THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

VOLUME 14 NUMBER 8

MAY 2015
INTERNATIONAL ISSUES

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

This month's *The CIP Report* focuses on **International Issues** of Critical Infrastructure Security and Resilience, recognizing that CISR threats are not limited by national boundaries. Likewise, national preferences and policies shape solutions in this space and provide the basis for different approaches. Therefore a consideration of international aspects is essential to understand threats, form solutions, and learn from different approaches.

GEORGE MASON UNIVERSITY
School of Law

CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

The first article, written by European colleagues Eric Luiijf MSc, Marianthi Theocharidou PhD, and Erich Rome PhD, highlights an online critical infrastructure security and resilience resource similar to Wikipedia. Next, an article from American and Canadian colleagues associated with Argonne National Laboratory, Public Safety Canada, and the U.S. Department of Homeland Security discuss their cross-border collaboration in developing a new tool to evaluate Canadian critical infrastructure.

The Fourth Annual Global Conference on CyberSpace, which took place in The Hague, The Netherlands in April 2015 is the subject of Eric Luiijf's second article. Ms. Tehreem Saifey, graduate research assistant with the Center for Infrastructure Protection and Homeland Security, offers an article on critical infrastructure considerations associated with Turkey's energy sector.

An enduring theme of the past few months' Director Letters has been change. To that end, I would like to keep you apprised of several developments you will see over the next few months. First, the Center is moving from the School of Law to the School of Business here at George Mason University. The GMU School of Law has been our home for over eleven years, and we will retain the close relationship built over a decade of collaboration as we move forward. We will remain located on the Arlington Campus of GMU, as the location affords us a close connection with thought leaders and research partners in the critical infrastructure space. The move to the GMU School of Business strengthens the multidisciplinary approach of our work. Our new affiliation reflects the reality that while security is a public concern, the vast majority of critical infrastructure assets reside in the private sector. Therefore, private-public partnerships and solutions are the path to success for CISR research and education.

Second, we will change *The CIP Report* from this PDF- and paper- based format to one that is more web-based. You will receive this publication monthly as you always have. The new format will contain the entire publication in the body of the e-mail and feature links to the articles which will be located on our website.

(Continued on Page 2)

(Continued from Page 1)

This change will allow us to publish articles as they are written, and will allow you to download individual articles rather than an entire document. We believe this evolution will make information more current and enhance your user experience. Don't worry- all of our previous *CIP Report* issues will be available on the archives section of our website as they have always been. To that end, our June issue on energy will be our last *CIP Report* in PDF format.

Finally, as part of our new affiliation, we asked and received permission from our University President to change our name to the ***Center for Infrastructure Security and Resilience***. We believe this evolution reflects thinking past a sole focus on security to one that considers all-hazard and risk- based approaches as well as solutions across all mission areas. As always, we seek to be thought leaders who stir research, education, dialogue, and solutions that lead to a secure and resilient infrastructure.

We would like to take this opportunity to thank this month's contributors. 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.

Warm Regards,

Mark Troutman, PhD
Director, Center for Infrastructure Protection and Homeland Security

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

CIPedia©: A Critical Infrastructure Protection and Resilience Resource

by Eric Luiijf MSc , Marianthi Theocharidou PhD, and Erich Rome PhD

CIPedia© (www.cipedia.eu) is a Wiki-based body of common knowledge for the wide international community of critical infrastructure (CI) protection and resilience stakeholders such as policy makers, researchers, governmental agencies, emergency management organizations, CI operators, and even the public.

CIPedia is developed within the European Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project. CIPRNet is a Network of Excellence project co-funded by the security research program within the 7th Research Framework Program (FP7) of the European Union. The CIPRNet consortium includes six European research institutes (Fraunhofer, ENEA, TNO, CEA, JRC, Deltares), the international union of railways UIC, the universities of Rome, Cyprus, Bydgoszcz (Poland), and British Columbia (Canada), and ACRIS GmbH (Switzerland). The project coordination is by the German Fraunhofer Institute for Intelligent Analysis and Information Systems. The consortium brings together a unique set of knowledge and technology gathered in over sixty previous national and international research and development projects in the field of Critical Infrastructure Protection (CIP). Each consortium partner also functions as a multiplier by connecting their (inter)national networks and research platforms to CIPRNet's core activities and capabilities.

CIPedia, The Idea

One of CIPRNet's objectives is to enhance the preparedness and response capabilities of the European CI stakeholders and to increase the resilience Europe's complex system of interconnected and dependent CI across the 28 EU member nations and some of its associated nations.

Based on earlier experience in European projects by the consortium partners and discussions during the project proposal phase, it was recognized that many definitions in the domain of critical infrastructure preparedness, protection and resilience differ from nation to nation, and from community to community. Sometimes the differences are slight; sometimes there are fundamental differences in approach. When one understands that there is a difference, it is easy to understand the other position. For that reason, the CIPRNet project has as one of its objective to improve the capability to cross-communicate within the multi-disciplinary domain of CI protection and resilience stakeholders by developing CIPedia.

The Objectives

CIPedia is a Wikipedia-based international glossary on CIP and Critical Infrastructure Resilience (CIR). CIPedia aims to establish itself as a much needed but, up to the advent of CIPedia, missing common global reference point for CIP concepts and definitions. CIP/CIR terminology varies significantly due to contextual or sectoral differences, which, combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia will not aim at resolving such conflicts. On the contrary, CIPedia tries to serve as a point of disambiguation where various meanings and definitions are listed, guiding the reader to seek additional information to the relevant sources. CIPedia should not attempt to decide upon a common definition, as this should be a process achieved collectively by the CIP/CIR community. CIPedia is a collaboration platform that may facilitate efforts towards such a direction, but it will not act as a moderator on terminology discussion. In this way, CIPedia will foster the efficiency of interdisciplinary communication and the cohesion of the multi-disciplinary CIP/CIR community, both foundations for enhanced innovation.

The Resource

CIPedia went public mid-2014. In its initial phase it was populated by members of the consortium by using definitions and terminology from earlier International projects such as Australia's Independent

(Continued on Page 4)

(Continued from Page 2)

Research Institute Infrastructure Support Scheme (IRIIS) and the Netherlands' Designing an Interoperable European federated Simulation network for Critical InfraStructures project (DIESIS), the European Reference Network for Critical Infrastructure Protection (ERNCIP) community, and national resources and literature known by the consortium partners. Many improvements took place based on inputs received from the early set of users. End of 2014, CIPedia moved to its next phase where stakeholders from the CIP/CIR domain can become a registered user. They can contribute and/or moderate this online global community service by providing additional entries to the glossary, and by further enriching it. To become a registered user, one needs to acquire a username/password combination by sending an email to the authors of this article. We invite you all to become actively involved in the international CIPedia community and making this resource even more useful.

CIPedia is currently already more than just a glossary. As a CIP/CIR portal it provides access to a list of CIP conferences, a table with web pointers to CI sector-specific glossaries, and a pointer to the CIP bibliography. Please let us know about yet unlisted articles 'that make the difference' and need to be added to the CIP bibliography. Please provide (validated) BibTeX entries describing those articles or other written resources by email to us. The address has been provided at the end of the article.

Roadmap

In the current stage of development, CIPedia may resemble a glossary, which means it will be a collection of articles—one article per concept with key definitions. However, we aim to expand it over time and include discussions on each concept, links to useful information, important references, disambiguation notes, et cetera. Just like Wikipedia, new entries or 'articles' should begin with an appropriate definition or possible two or more rival definitions as well as other types of information about that topic as well. The full articles will eventually grow into a form very different from dictionary entries. Moreover, if two concepts are used in a similar way, they can be merged into one article and a discussion on their use can follow. As explained above, CIPedia will not try to reach consensus about which term or which definition is optimum, but it will record any differences in opinion or approach.

We are already making our mind up about CIPedia© 2.0. Your input is welcome. Do not refrain from sending us your suggestions for improvement and pointers to additional resources that need to be considered for inclusion.

Conclusion

To conclude: take a look, contribute, and spread the news about this resource developed for the whole global CIP/CIR community!

*Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. Since 2000 he contributed to many national and EU projects

(Continued on Page 5)

(Continued from Page 4)

in the field of Critical (Information) Infrastructure Protection, both at the technical and policy levels. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism and warfare, C(I)IP, process control security, and cyber security. He has been interviewed many times by press, radio and TV on these topics. Contact information: eric.luiijf@tno.nl

Marianthi Theocharidou PhD works as a scientific/technical support officer at the European Commission Joint Research Centre Institute for the Protection and Security of the Citizen in Ispra, Italy. She is currently working for the FP7 project CIPRNet and for JRC's European Reference Network for Critical Infrastructure Protection (ERNCIP). She has published several peer-reviewed articles about risk assessment and critical infrastructure protection. Contact information: marianthi.theocharidou@jrc.ec.europa.eu

Erich Rome PhD is a senior researcher and project manager at Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS' ART department in Germany. Since 2007, Erich Rome investigates MS&A for CIP and multi-sensory systems for surveillance and security. He published numerous peer-reviewed publications, edited several books and is a member of the steering committee of the workshop series CRITIS. So far, he coordinated four EU projects, CIPRNet being the current one. Contact information: erich.rome@iais.fraunhofer.de ❖

The Critical Infrastructure Resilience Tool – A Tool to Evaluate Canadian Critical Infrastructure

by Marie-Pierre Parenteau, PhD, Karen Guziel, Frederic Petit, PhD, and Michael Norman

Background

Recognizing the interconnected nature of critical infrastructure and the already strong private cross-border collaboration, the governments of the United States and Canada released the *Canada-United States Action Plan for Critical Infrastructure* in 2010.[1] This document was aimed at strengthening the safety, security, and resilience of both Canada and the United States by promoting an integrated approach to critical infrastructure protection and resilience. Announced in 2011 by President Obama and Prime Minister Harper, the *Beyond the Border Action Plan* identified four areas of cooperation between the two nations.[2] Part IV of the Action Plan, Critical Infrastructure and Cyber-Security, "includes measures to enhance the resiliency of our shared critical and cyber infrastructure, and to enable our two countries to rapidly respond to and recover from disasters and emergencies on either side of the border."[3]

Launched in 2011 as a deliverable under the *Beyond the Border Action Plan* and the *Canada-United States Action Plan*, a pilot Regional Resilience Assessment Program (RRAP) project was completed in 2013 by Public Safety Canada (PS) and the U.S. Department of Homeland Security (DHS). Focused on the energy sector in the geographic area of Maine and New Brunswick, the project included site assessments in the United States and Canada. The project team employed the Infrastructure Survey Tool (IST) — a question set developed by DHS and Argonne National Laboratory (Argonne) for the Enhanced Critical Infrastructure Protection (ECIP) program[4]— to collect information from critical infrastructure stakeholders in order to assess individual facilities' protective and resilience measures and compare them with measures implemented at similar facilities.

Following the success of this cross-border project, Canadian critical infrastructure stakeholders expressed a strong interest for the IST and supported PS's initiative to adopt a survey approach in its infrastructure protection efforts. Leveraging existing mechanisms for information sharing between Canada and the United States, PS was able to initiate a project with DHS and Argonne for the development of the Canadian Infrastructure Resilience Tool (CIRT).

Critical Infrastructure Resilience Tool

The CIRT is based on the IST and was developed by DHS and Argonne in close collaboration and partnership with PS. Like the IST, it uses multi-attribute utility theory (MAUT) and Value-focused Thinking principles to generate reproducible indices (Protective Measures Index [PMI] and Resilience Measurement Index [RMI]) that capture and evaluate aspects of protection, resilience, and dependencies in a standardized process. The output of the tool includes a report and

(Continued on Page 7)

[1] United States Department of Homeland Security and Public Safety Canada, *Canada-United States Action Plan for Critical Infrastructure* (2010), available at http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (accessed April 10, 2015).
[2] *United States-Canada Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, (Washington, D.C.: The White House, 2011), available at http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf, (accessed April 10, 2015).
[3] Ibid.
[4] "Enhanced Critical Infrastructure Protection," *U.S. Department of Homeland Security* (Dec. 4, 2014), available at http://www.dhs.gov/ecip (accessed April 27, 2015).

(Continued from Page 6)

indices dashboards that compare a stakeholder's facility with other similar facilities. The PMI[5] characterizes the security posture of a facility at its "weakest link" across each aspect of security. The RMI[6] characterizes resilience management procedures, disaster response, and business continuity. The PMI and RMI together can be used by the owner and operator of the facility to guide risk-based decision making to improve the overall security and resilience at a facility.

The CIRT components rely on the following Microsoft Office 2010 tools for execution:

1. Builder (Access)
2. PMI and RMI Dashboards (Excel)
3. Report (Word)

The CIRT is available in both official languages, English and French.[7] The Builder provides the assessor with the option of displaying the question set in either language while conducting the assessment. Products for the stakeholders are also available in both official languages, with the option of toggling from one language to the other when displaying the PMI and RMI dashboards.

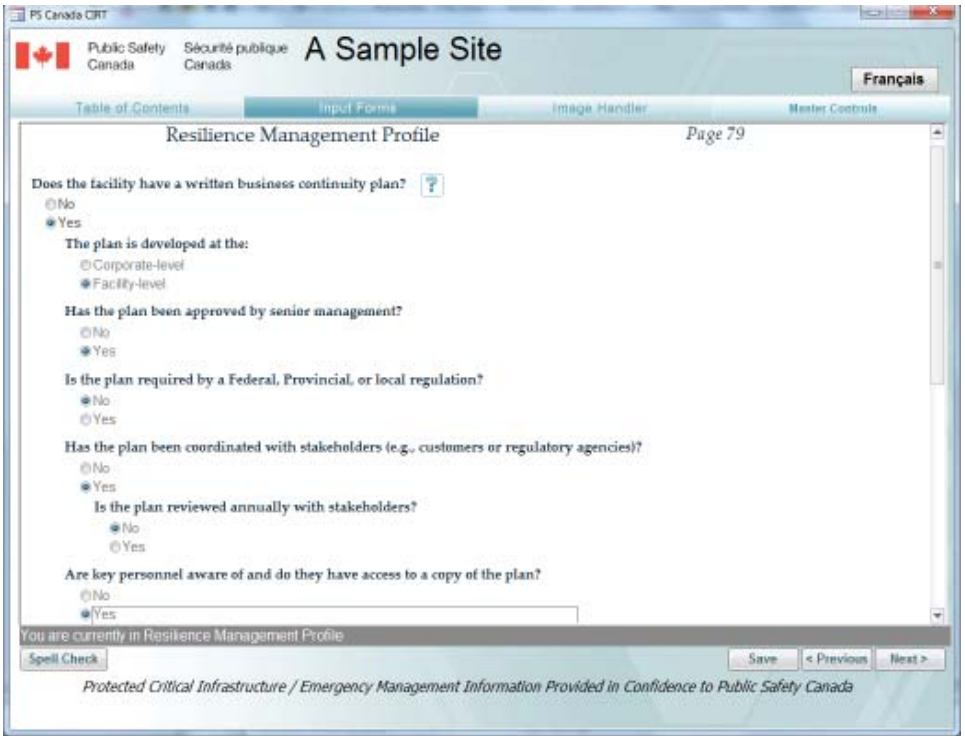

Figure 1 CIRT Builder — Used by Field Assessors to Collect Information

The CIRT question set follows the structure established in the DHS IST V.4, with adjustments to reflect conditions specific to Canada. For example, information-sharing organizations were revised to reflect Canadian organizations such as the Royal Canadian Mounted Police, PS, and Natural Resources Canada.

Builder

The Builder enables the collection of standardized information by a team of PS field assessors during interviews with stakeholders. The Builder allows the information to be collected by one assessor or by a team of assessors for a single facility; in the latter case, the information from multiple assessors is merged at PS Headquarters. The Builder (Figure 1) presents assessment questions and comment boxes for use by the assessor to capture supplementary information and information specific to vulnerabilities, options

(Continued on Page 8)

[5] The PMI is presented in more detail inFrederic D. Petit, Gilbert W. Bassett, William A. Buehring, Michael J. Collins, David C. Dickinson, Rebecca A. Haffenden, Andy A. Huttenga, Mary S. Klett, Julia A. Phillips, Sara N. Veselka, Kelly E. Wallace, Ronald G. Whitfield, and James P. Peerenboom, P*rotective Measures Index and Vulnerability: Indicators of Critical Infrastructure Protection and Vulnerability*, ANL/DIS-13-04 (Chicago: Argonne National Laboratory, 2013).

[6] The RMI is presented in more detail in Frederic D. Petit, Gilbert W. Bassett, Ronald Black, William A. Buehring, Michael J. Collins, David C. Dickinson, Ronald E. Fisher, Rebecca A. Haffenden, Andy A. Huttenga, Mary S. Klett, Julia A. Phillips, Melvin Thomas, Sara N. Veselka, Kelly E. Wallace, Ronald G. Whitfield, and James P. Peerenboom, *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, ANL/DIS-13-01 (Chicago: Argonne National Laboratory, 2013).

[7] In accordance to the *Official Languages Act,* which reaffirms the equal status of English and French as the official languages of Canada and establishes equal rights and privileges for their use in institutions. More information on the Official Languages Act is available from the Department of Justice (Official Languages Act, R.S.C. 1985, c. 31 (4th Supp.)).

(Continued from Page 7)

for consideration, and commendables.

PMI and RMI Dashboards

Once the information collected by the assessors has been verified by analysts at PS Headquarters, the PMI and RMI dashboards are generated from the Builder. The interactive dashboards are Excel files that allow stakeholders to view their results in comparison with those of other similar facilities. The comparison groups are currently based on DHS Taxonomy categories,[8] but as the number of CIRT assessments increases, Canada-specific data will be available for comparison. The dashboards can be used to create scenarios and assess the relative improvement of a facility's overall security posture and resilience when specific measures and/or procedures are added or changed. The facility may enhance its security posture and resilience by developing policies, procedures, or operational methods.[9]

The Overview Tab of the PMI dashboard (Figure 2) displays the overall PMI chart and its five level 1 variables (Physical Security, Security Management, Security Force, Information Sharing, and Security Activity Background). The dark bars represent the facility's current PMI values; the light bars represent the resulting PMI based on an owner-defined scenario using the interactive feature of the dashboard. The PMI values for the facility can be compared with the lowest value of the comparative group (white circle), the average value (light grey circle) and the comparative group high (dark circle). The RMI dashboard is structured in the same manner as the PMI dashboard; it has an Overview tab that displays the overall RMI chart and its four level 1 variables (Preparedness, Mitigation Measures, Response Capabilities, and Recovery Mechanisms).

Figure 2 PMI Dashboard — The Overview Tab (Illustrative)

The remaining tabs in the PMI and RMI dashboards provide the capacity to create 'what-if' scenarios. By selecting an option, a user can see how changes to policies, procedures, or operational methods would affect the overall PMI or RMI and their respective sub-level values (Figure 3).

(Continued on Page 9)

[8] "Infrastructure Data Taxonomy – Common Terminology for Describing Critical Infrastructure," *U.S. Department of Homeland Security* (March 11, 2015), http://www.dhs.gov/infrastructure-data-taxonomy (accessed April 27, 2015).

[9] "Infrastructure Data Taxonomy – Common Terminology for Describing Critical Infrastructure," U.S. Department of Homeland Security (March 11, 2015), http://www.dhs.gov/infrastructure-data-taxonomy (accessed April 27, 2015).

(Continued from Page 8)

Report

The CIRT also generates a report by extracting information from the Builder and the PMI and the RMI dashboards. The report includes background information on the CIRT, components of the PMI and the RMI, significant assets and areas, dependencies, commendables, vulnerabilities and options for consideration. Graphs of the overall PMI and overall RMI are also included in the report, along with a short description. The report provides information that reflects facility conditions at the time of the assessment.

Information Protection

PS's responsibilities under both the Emergency Management Act (EMA)[10] and the *Department of Public Safety and Emergency Preparedness Act*,[11] include facilitating the sharing of information to strengthen emergency preparedness and public safety.

The EMA includes a consequential amendment to the *Access to Information Act* that allows the Government of Canada to protect specific critical infrastructure information supplied in confidence to the Government by third parties. All CIRT products are appropriately marked so that they can be protected under this exemption. Exemptions from disclosure for reasons of national security and public safety also exist under legislation addressing Federal/provincial/territorial access to and freedom of information.[12]

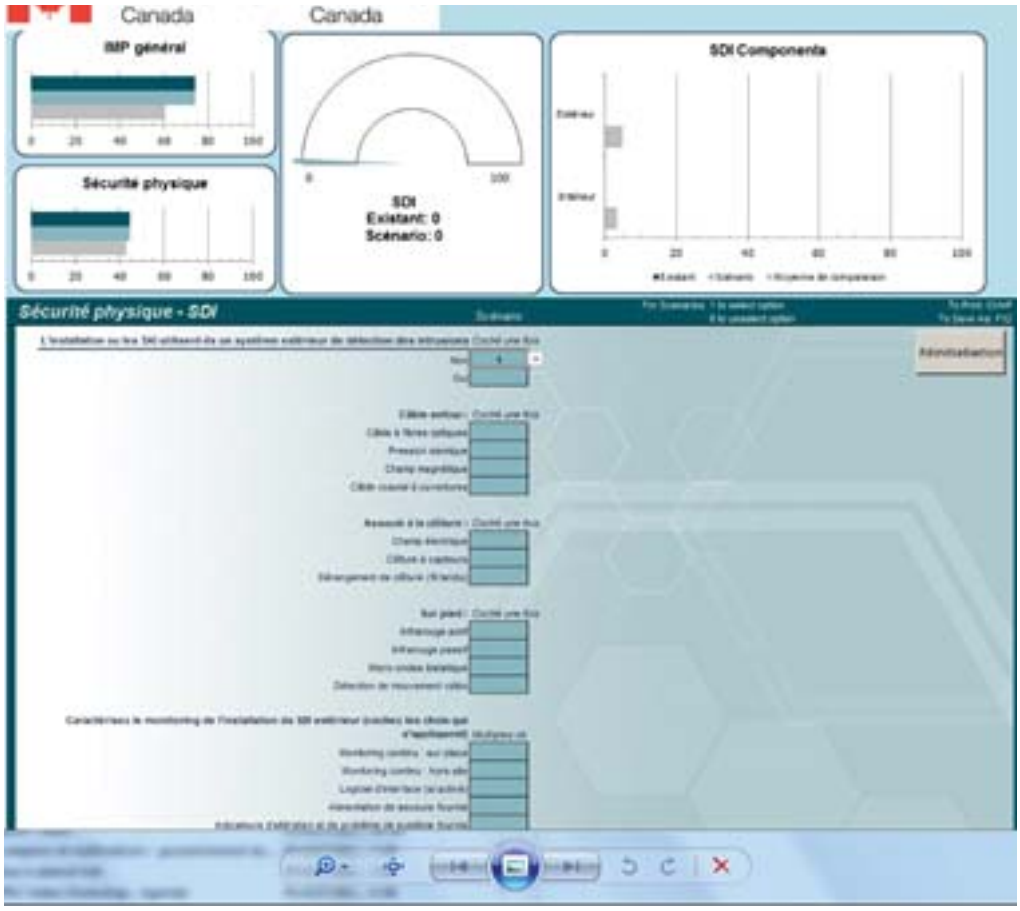

Figure 3 PMI Dashboard — The Physical Security/IDS Tab (Illustrative)

Tool Implementation

In addition to supporting Canada-United States critical infrastructure initiatives, the CIRT will enable PS to deliver on its commitment under the *National Strategy for Critical Infrastructure*[13] and *Action Plan for Critical Infrastructure*.[14] The Action Plan identifies three strategic objectives for enhancing the resilience of critical infrastructure in Canada; one of them is the implementation of an all-hazards

(Continued on Page 10)

[10] Emergency Management Act, S.C. 2007, c. 15 (Can.), available at http://laws-lois.justice.gc.ca/eng/acts/E-4.56/.
[11] Department of Public Safety and Emergency Preparedness Act, S.C. 2005, c. 10 (Can.), available at http://laws.justice.gc.ca/eng/acts/P-31.55/.
[12] Public Safety Canada, *Identifying and Marking Critical Infrastructure Management (CI/EM) Information Shared in Confidence with the Government of Canada* (Ottawa; Public Safety Canada, 2014), available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dntfng-mrkng/dntfng-mrkng-eng.pdf (accessed April 8, 2015).
[13] Public Safety Canada, *National Strategy for Critical Infrastructure* (Ottawa; Public Safety Canada, 2014), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx (accessed April 7, 2015).
[14] Public Safety Canada, *Action Plan for Critical Infrastructure* (2014-2017) (Ottawa: Public Safety Canada, 2014), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx (accessed April 7, 2015).

(Continued from Page 9)

risk management approach. A key action identified to attain this objective is the implementation of assessment tools acquired during the inaugural Maine-New Brunswick RRAP, including the CIRT.

It is anticipated that PS will leverage U.S. data in the dashboards' comparative analysis for the next 3 years. During that period, PS will create a database to support development of Canadian comparative statistics. In accordance with PS's commitment to stakeholders, only aggregated data will be used to support the comparative analysis.

A second objective is to develop analytical products for stakeholders that leverage the CIRT database. Analytical products focused on vulnerabilities, dependencies, and other information extracted from the CIRT will be developed by each sector/sub-sector as sufficient Canadian data become available. PS has conducted assessments at key critical infrastructure sites across the country. For example, some provincial legislatures have been assessed and it is anticipated that additional facilities of the same sub-sector will be visited. The CIRT will also be used by PS to assess key infrastructure (e.g., main sites, utilities) supporting major events. For example, the Grey Cup is an annual event hosted by the Canadian Football League (CFL) and draws spectators from across North America, including VIPs and senior government officials. In 2013, PS provided support for the 101st Grey Cup in Regina, Saskatchewan, that included conducting site assessments. PS is committed to supporting the 103rd Grey Cup and future events. In the future, PS will likely use the CIRT to support other major events by working collaboratively with national organizations, provincial/territorial governments, local governments, and first responders.

Conclusion

A strong collaboration among PS, DHS, and Argonne has led to the development of a critical infrastructure assessment tool for Canadian stakeholders. Leveraging existing information-sharing mechanisms between Canada and the United States, PS acquired comparative U.S. datasets that are essential to the dashboards. Awareness of the CIRT is growing among the Canadian critical infrastructure community; PS has already conducted a large number of assessments and many more stakeholders have already expressed interest in having an assessment conducted.

Acknowledgment

The work presented in this paper has been funded by PS, in collaboration with the DHS Infrastructure Information Collection Division under Contract No. HSHQDC-11-X-00230. For additional information, please email RRAP_PERR@ps-sp.gc.ca.

*Marie-Pierre Parenteau, Ph.D., Senior Policy Advisor, Public Safety Canada

Karen Guziel, Senior Infrastructure Analyst, Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory

Frédéric Petit, Ph.D., Principal Infrastructure Analyst, Risk and Infrastructure Science Center, Global Security Sciences Division, Argonne National Laboratory

Michael Norman, Director of the Infrastructure Information Collection Division, U.S. Department of Homeland Security

❖

Building Public Private Cooperation in Cyber Security

by Eric Luiijf MSc

As part of the Building Public Private Cooperation in Cyber Security session—part of the security track—at the fourth Global Conference on CyberSpace (GCCS 2015) three deliverables were developed: "From Awareness to Action: Bridging the Gaps in 10 Steps", "Sharing Cyber Security Information" and "Cyber Security of Industrial Control Systems (ICS)".

Global Conference on CyberSpace

GCCS2015 took place in The Hague, The Netherlands on April 16-17 2015. More than 1600 governmental, private sector and civil society representatives from 100+ nations gathered together to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behavior in cyberspace. The Cyber Security track included a session on Building Public Private Cooperation in Cyber Security. In support of that topic, a set of deliverables was developed and handed over to the international community. The Netherlands Organisation for Applied Scientific Research TNO was responsible for developing three of the deliverables which will be described below.

Towards Action

The first deliverable "From Awareness to Action: Bridging the Gaps in 10 Steps" is an interactive webpage. It is the result of the cyber security debates which take place at both the Board Level and the government policy levels at the earlier The Grand conferences (Amsterdam 2013, Rotterdam 2014), the MERIDIAN conference, and the meetings of the 'Risk and Responsibility in a Hyperconnected World' working group of the World Economic Forum (WEF). This deliverable is a stepping stone for the 2016 cyber security activities by the Dutch EU Presidency.

Sharing Cyber Security Information

The second deliverable "Sharing Cyber Security Information" reflects the good practice and lessons learned stemming from the Dutch public-private participation approach. Moreover, knowledge collected about many international experiences made its way into the booklet. Contributions by the Meridian CIIP community were included.

As the threat landscape is continuously changing, the sharing of cyber security-related information between organizations—whether in a critical sector or cross-sector, both nationally and internationally—is widely perceived as an effective measure in support of managing the security challenges. Information sharing, however, is not an easy topic as it comes with many facets. The booklet aims to support the cyber security and resilience governance. Its aim is to assist public and private policy-makers, middle management, researchers, and cyber security practitioners, and to steer you away from pitfalls.

(Continued on Page 12)

(Continued from Page 11)

Cyber Security of Industrial Control Systems

The third deliverable is a booklet on "Cyber Security of Industrial Control Systems (ICS)." The document was developed with support by the Meridian community as well as several associations and private organizations. Crucial processes in most critical infrastructures, and many other organizations rely on the correct and undisturbed functioning of Industrial Control Systems (ICS). A failure of ICS may both cause critical services to fail and may result in safety risk to people and or the environment. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organizations which use ICS.

The good practice document first and foremost provides private- and public-sector executives with an Executive Summary outlining the ICS risk and challenges. The document appeals to the executive leadership of organizations to address the clear and present cyber security danger to their organizations and our societies as a whole. Underpinning the Executive Summary, the good practice document provides governmental policy-makers, technical managers, ICS suppliers, and others involved in the ICS domain with background and security awareness information about the cyber security challenges for ICS. Moreover, the document provides a perspective for action and pointers to seventy relevant resources.

As part of the outreach, one may distribute both good practice documents.

References

From Awareness to Action: Bridging the Gaps in 10 Steps: https://zoom.frontwise.com/public/4/towards-gccs2015#
Sharing Cyber Security Information: http://www.tno.nl/infosharing
Cyber Security of Industrial Control Systems: http://www.tno.nl/ICS-security

*Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. Since 2000 he contributed to many national and EU projects in the field on Critical (Information) Infrastructure Protection, both at the technical and policy levels. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism and warfare, C(I)IP, process control security, and cyber security. He has been interviewed many times by press, radio and TV on these topics. Contact information: eric.luiijf@tno.nl .

Geo-Strategic Importance of the Caspian Sea

by Tehreem Saifey

The Caspian Sea is a landlocked body of water between Asia and Europe. Five coastal countries surround the Caspian: Russia to the north, Iran to the south, Kazakhstan and Turkmenistan to the east, and Azerbaijan to the west.[1] Rivers from the sea also discharge into Georgia, Armenia, and Turkey. The Caspian region holds enormous economic, political, and geographical importance for the world.

The geo-strategic importance of the Caspian lies in its location and abundance of oil and natural gas resources. The sea contains large volumes of oil and natural gas reserves both in offshore deposits and in onshore fields. According to a data analysis report by the Energy Information Administration (EIA), the Caspian basins area produced an average of 2.6 million barrels per day of crude oil in 2012, around 3.4 percent of world supply, with just over a third of that coming from offshore fields.[2] It is estimated that the Caspian contains 48 billion barrels of oil and 8.7 trillion cubic meters of gas in proven or probable reserves.[3]

The legal status of the Caspian area is problematic due to the lack of international agreement on defining the body of water either as a 'sea' or 'lake'. Different international laws could be applied in each case. Currently, there is no set legal definition for the Caspian because the coastal states must unanimously agree on a definition.[4] Hence, despite the fact that all Caspian states are major energy producers, most of the offshore oil and natural gas resources in the Caspian Sea remain untapped due to territorial and maritime disputes among the five bordering states.

Europe has special interests in the

(Continued on Page 14)

[1] Jan H. Kalicki, "Caspian Energy at The Crossroads," *Foreign Affairs 80*, no. 5 (Sep./Oct. 2001) https://www.foreignaffairs.com/articles/russia-fsu/2001-09-01/caspian-energy-crossroads.
[2] U.S. Energy Information Administration (EIA), *Overview of Oil and Natural Gas in the Caspian Sea Region*, (Last updated August 26, 2013), 2-25, available at http://www.eia.gov/beta/international/analysis_includes/regions_of_interest/Caspian_Sea/caspian_sea.pdf.
[3] "The Strategic Importance of the Caspian Sea," *Stratfor Global Intelligence* video, 1:45, May 19, 2014, https://www.stratfor.com/video/strategic-importance-caspian-sea.
[4] U.S. EIA, *Overview of Oil and Natural Gas in the Caspian Sea Region*, 4.

(Continued from Page 13)

Caspian region, mainly for its own growing energy needs. An important secondary interest is to secure the transport of gas from Turkmenistan to Turkey via Azerbaijan and on to the heart of the European market. This trans-Caspian exploitation of energy and its shipment via the strategic Southern Corridor route is meant to send a clear message to Russia and Iran to stop impeding EU-sponsored projects in the region since both countries vehemently oppose such moves. This has created a tense geopolitical rivalry in the region, with competition among nations to control and exploit the energy reserves in the Caspian. Here, roles played by powerful external actors such as the United States, China, and Russia remain critical but internal players are equally important in maneuvering this great power competition of energy politics.

Geology. According to the United Nations Global International Waters Assessment (GIWA), the Caspian Sea is the world's largest inland water body with 3,300 miles of coastline and contains more than 40 percent of the world's inland waters.[5] The Greater Caspian encompasses five different geological basins with different basin history, rock age and type, and hydrocarbon types and reserves.[6] These basins are:

- South Caspian Basin. The South Caspian basin occupies the area of Azerbaijan, western Turkmenistan, and part of Iran. The Northern Caspian basin is separated from the South Caspian basin by the Absheron sill, and is shallow with an average depth of 10 m.[7] Water depth is greater in the Southern part of the Caspian Sea.

- North Caspian Basin. The North Caspian basin is located on the southeastern margin of the Russian Plate and extends to the northern coast of the Caspian Sea. Approximately, two-thirds of the basin is located on the Territory of Kazakhstan; the rest remains territory of the Russian Federation. Technical difficulties such as very shallow waters and the coastal transitional environment have made exploration projects difficult in the past.[8]

- North Ustyurt Basin. The North Ustyurt basin is located on the territory of Kazakhstan and Uzbekistan and occupies 240,000 sq. km. It is located south of the North Caspian basin.

- Mangyshlak Basin. The Mangyshlak basin lies almost entirely within the territory of Kazakhstan with a small part extending into Uzbekistan. The Mangyshlak Shelf separates the northern basin from the middle basin. This basin makes up about 38 percent of the surface area.[9]

(Continued on Page 15)

[5] United Nations Environment Programme, *Global International Waters Assessment: Caspian Sea*, GIWA Regional Assessment 23, (Kalmar: 2006), 14.
[6] Yelena Kalyuzhnova et al., *Energy in the Caspian Region: Present and Future* (New York: Palgrave, 2002), 13-22.
[7] Kalyuzhnova l, *Energy in the Caspian Region*, 14.
[8] Ibid.
[9] U.S. EIA, *Overview of Oil and Natural Gas in the Caspian Sea Region*, 3.

(Continued from Page 14)

• Amu-Darya Basin. The Amu Darya basin extends over an area of 370,000 sq. km of Eastern Turkmenistan and western Uzbekistan. Another 57,000 sq. km is located in the neighboring countries, particularly, northern Afghanistan. The Amu Darya basin is positioned within the Turan plate, a feature that extends into the Caspian Sea and farther west into Europe and is known as the Scythian platform. On the north, the basin is connected with the West Siberian platform through the Turgay depression. The Amu Darya basin is gas prone.[10]

History. The history of oil and gas in Central Asia is very old. Almost a century ago, Baku was the hub of great commercial and entrepreneurial activity. Daniel Yergin, an oil historian and energy consultant, discusses in his book, The Quest, that in the early 1990's, the development of the Caspian oil and natural gas resources was intricately entangled with geopolitics and the ambitions of nations.[11] In many ways, it helped establish the way the new world looked and operated after the end of the Cold War. In a historic turn of the wheel, with the collapse of the Soviet Union, the newly independent states diverged in their approach to managing the oil and natural gas sectors of their countries, ranging between private ownership and full state control.[12] The results redrew the map of world oil and gas.

"The Deal of the Century." In1994, a BP-led landmark deal was signed by ten oil companies representing six nations including Azerbaijan International Operating Company (AIOC) plus the State Oil Company of Azerbaijan Republic (SOCAR) in Baku.[13] As a result, the Caspian Sea regained the world's attention. There was an agreement to develop Azerbaijan's offshore reserves when the huge Azeri-Chirag-Guneshli (ACG) field was discovered. Since then, Caspian fields have attracted huge inflows of investment into major projects such as Kazakhstan's Kashagan field.

Pipeline. One of the major challenges faced by the Caspian oil and natural gas extraction is transportation. How to get the oil and gas out to the world markets? In the nineteenth century, it could be shipped through railway tank cars, but this became an unsatisfactory and limited option moving forward. As Yergin maintains in The Quest, the only obvious alternative was a pipeline.[14]

Major Pipeline Routes in the Caspian Region

"Pipeline projects are critical not just for energy security but also for economic development." - Natig Aliyev, Minister of Energy of the Republic of Azerbaijan, April 15, 2015[15]

Caspian oil and natural gas fields are located quite far from export markets. They require expensive and highly technical export infrastructure to move oil and gas to domestic and western markets.In the Soviet era, oil and gas exports tend to rely on old pipeline networks. After the dissolution of the Soviet Union, each state negotiated export routes based on its geographic location. Some countries cooperated and developed joint export capacity, while others created their own export routes.

Landlocked Countries. Historically, pipeline transportation carries exceptional importance for landlocked countries. The United Nations has been discussing the issue of about 30 landlocked countries for years. Majority of these countries are either less developed countries or economies in transition. The disadvantage is that they have to depend upon the transit countries to have access to the sea and international market.[16] The political and social stability of the transit countries pose geopolitical risks and challenges—critical considerations for

(Continued on Page 16)

[10] Kalyuzhnova, *Energy in the Caspian Region*, 22-23.
[11] Daniel Yergin, *The Quest: Energy, Security, And The Remaking of The Modern World* (New York: Penguin, 2011), 43-44.
[12] U.S. EIA, *Overview of Oil and Natural Gas in the Caspian Sea Region*, 4.
[13] Yergin, *The Quest*, 54.
[14] Ibid., 55.
[15] "The Caspian: Energy Outlooks," *Caspian Energy News Agency*, April 10, 2015.
[16] Tatsuo Masuda, "Security of Energy Supply and the Geopolitics of Oil and Gas Pipelines," *European Review of Energy Markets 2*, no. 2 (2007): 32.

(Continued from Page 15)

the producer countries as they craft their energy policies and solutions. As it is said, it is not only the oil but also the political message that flows through a pipeline.

"Pipelines mean political leverage." - Frank A. Verrastro, the Center for Strategic and International Studies[17]

Pipelines Security in the Caspian Region

"Pipelines play a critical role in an age of increased tightness in energy markets, terrorist threats to energy infrastructure, and political use of energy resources." - Anne Korin, the Institute for the Analysis of Global Security[18]

One of the drawbacks of pipelines is that they are easy targets of terrorist attacks and other threats. These threats include physical attacks on pipelines (Iraq, Pakistan), cyber attacks (Turkey, Rafahiye Gas Pipeline incident), or could be a result of a natural disaster like an earthquake (Iran). Countries where pipelines are developed underground are highly vulnerable if they are passing seismically active countries such as Iran or Colombia.

Conclusion and Future Outlook. In this article, the main focus was on the historical and geo-strategic importance of the Caspian region with technical aspects of Caspian export routes and pipelines. Next month, I will continue with an analytical and investigative look at the politics of energy security in the Caspian region.

I will investigate whether the research and policy analyses regarding the challenges to energy security in the Caspian region are headed in the right direction or are more like the Chinese saying, "Big noise upstairs. No one coming down."[19]

Below are the main pipelines with

(Continued on Page 17)

[17] Jad Mouawad, "The Pipes Carry Clout With the Oil," *The New York Times*, May 14, 2006, http://www.nytimes.com/2006/05/14/weekinreview/14mouawad.html?_r=0.

[18] Mouawad, "The Pipes Carry Clout With the Oil."

[19] Jan Kalicki and Brenda Shaffer, "Ahtisaari Symposium: The New Geopolitics of European Energy," *Wilson Center*, May 5, 2014, available at http://www.wilsoncenter.org/sites/default/files/Energy%20Geopolitics%20Transcript_formatted.pdf.

(Continued from Page 16)

their transit routes to Europe, South Asia and East Asia markets.

*Tehreem Saifey has a Master's in Politics from the George Washington University. She is currently finishing a Master of Public Policy degree at George Mason School of Policy, Government, and International Affairs and is a Graduate Research Assistant at the Center for Infrastructure Protection and Homeland Security.❖

Major Caspian oil and natural gas export routes

Destination	Pipeline	Status	Content	Estimated capacity	Transit route (origin-destination)	Major source fields	Owner
To European markets							
	Baku-Tbilisi-Ceyhan(BTC)	Operating	Crude oil	1,000,000 bbl/d	Kazakhstan-Azerbaijan-Georgia-Turkey	ACG, Shah Deniz, Tengiz	BTC Pipeline Co.
	Caspian Pipeline Consortium (CPC)	Operating	Crude oil	684,000 bbl/d	Kazakhstan-Russia	Tengiz	Transneft, Chevron Caspian Pipeline Consortium, LukArco, ExxonMobil, Rosneft/Shell, Agip, Oryx, BG, KazMunaiGas, BP
	Uzen-Atyrau-Samara	Operating	Crude oil	600,000 bbl/d	Kazakhstan-Russia	Tengiz	Transneft
	Baku-Novorossiysk (Northern Route Export Pipeline)	Operating	Crude oil	100,000 bbl/d	Azerbaijan-Russia	Sangachal	Transneft
	Central Asia Center gas pipeline system (CAC)	Operating	Natural Gas	eastern branch: 2,200 Bcf western branch: 120 Bcf	Turkmenistan-Uzbekistan-Kazakhstan-Russia	Dauletabad	Gazprom, Turkmengaz, Uzbekneftegas, KazMunaiGas
	Baku-Tbilisi-Erzurum (BTE, South Caucasus Pipeline)	Operating	Natural Gas	280 Bcf	Azerbaijan-Georgia-Turkey	Shah Deniz	BP, Statoil, SOCAR, LUKOil,Total, Naftiran Intertrade, TPAO
	Kazakhstan Caspian Transportation System (KCTS)	Proposed	Crude oil	init. 300,000 bbl/d expand to 800,000 bbl/d	Kazakhstan-Azerbaijan	Tengiz	Gazprom, Turkmengaz,Uzbektransgaz

GEORGE MASON UNIVERSITY | Executive MBA

Critical Infrastructure Protection and Management

Meeting an urgent need to prepare leaders to safeguard industries vital to U.S. national security

This innovative new EMBA track is not found at any other accredited university in the country. Offered in partnership with Mason's Center for Critical Infrastructure Protection and Homeland Security, the curriculum answers an impassioned call to develop knowledgeable and visionary executives who can lead the effort to protect our vital resources.

Program at a Glance

- 20-month program with no career interruption
- Program offered in-class or fully online
- Domestic residencies highlighting contemporary infrastructure business issues
- Emphasis on risk analysis and management, systems analysis, and cyber security

Cooperation and communication are fundamental to effective national security; no single level or department of government has total jurisdiction over infrastructure protection and its complexities. The Critical Infrastructure Protection and Management track in the EMBA program will cultivate skills that emphasize business efficiency through interagency coordination.

The courses are oriented to strategy, policy and leadership for those who will lead critical infrastructure security efforts.

"Business leadership is vital to homeland and national security. Today, over 85 percent of critical infrastructureassets are in the private sector. The Executive MBA with concentration in Critical Infrastructure Protection and Management prepares students to be innovative and creative professionals empowered to secure vital infrastructure and enhance resilience."

–Mark Troutman
Director, Center for Intrastructure Protection

A 2013 Presidential Policy Directive made clear the pressing need to strengthen and maintain secure and resilient critical infrastructure within 16 high-risk sectors, including communications, energy, health care, transportation and critical manufacturing.

"Our goal is to fully prepare the individuals who will lead our country's efforts to secure assets, systems and networks that underpin American society."

–Paige Wolf
EMBA Director

Learn More

Join us at our next Executive MBA information session on June 4, 2015 at 6 p.m. at George Mason University's Arlington Campus. Register at

business.gmu.edu/join-us