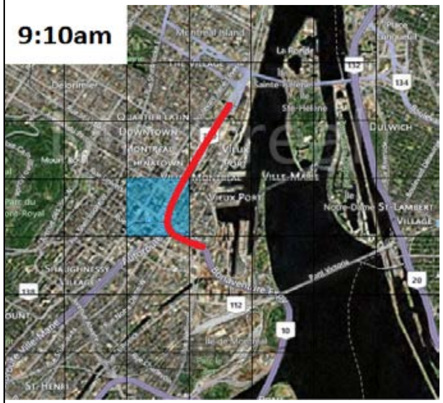
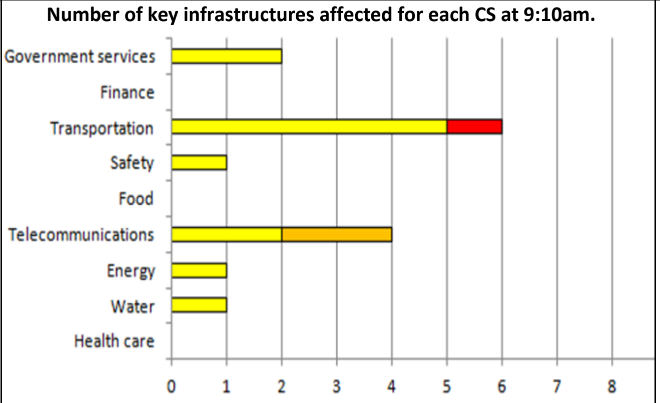
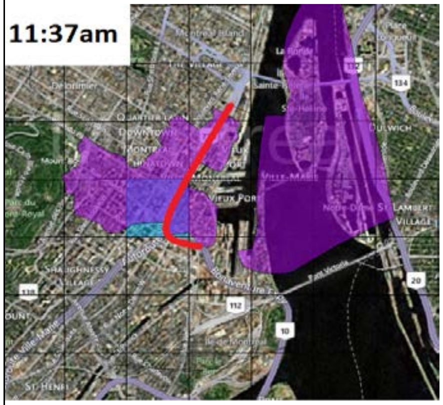
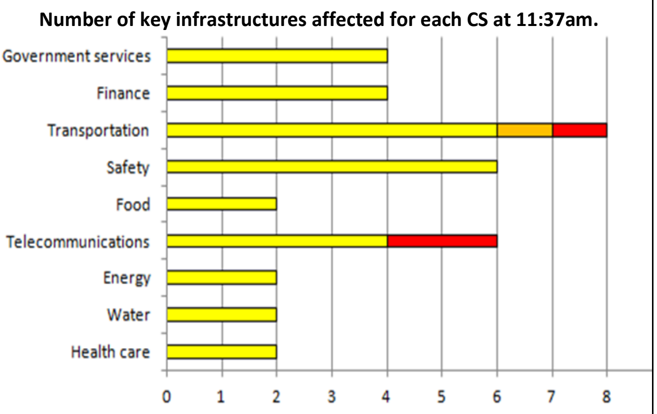
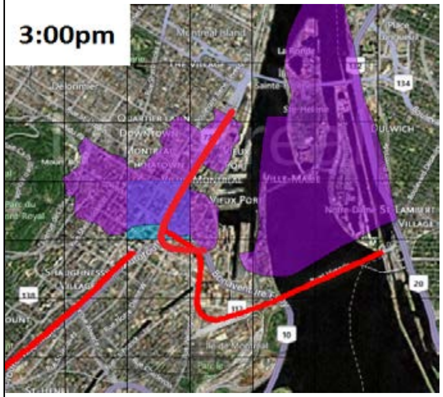
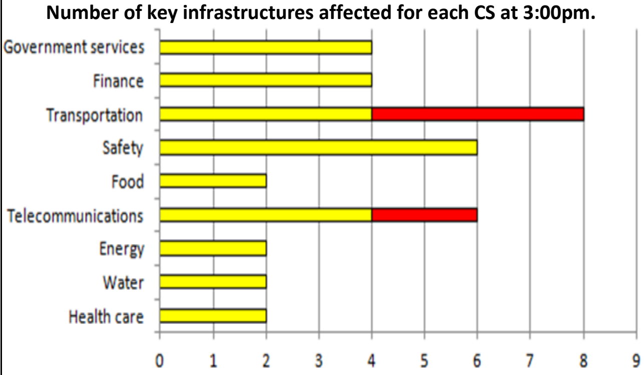
The concept of risk is based on a combination of hazards and consequences. DOMINO provides information on the consequences of a CS failure. This information must then be coupled with other tools describing certain natural and anthropogenic hazards.

For natural hazards, Figure 3 (Page 16) presents a map of the flood zone ensuing from the risk of a dam break. Some critical infrastructures are present in this flood zone, including an item of electrical equipment. The potential failure of this equipment would result in an outage in a zone within which more than 60 other infrastructures would be affected.

As for anthropogenic hazards, Figure 4 (Page 17) presents the simulation of an explosion of a ship in a port. Based on the radius of impact, DOMINO can be used to identify the infrastructures that may be affected, generating potential domino effects.

In addition to awareness of risks, such results can be used to develop emergency plans to manage multiple failures, as well as specific

(Continued on Page 6)

DOMINO simulation	Identification of CSs affected	Notes
		• Interruption of water supply in a specific geographic sector (blue square). • 15 critical assets impacted by the water outage among which 3 have a potential to fail (for confidentiality purposes, the figure do not show the assets).
		• Failure of an infrastructure belonging to a transportation system. • Disruption of road traffic anticipated (red zone).
		• Interruption of certain telecommunication services in the zone shown in purple. • Expansion of the impact zone.
		<u>**Situation after 7 hours**</u> • Loss of water supply. • Road traffic. • Disrupted telecommunications. • Effects on several transportation systems.

Legend : 🟡 Disrupted infrastructure - 🟠 Disrupted infrastructure with potential to fail - 🔴 Failed infrastructure

Figure 2 – Fictitious example of a spatiotemporal propagation of domino effects among the CI.

(Continued on Page 14)

Social Media Risks

by Mark Johnson, Chairman, The Risk Management Group, United Kingdom

Introduction

As technology continues to advance, eliminating communication barriers and challenging traditional border identities, cybersecurity has received no shortage of attention across the globe. One reason the cyber realm has become such a cause for concern is the vast amount of information now available on social media sites like Facebook, Twitter, and LinkedIn. This willingness to display personal information online provides ample opportunity for nefarious infiltration, resulting in amplified risk to connected critical infrastructure.

In late 2010, concerned about an increase in the number of burglaries being facilitated through social engineering of victims via Facebook, insurers Legal & General conducted a survey to assess the willingness of people in the United Kingdom to share personal data with strangers online.[1] The results were startling and showed that 59% of men and 42% of women surveyed admitted that they had accepted friend requests from strangers on Facebook based solely on liking the other person's photo. Another 13% of men and 9% of women had shared their phone numbers via Facebook, and 13% (9% men; 4% women) had posted their home addresses. As concern about vulnerabilities in Facebook and similar social media services grew during 2011, the University of British Colombia (UBC) conducted its own experiment, launching 100 fake profiles which generated 5,000 friend requests to test user's willingness to “friend” strangers.[2] According to the UBC report, 19% (596 users) accepted this first round of requests. The fake accounts then targeted the friends of the 19% and 59% (2,079) of those invited to ”friend” accepted.

While the Legal & General survey focuses on the importance of ”attractiveness,“ the UBC study addresses the principle of Triadic Closure — a theory postulating that you are more likely to accept a request of friendship from someone who is already a ”friend of a friend.” At The Risk Management Group (TRMG), we decided to conduct our own tests, fabricating five Facebook accounts, four with female profiles and one with a Neanderthal image and name. Within a week, the female profiles each had up to 140 Facebook friends and currently maintain an average of 175 friends. By friending and recommending the Neanderthal account, the fake female accounts were then able to find 36 friends willing to link with it, despite it clearly being a completely fake profile. Furthermore, the Neanderthal account would often ”like” photos and comments posted by others, leading some to offer friendship voluntarily. All five profiles were also consistently logged on from the same IP address, and after eight months neither Facebook, nor any of the ”friends” challenged any of the five profiles, including the Neanderthal.

This research indicates that the combination of Triadic Closure, Attractiveness, and Liking represents a valuable tool for those with malicious or criminal intent. There are several scenarios in which criminals might profit from these vulnerabilities, the main ones listed on the next page.

(Continued on Page 8)

[1] http://www.legalandgeneral.com/_resources/pdfs/insurance/digital-criminal-2.pdf.

[2] http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf.

Social Media *(Cont. from 7)*

Key Social Media Risks:

- **Targeting:** LinkedIn, Facebook, and others are excellent sources for criminals to target information. Many users post their locations, sometimes updating these automatically. Travel plans are included via services such as Tripit and Trip Advisor. This is compounded when "face bragging" occurs, and people boast about their wealth via social media sites or post images of their disposable assets. The concerns of Legal & General arose from this risk and observations about a number of insurance claims related to burglaries.

- **Identity Theft and Impersonation:** Not only are real names and photos displayed, but email addresses, phone numbers, children's names, and even dates of birth are regularly included in public profiles. All of this data can provide a basis for identity theft attacks and fraud exploits, and there is much anecdotal evidence to suggest that this is a widespread problem.

- **Data Disclosure:** Social media provides a mechanism for broadcasting confidential data to the whole planet, leading to breaches of data protection laws or other issues such as the Wikileaks disclosures.

- **Market Distortion via Fake Profiles:** Setting up a fake Facebook, Twitter, or LinkedIn profile is child's play, and the creation of fake company web pages is equally straightforward. By putting out inaccurate market information, a person could potentially distort the market with minimal risk of being detected. In fact, in December 2011, a series of false Tweets sent many thousands of Latvians running to their ATMs on a weekend to take out cash for fear that two banks, SEB and Swedbank, were pulling out of the country on Monday.

- **Reputational Harm & Blackmail:** By exploiting the attractiveness principle, a would-be blackmailer could execute a "honey trap attack" on a target, enticing him or her to say or do things that would be harmful if exposed. Blackmail can then follow.

- **Nigerian 419 Frauds:** These attacks, whereby an individual is convinced to advance a sum of money on the promise of a greater financial return, still occur and social media offers a potential gold mine to those wishing to more effectively adapt their 419 messages to their targets.

- **Exposure to Malware:** Social media sites can serve as malware vectors. There have been numerous instances of video and other links promoted via social media leading to malware infections. One piece of malware, "Koobface," has been specifically designed to install Botnet malware on Facebook user's systems. In this case, Facebook is fighting back by naming and shaming those behind the attack.

Open Source Social Media Monitoring Opportunities

While the online networking craze has led to increased cybersecurity risks in many areas, social media also provides an unprecedented open source monitoring opportunity for crime fighting and fraud prevention, necessary for protecting critical infrastructures such as those crucial to the financial industry. Examples of the types of fraud that can be detected through monitoring of social media feeds include:

- Market Distortion
- Insurance Fraud
- Fraudulent Sick Leave Claims
- Social Engineering Investigations
- Benefits Fraud

Due diligence research for anti-money laundering and other financial assessments (to assess politically exposed persons, for example) are also benefiting from social media monitoring.

Yet, open source monitoring is not a substitute for traditional intelligence and investigative techniques; rather, it provides an additional stream of data that can resolve different sets of issues and reveal personal information about criminals and their associates that would not previously have been available. Any investigator embarking on a social media open source intelligence (OSINT) exercise is advised to consider the risks very carefully. Foremost among these is the mistake of confusing intelligence with evidence. While the courts

(Continued on Page 15)

Creating a Secure and Efficient Supply Chain

In January 2012, the White House published the National Strategy for Global Supply Chain Security ("the Supply Chain Strategy") to "strengthen the global supply chain in order to protect the welfare and interests of the American people and secure our Nation's economic prosperity."[1] The Supply Chain Strategy sets two major goals: (1) to promote the secure and efficient movements of goods; and (2) to foster a resilient supply chain. Efficiency and security are often viewed as opposing goals when designing systems. Under this view, greater security requires more checkpoints, higher costs, greater delays and therefore reduces the efficiency of that system. The Supply Chain Strategy challenges this viewpoint and links security and efficiency under one goal and looks to link security as part of any efficient supply chain. This goal emphasizes the following objectives:

- Resolving Threats Early: Early identification of threats in a building in security practices into global supply chain processes will enable threats to be dealt with as soon as possible.

- Improving Verification and Detection: By improving on existing methods and techniques, screening processes will become more efficient and will help in ensuring only allowable cargo is transported and that the cargo is sent through in a predictable, expected manner pursuant to all regulations.

- Enhancing security of infrastructure and conveyances.

- Maximizing the Flow of Legitimate Trade: A multi-pronged approach will reduce the regulatory burden on low risk cargo, will enhance existing supply chain infrastructure, and improve relationships with important stakeholders. These steps will all help to enhance the efficiency of the supply chain as a whole.

The second goal of the Supply Chain Strategy is to create a resilient supply chain that, (1) mitigates systemic vulnerability and (2) promotes trade resumption policies and practices. When implemented, the two major goals will create a secure, efficient, and resilient supply chain system that will help promote American security and prosperity.

The Supply Chain Strategy also lays out a pathway from goals to reality. In particular, it envisions an integrated Federal effort that utilizes Federal resources in the most cost-effect manner by increasing information sharing, streamlining processes, and minimizing the differences in requirements across units. However, Federal effort must be supplemented by cooperation with State, local, tribal, and private sector stakeholders; the Supply Chain Strategy emphasizes the need to work with these partners to create an all-of-nation approach. International cooperation is also identified as a necessary component of this effort since the supply chainis globally interconnected and therefore extends beyond the exclusive jurisdiction of the United States. Addressing this will require the development of global standards, capability sharing, and "end-to-end supply chain security efforts."

Effective risk management must also be integrated into the supply chain process and the Supply Chain Strategy lays out steps to develop a supply chain risk management framework which will understand and address vulnerabilities, utilize layers of defense, and create an adaptive security posture to meet evolving steps.

The following diagram,[2] while slightly dated (on Page 12), provides a general outline for how implementation of the Supply Chain Strategy is envisioned to proceed.

(Continued on Page 12)

[1] National Strategy for Global Supply Chain Security, http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

[2] The U.S. National Strategy for Global Supply Chain Security, Presentation, Sean K. Moon, Senior Policy Advisor Transportation and Cargo Policy Development U.S. Department of Homeland Security (June 2011), available at http://www.dhs.gov/xlibrary/assets/global-supply-chain-moon-s.pdf.

Legal Insights

Cybersecurity: East versus West in the Struggle to Secure Technology

by Jessica Herrera-Flanigan
Partner, Monument Policy Group, and former Staff Director, House Homeland Security Committee

During the last twenty years, there has been an increasing amount of attention being paid to cybersecurity within the international community and among intergovernmental, international bodies such as the Council of Europe, Organisation for Economic and Cooperative Development, the then G-8, and other entities. Early on, these efforts focused largely on criminal laws (both substantive and procedural) or developing awareness of security in the broadest sense.

In recent years, however, the attention has shifted to larger debates about the future of the Internet and technology and the role cultural norms play in how nations agree to secure cyberspace. This debate has penetrated Internet governance, affecting Internet Corporation for Assigned Names and Numbers (ICANN), as well as larger international efforts to establish commonalities on a global problem that does not recognize international boundaries.

Interestingly, the debate has turned into one of East versus West and global dominance. This was last laid clear during the EastWest Institute's Second Worldwide Cybersecurity Summit: Mobilizing for International Action, where participants all agreed something should be done globally to address cybersecurity, but there was no consensus on the "something" that should be done.

One on side, the United States and many of its Western European allies have pushed for protecting systems against damage and compromise and protecting privacy, intellectual property, and human rights. The May 2011 International Strategy for Cyberspace issued by the White House summarized the Western position:

To realize fully the benefits that networked technology promises the world, these systems must function reliably and securely. People must have confidence that data will travel to its destination without disruption. Assuring the free flow of information, the security and privacy of data, and the integrity of the interconnected networks themselves are all essential to American and global economic prosperity, security, and the promotion of universal rights.[1]

On the other side, China and Russia have framed the debate as one of nations securing their systems by controlling content, communications, and social networking tools so as to ensure a nation's perceived cultural, political, economic, and social stability. Indeed, just last September, the two countries, joined by Tajikistan and Uzbekistan, proposed to the United Nations an International Code of Conduct for Information Security that required nations to pledge:

To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment…[2]

The code of conduct did not advance, but it did draw clearly the differences between the two approaches to cybersecurity. These differences are not easily overcome;

(Continued on Page 13)

[1] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[2] http://www.rusemb.org.uk/data/doc/internationalcodeeng.pdf.

Resiliency DC

at

George Mason University's Arlington Campus
Founder's Hall

Washington DC's Preeminent Government & Business Continuity Thought Leadership Event is Back!

The Center for Infraastructure Protection and Homeland Security (CIP/HS), the Business Continuity Institute (BCI), and NorthEast Disaster Recovery Information Exchange (NEDRIX) will be hosting this 1-day conference.

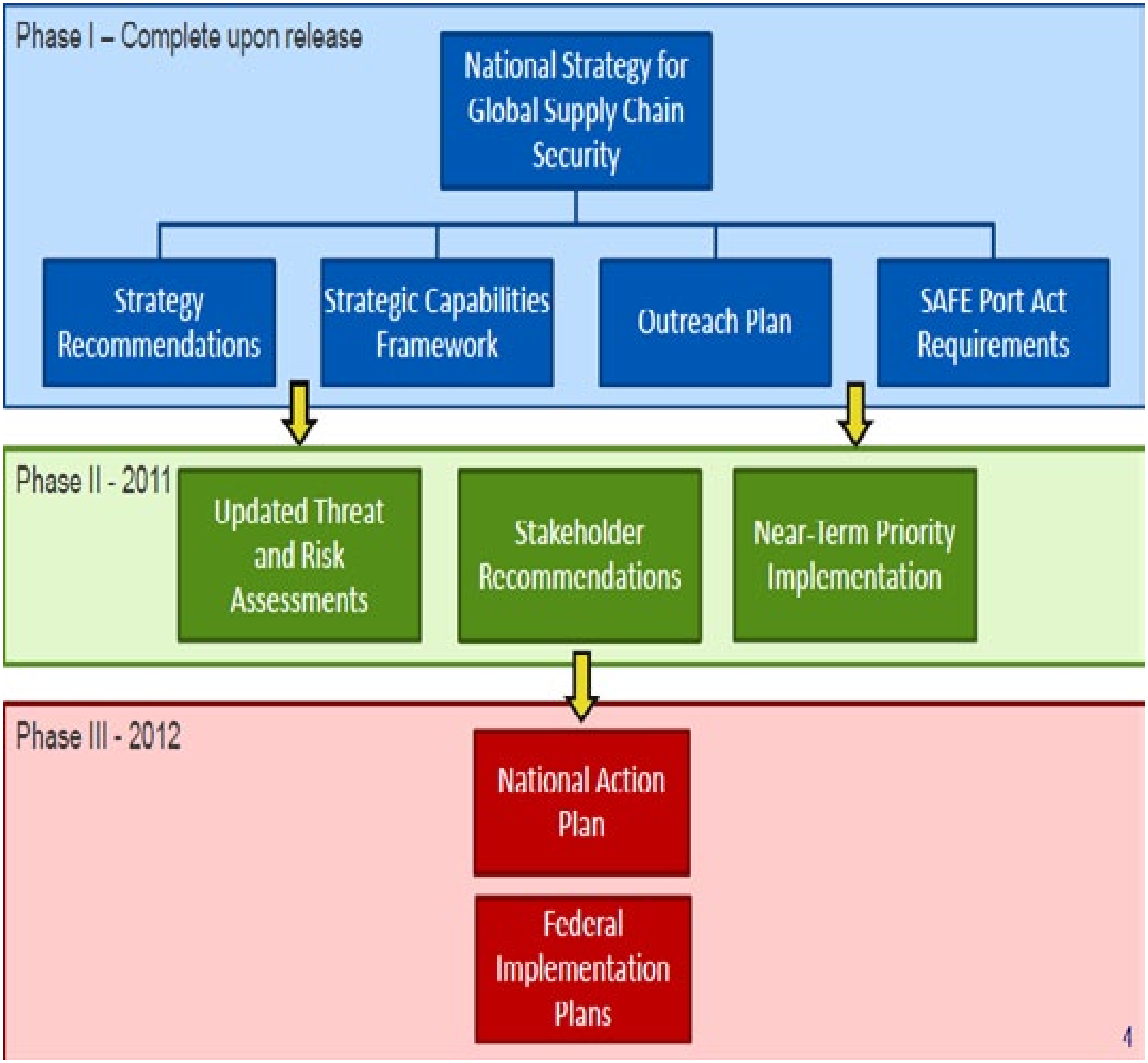
"Resiliency Integration of complementary disciplines and approaches." Over the past decade both the government and private sector have independently and collectively focused on developing and implementing various programs to ensure their organization is resilient to any threat or hazard. These complimentary programs include Continuity, Critical Infrastructure Protection (CIP), Emergency Management and Cyber Security. This event brings together experts from both the government and private sector to discuss how these programs are working to integrate and streamline while sharing their best practices, insights, and case studies. In addition, there will be a collaborative table-top exercise that will foster communication and information sharing amongst all attendees.

This one day conference brings together leaders and managers from both the government and private sector to discuss resiliency programs, challenges, successes, and case studies. This year's event expects to be better than last year as it will be held at George Mason University's Founders Hall, has some great speakers, and an interactive information sharing session in the afternoon. Below is the link to the website that provides information on the agenda and allows you to register.

For more information and to register, please visit
http://www.resiliencydc.com/

Global Supply Chain *(Cont. from 9)*

As the chart below indicates, efforts are already underway to implement the strategy. It is being led by the Cross-Sector Supply Chain Working Group, which was established under the Critical Infrastructure Partnership Advisory Council framework. Interested domestic and international partners who are not part of the working group can also submit comments via the DHS website.[3] The Supply Chain Strategy intends to build on earlier legislative acts[4] and incorporate them with public and private input in order to develop a robust, efficient and safe global supply chain. ❖


Phase I – Complete upon release
National Strategy for Global Supply Chain Security
Strategy Recommendations
Strategic Capabilities Framework
Outreach Plan
SAFE Port Act Requirements
Phase II - 2011
Updated Threat and Risk Assessments
Stakeholder Recommendations
Near-Term Priority Implementation
Phase III - 2012
National Action Plan
Federal Implementation Plans
4

[3] For more information, please visit http://www.dhs.gov/files/publications/national-strategy-for-global-supply-chain-security-feedback.shtm.

[4] Enacted legislation includes the Security and Accountability for Every Port Act, the Maritime Transportation Security Act and others.

European Commission *(Cont. from 2)*

supply chain visibility.

The FishBizz CWA intends to provide a technical specification for interoperable traceability solutions, which will connect both small and large supply chain actors and enable subject-matter experts to implement traceability requirements in an automated and cost-effective manner, and thus assist them in harvesting, processing, selling, and delivering sustainably sourced seafood to domestic and international markets. The CEN FishBizz Workshop will be completed in 2013. ❖

Legal Insights *(Cont. from 10)*

they threaten the possibility of cybersecurity success, as well as how innovation will develop in the future, especially as intellectual property threats and regime control over technology in certain nations increase. As the United States and its allies prioritize intellectual property theft as a cybersecurity issue, the role that China plays in cyber espionage cannot be taken lightly or disregarded.

Conversely, China is wary of the U.S. push for the international community to protect what the United States Department of State and Secretary of State Hillary Clinton has called the "freedom to connect"[3] — that is, the need to protect "freedom of expression, association and assembly in an online world."[4] This push is counter to China's "cultural" push for cybersecurity integrity.

It is not clear whether there can be a solution to the Internet liberty versus Internet sovereignty debate, which hinders our Nation's cybersecurity efforts, despite whatever laws the U.S. Congress may pass to address the issue. Cybersecurity is a global issue and only a global solution will ensure that the "weakest" links are addressed.

Unfortunately, the lack of a clear path forward could result in unintended consequences. Nations could decide that they will develop their own technical standards for the Internet and emerging technologies to try to address cybersecurity. If this occurs, we may find ourselves in a tech-Cold War where networks increasingly do not work together and are not compatible. Nations would maintain their sovereignty and values, but cybersecurity efforts would be left behind.

In order to successfully address cybersecurity, international norms must be developed and agreed upon by nations with fundamental differing visions of how technology should be managed and used by their citizens. Overcoming this barrier will require some creativity and quite possibly a grassroots movement on a global scale to push forward a forward-leaning comprehensive cybersecurity solution. ❖

[3] http://www.state.gov/secretary/rm/2010/01/135519.htm; and http://www.state.gov/secretary/rm/2011/02/156619.htm.

[4] http://www.state.gov/r/pa/prs/dpb/2011/12/178428.htm.

Montréal *(Cont. from 6)*

intervention plans for dealing with the failure of a resource, such as a plan related to the unavailability of drinking water in a specific district of a city. Such a plan should include all the CSs identified by DOMINO.

Needless to say, such results, which change over time, are particularly important for planning but are also valuable for conducting tabletop exercises.

Future Developments

DOMINO possesses the key advantage of being a simple, user-friendly tool. Given that it provides relevant information on CSs and their interdependencies, it is flexible enough to be used both for prevention/preparation and for intervention/recovery.

DOMINO is still in the prototype phase. Communication interfaces will have to be adapted for future uses. It will also have to be able to take account of multiple outages affecting infrastructures. For example, an infrastructure might be affected by a water outage and an electric outage simultaneously. At present, DOMINO is not accessible remotely. Ideally, such a system should be available 24/7. So it will be necessary to transfer DOMINO to a secure Web platform with links to geomatic tools.

Conclusion

DOMINO is not an end in itself; to fully understand what this tool represents, it is necessary to go well beyond its technical development. The development of such a tool requires a multidisciplinary approach that calls for managers and system experts to become involved in order to understand the way their systems function, their interdependencies and interconnections, and the consequences of their failure.

Although it is still only a prototype, this tool does respond to certain needs expressed by the CSs managers and civil security organizations in Quebec that participated in its development.

DOMINO is a tool that is integrated into an overall process intended to increase the resilience of our societies and their CI. The ultimate objective of this approach is to increase and share knowledge so we can make societies and organizations less vulnerable to failures and more resilient.

This process demands that organizations demonstrate a real will to cooperate over the long term. Such cooperation must be based on a mechanism for sharing and handling sensitive data in a context of mutual trust and respect of confidentiality.

Several challenges must still be met to enable the real-world implementation of this tool. The CRP's next projects will in fact involve meeting these challenges and actually deploying DOMINO in one or more municipalities. ❖

Acknowledgments

The CRP would like to thank its various public- and private-sector partners that contributed financially and with their expertise to the DOMINO research and development project: Agence Métropolitaine de Transport, Bell Canada, Defence Research and Development Canada, Gaz Métro, Hydro Québec, Ministère de la Sécurité publique du Québec, Ministère des Transports du Québec, Natural Sciences and Engineering Research Council of Canada, Public Safety Canada, Société de transport de Montréal, Ville de Montréal, Ville de Québec.

**Benoît Robert, Luciano Morabito and Irène Cloutier can be contacted at the Centre Risque & Performance of the École Polytechnique de Montréal at www.polymtl.ca/crp or benoit.rt@polymtl.ca.*

Social Media *(Cont. from 8)*

may not yet recognize the weaknesses inherent in data gathered from social media sites, this must surely change as time passes. There is an increasing awareness that the complete absence of identity verification and the apparently ineffective nature of the security mechanisms employed by sites like Facebook mean that "evidence" gathered from such sources is more and more likely to be contested. Indeed, retrospective reviews of such evidence may one day be required.

There are also serious ethical considerations to bear in mind, so before taking action, it is necessary to seek advice from both legal and human resource departments. The creation of a fake profile that leads to a conversation with the subject may represent entrapment in some circumstances. Clear legal guidelines are essential and evidentiary standards and principles will always apply. Privacy settings are available to all social media users and OSINT investigators must respect these; anything that lies behind the wall of privacy is not open source.

Whether being used by an OSINT investigator or a high school student, social media is a powerful tool that is fundamentally changing how humans interact around the world. The amount of information publicly posted and exchanged online is staggering, and magnifies the risks to increasingly interdependent critical infrastructures. Managing these risks begins with educating individuals about the potential harms that might result from a seemingly innocuous wall post or friend request. ❖

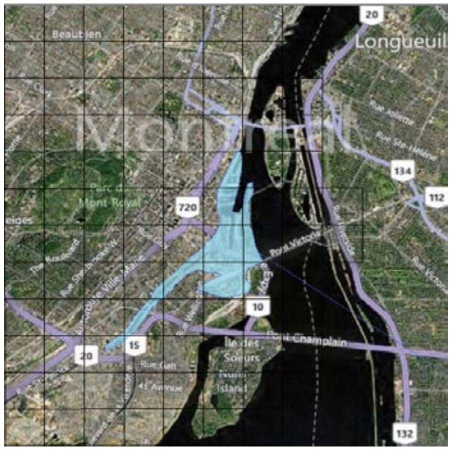
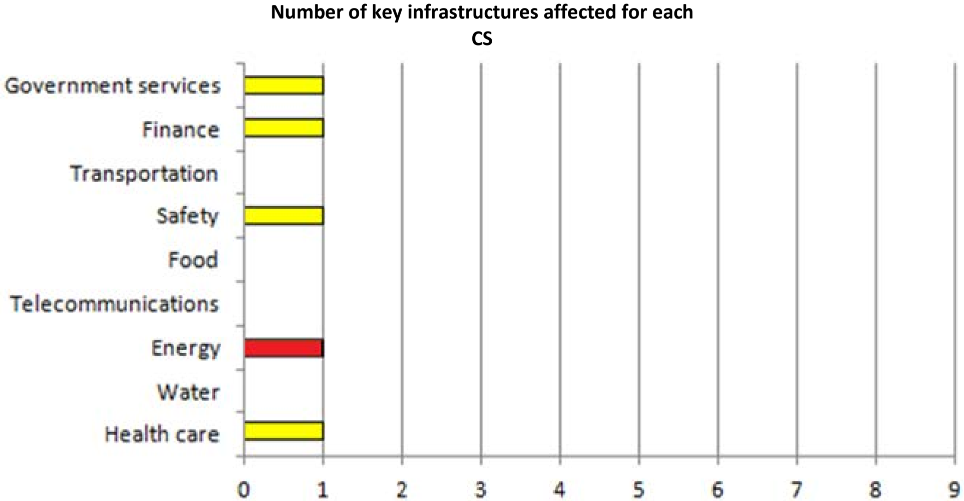
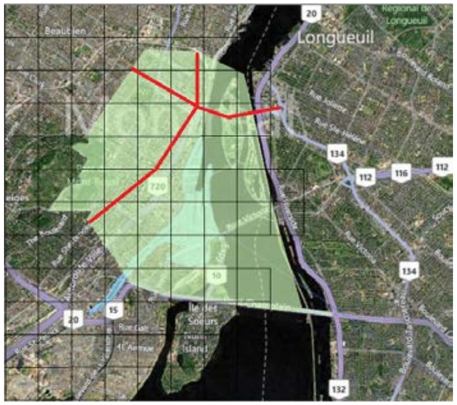
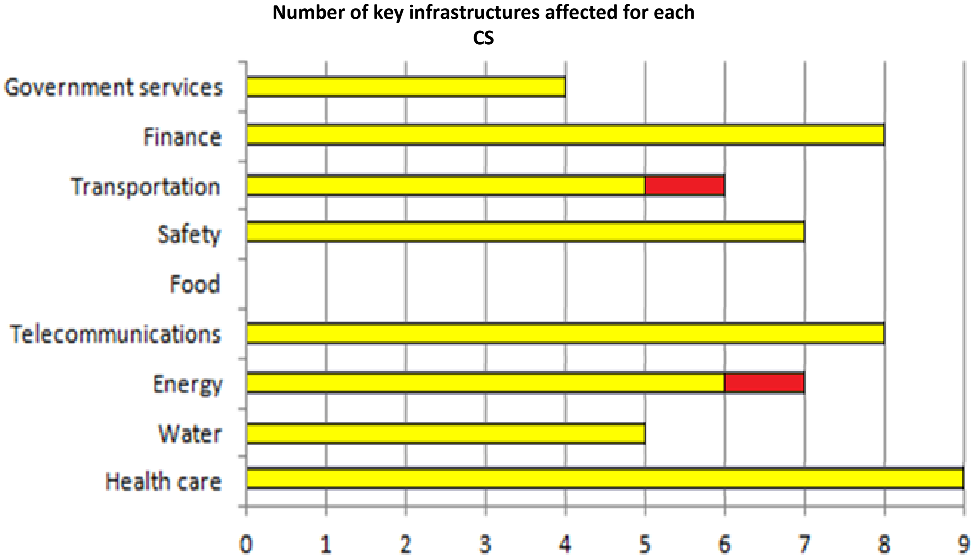
About TRMG

The Risk Management Group specialises in high tech risk management with a particular focus on cyber-crime, cyber laundering, communications fraud, and revenue assurance.

Since we were founded in 2001, our clients have included several leading solutions vendors in the fraud and revenue assurance space, major telecoms operators worldwide, large financial services organisations, the European Union Commission, the United Nations, The City of London Police, and many other private and public sector bodies.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University 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

DOMINO Simulation	Identification of CSs affected	Notes
 Longueuil Montréal Mont Royal 20 134 112 720 10 15 20 132 Pont Champlain Île des Soeurs Island		• Flood in the area depicted in blue. • 5 critical assets potentially impacted by the flood among which one will generate a power failure. • Multiple roads closures in the flooded area.
 Longueuil 20 134 112 116 112 20 15 134 132		• Potential electricity outage in the area depicted in green. • Over 60 critical assets impacted by the loss of electricity. • Loss of electricity at a metro power station creating a loss of service on 3 lanes. • Potential road traffic caused by the non-operating traffic lights. • No other domino effects anticipated for the first 72 hours if all backup systems are operating correctly.

Legend : 🟡 Disrupted infrastructure - 🟠 Disrupted infrastructure with potential to fail - 🔴 Failed infrastructure

Figure 1 – Fictitious example of the use of DOMINO to analyze the consequences of a flood for CSs.

(Continued on Page 17)

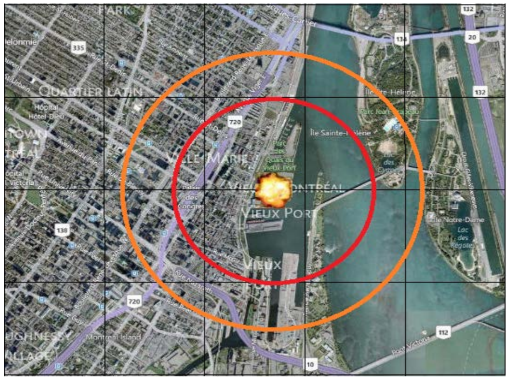
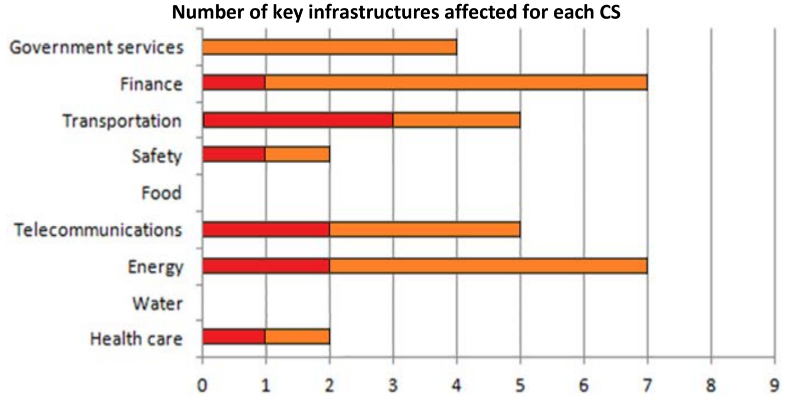
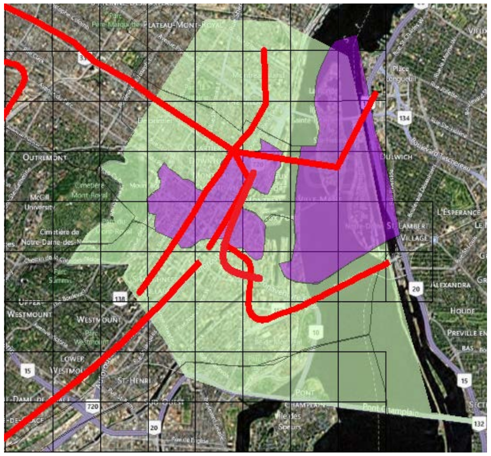
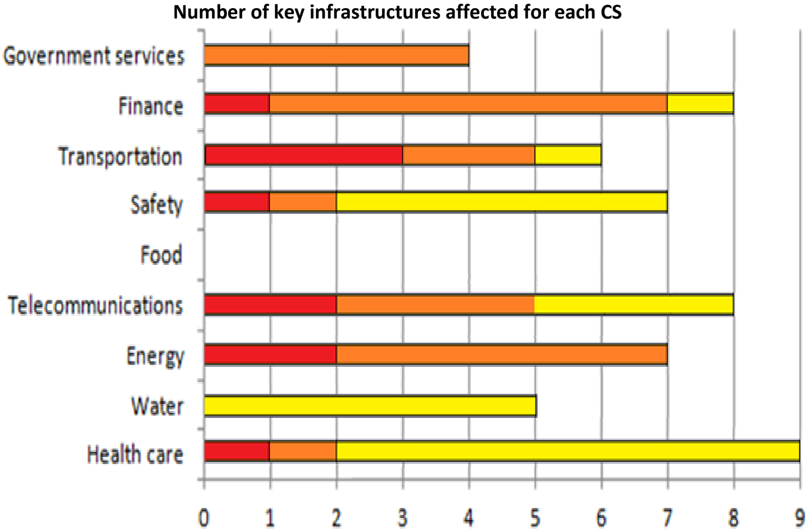
DOMINO Simulation	Identification of CSs affected	Notes
		• Explosion in the port. • Radius of impact : 1km – 1,5km • 9 critical assets located in the 1km radius • Over 30 critical assets located in the 1,5km radius.
		• Massive evacuation of multiple buildings. • Potential loss of telecommunications in the area depicted in purple impacting other critical assets. • Potential loss of electricity in the area depicted in green impacting other critical assets. • Potential loss of service in public transit and road transit.
Legend : 🟡 Disrupted infrastructure - 🟠 Disrupted infrastructure with potential to fail - 🔴 Failed infrastructure		

Figure 4 - Fictitious example of the use of DOMINO to analyze the consequences of an explosion for CSs.