VOL 1, ISSUE 7 **July 2018**

EDITOR

Dr. Robyn Fiori

IR^3 FEATURE ARTICLES

The Infrastructure Resilience Research Group (IR^{2}G), **Office of the Dean, Faculty of Engineering and Design, Carleton University and The Editors of the *"Infrastructure Resilience Risk Reporter (IR^3)"* make no representations or warranties whatsoever as to the accuracy, completeness or suitability for any purpose of the Content. Any opinions and views expressed in this online journal are the opinions and views of the authors, and are not the views of or endorsed by *IR^{2}G* or the Office of the Dean. The accuracy of the content should not be relied upon and should be independently verified with primary sources of information. *IR^{2}G* or the Office of the Dean shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to, or arising out of the use of the content.**

The Infrastructure Resilience Risk Reporter (IR^3) may occasionally receive unsolicited features and materials, including letters to the editor; we reserve the right to use, reproduce, publish, re-publish, store and archive such submissions, in whole or in part, in any form or medium whatsoever, without compensation of any sort. IR^3 is not responsible for unsolicited manuscripts and photographic material.

Editorial Corner

Dr. Robyn Fiori

About the Editor

Dr. Robyn Fiori is a research scientist for the Canadian Hazards Information Service of Natural Resources Canada specializing in space weather. Her research is applied to the development and improvement of space weather tools and forecasts to be used by operators of critical infrastructures and technologies in Canada. As well, it has been published in numerous peer reviewed scientific journals, including the Journal of Geophysical Research, the Journal of Atmospheric and Solar-Terrestrial Physics, and Space Weather. Dr. Fiori received her B.Sc., M.Sc., and Ph.D., from the University of Saskatchewan, Department of Physics and Engineering Physics while studying in the Institute of Space and Atmospheric Studies.

This Issue

The seventh issue of IR^3 explores a variety of topics in infrastructure resilience, including cyber security, securing energy during disasters, and protection of resources against bomb threats.

In the article, and keynote address given on May 10th, 2018, at the 2nd International Urban Security and Resilience Conference, held in Toronto, Ontario, "*Violent Extremism: European Perspective"*, Anna Hedin Ekström shares experiences from Sweden and Spain.

Katherine Thompson, in her article, "*The Opportunities and Risks for Canada and the Cyber Security Industry"* discusses a Canadian cyber security strategy introduced in 2010 with respect to budgetary commitments made in 2018 to fund a refreshed National Cyber Security Strategy. Ambitious cyber security goals require engagement and support between Government and industry leaders to ensure success.

John Agostino describes microgrids as a means of securing energy during disasters. Super storms put excessive strain on aging power infrastructure prompting both the government and private sector to find innovative solutions to generate power. Microgrids of varying scale offer an innovative solution for providing a reliable power source.

Authors Bert von Rosen and Samuel Maach point out that the current world climate has made it necessary for government and industry to consider bomb threats in their security awareness. In their article, they seek to educate readers about explosives and the fundamentals of blast and blast related security measures for the purpose of critical infrastructure protection. They address the need for blast vulnerability assessments and the need to identify sensitive assets, and discuss crucial mitigation techniques.

The article, "*Navigating Security Assessments: Tools and Methodologies",* by Alexander St-Jacques, Dr. Felix Kwamena, and Andrew Lackey provides descriptions of the four most commonly used assessment practises: risk assessments, vulnerability assessments, security audits, and penetration testing. They examine the key differences between the methodologies, their intended outcomes, and limitations.

This issue concludes with an article on, "*Decarbonization of Heavy Industries: A Multi-Stakeholder, Multi-Disciplinary Approach to Addressing Challenges and Leveraging Opportunities.* The authors will convene a workshop of representatives from academia, industry, government, and non-governmental organizations, November 28-29, 2018, at the Fairmont Chateau Laurier Hotel, Ottawa, Ontario. The workshop will wrap up with the Dean's Lecture on the evening of November 29, 2018,

Next Issue:

Issue 8 will focus on the use of UAVs for infrastructure resilience. We invite authors to contribute articles relating to their experience in the field of infrastructure resilience. Draft articles of 2500-4000 words are requested by July 30, 2018. You may not have much time or experience in writing 'academic' articles, but IR^3's editorial board can provide guidance and help. Your experience is valuable and IR^3 provides an ideal environment for sharing it.

Violent Extremism: European Perspective

2nd International Urban Security and Resilience Conference-Workshop

Toronto, Ontario, May 8-10, 2018

Keynote Address, Day 3

*Anna Hedin Ekström**

Senior Adviser and Expert on Violent Extremism, Crisis Management and Security

Email: anna.ekstrom@sakeranalys.se

Abstract

During the 2nd International Urban Security and Resilience Conference in Toronto, I had the great pleasure of giving a keynote address and moderating a European panel on violent extremism. The aim of the panel was to present different European perspectives on preventive work and to share experiences from Sweden and Barcelona. Sadly enough, just weeks before, Toronto was hit by an attack by a truck in the city center – adding another city to the unfortunate list of cities that have been hit by such an attack. Stockholm and Barcelona gave their condolences and shared their own experiences.

Violent extremism as we know it has somehow changed its shape and form. New collaborations between organizations and movements have become a new reality in most countries in the western world. White power movements are inspired by Daesh's narratives for recruitment, gangs and persons who have fought for Daesh in Syria and Iraq commit crimes together, football hooligans and activists from the violent left-wing movement one day cheer together and the next day confront each other. Organized crime benefits from the experiences of foreign fighters and activists from left-wing and right- wing movements all demonstrate against Israel, sometimes together with persons from radical Islamist movements. This change in scenery is not unique to Sweden. Sweden, however, sometimes serves as a micro-cosmo for study of the evolution of violent extremism.

For the last 4-5 years, the violent extremist scene in Sweden has changed dramatically. Right-wing, left-wing and Islamist violent movements have changed in composition, ways of expressing agendas and visibility. The movements have adapted to new circumstances and have gone from being a rather clearly defined set of different groups and organisations to a more complex and diverse multitude of actors. They sometimes cooperate, not only between politically or religiously motivated actors, but also with gangs and organized crime. The overlap, or nexus, between different movements that were once regarded as separate has become more blurred.

The democratic system is often challenged and rightfully so. A stable democracy is expected to endure challenges from various actors. The legitimacy is however sometimes challenged by other actors, networks, rouge states and ideologies. The promotion of violence for political purposes can be expressed in various ways: verbally encouraging others to carry out acts of violence; providing logistical support and funding to terrorist groups; or preparing / carrying out terrorist attacks. Violence promoting radicalisation does not necessarily lead to terrorism, but may lead to other serious acts of violence and unlawful pressure. In the case of violent extremism in Sweden, it consists primarily of three identified groups: right-wing, left-wing and Islamist extremisms. These groups have different agendas, but their activities undermine and challenge democracy in different ways. People who are actively involved in violent right-wing extremism commit and encourage others to crimes that have racist and homophobic undertones. They threaten persons with opposing political views and try to make them leave their political positions. People who are actively involved in the extremist autonomous movement harass, threaten and sometimes use violence against democratically elected representatives, civil servants and people in the right-wing extremist movement. In the summer of 2017, the Swedish security service announced an estimate of the number of persons considered to be involved in or advocates of violent extremism: 2,000 persons in the extreme violent Islamist movement, around 700 persons in the violent right-wing movement, and around 300 in the violent left-wing movement. New research shows the overlap between various movements, including football hooligans. This is also the case in Barcelona where street gangs overlap with extremists and criminals.

Regarding the white power movement, the Swedish security service has noted an increase in activities, in the spreading of propaganda, demonstrations and violent acts. Several people were recently convicted of bombing the Syndicalists' offices in Gothenburg and attempting to attack two asylum accommodation centres. The longest prison sentence handed down was five and a half (5½) years. The prosecutor specifically emphasised that bombs in the Gothenburg case were equipped with timing devices. Two of the bombers had undergone paramilitary training in Russia. The European white power movement also showed a significant interest in the demonstrations in Charlottesville in 2017, among others, Swedish activists were represented.

The violent left-wing movement has also undergone a dramatic change during the past years. The extremist left-wing scene in Europe has been rather invisible for a number of years, mainly due to convictions against a number of leading figures, but also due to a lack of shift in generations and therefore less recruitment and "new blood" into the violent prone falang. This decrease in activities is a trend that was somehow disrupted with the violent demonstrations in Hamburg during the high-level meeting in 2017 where protests against the G7 leaders led to violent confrontations between activists and the police.

Since the uprising in Syria in 2011, foreign fighters joining terrorist organizations have grown in number and impact, and Sweden is no exception. According to the International Centre for Counter-terrorism (ICCT: https://icct.nl/topic/foreign-fighters/), Sweden is among the countries with the highest number of foreign fighters per capita, only second to Belgium and Austria. According to the Swedish security service (SÄPO), the number of people travelling to conflict zones has decreased dramatically during the past couple of years, for various reasons – one is change in legislation. From April 1, 2016, it constitutes a crime to travel to join a terrorist movement. Another reason is the changed situation in Syria, Iraq, and the Islamic State's shrinking influence in the region. A third reason is that the situation in Syria is now known to the world. It is no longer possible to recruit in the same way as before, to decoy with promises of a better future and prosperity. However, it is not only the persons travelling who may pose a threat to societal security. A person who chooses to stay in Sweden can also be encouraged to act where they are, as is the case in many European cities. This is also what happened in Stockholm, on Friday, April 7, when one person hijacked a truck during the early afternoon in the city centre of Stockholm, killing five (5) persons.

The estimated number of violent extremists in Sweden has increased dramatically. The Swedish security service stated in the summer of 2017 that the number of violent extremists in the violent Islamist milieu is estimated to be around 2,000 persons (The security service also said the left-wing and right-wing together constitutes around 1,000 persons – the majority in the right-wing movement). Not all of them have the intention to commit violent acts, nor do they have the capabilities, but they adhere to a violent agenda – 10 years ago the equivalent number was around 200 persons. In the new estimate, both persons who have a violent agenda, willingness and capability to conduct violent acts, and persons who are mainly supporters with no intention or capability to follow through with violent actions, are included.

The development in Sweden is not specific, but it is part of an international trend. The travelling to Syria and/or Iraq has almost completely come to a halt, due to the situation on ground and legislation – among other factors. Daesh is instead encouraging persons to commit crimes in other countries with weapons that are easy to find and use, such as knives and trucks. The violent right-wing movement is using new ways to attract supporters, and is in some ways inspired by Daesh in their rhetorics. The violent left-wing movement is finding new fuel to their commitment, by the rise of right-wing extremism, the political polarization, which is to be seen both on a national level, such as in Sweden, and also on an international level as with the riots in Hamburg 2017. This calls for an understanding of how these milieus operate – both within the separate forums, between violent prone and antagonistic groups. Violent threats to society are one of the main challenges of our time, where perpetrators come from a range of ideological and criminal milieus, and where distinctly different violent groups sometimes act on their own, sometimes in collaboration in a way that has not been seen before. Recent studies suggest the nexus between crime and terror is the new reality for many democratic societies. Experiences from a number of countries show that organized groups and extremism are not divided into different silos. Individuals cooperate and move between antagonistic milieus, they collaborate and share experiences and influence each other. There is a need for research to take this into account and share experiences between countries. The Canadian and Swedish collaboration has proven fruitful for many years. The countries share many similarities and experiences which have created and increased knowledge in many areas throughout the years. The excellent initiative and organization of the 2nd International Urban Resilience and Security Conference is another way of exploring new possible ways for collaboration and information sharing – giving energy to new networks that will bestow long after the conference.

About the Author

Anna Ekström giving keynote address

***Anna Hedin Ekström** moderated the panel that consisted of Superintendent Gunnar Appelgren at the Swedish police, Amir Rostami, Ph. D., at the Institute for future studies (Sweden) and Inspector Lluís Paradelli Fernàndez, Head of the Central Analysis Unit Intelligence and Counterterrorism Office in Barcelona.*

The Opportunities and Risks for Canada and the Cyber Security Industry

*Katherine Thompson**
Principal, Human Firewall Solutions
Chair and Founder of CATA Cyber Council
Email: kthompson@cata.ca

On February 27th of this year, the Liberal government announced it would be spending $507M over 5 years on a refreshed National Cyber Security Strategy. Among disclosed priorities a significant investment of funds was allocated to upgrade the governments aging technology to defend against the potentially devastating impact of attacks on critical infrastructure.

The original cyber security strategy was introduced in 2010. At that time, the government identified 10 areas of critical infrastructure which include the following:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Information and communication technology
- Health
- Water
- Safety
- Manufacturing

ARE WE READY?

In March of this year, shortly after the initial details of the strategy were released, Public Safety Minister Ralph Goodale commented that Canada was in "pretty good shape" to defend against a cyber attack on infrastructure, but also "needs to get better." However, not everyone agrees with that summation. Melissa Hathway, President of Hathway Global Strategies and former cyber security advisor to both the Obama and Bush administrations recently commented that she believed critical infrastructure and services in Canada were vulnerable and believed that a detailed risk assessment would uncover the alarming extent of risk currently facing Canada.

IT TAKES A VILLAGE

While the strategy was long awaited, there were no quick fixes with the announcement. In fact, the two years of consultations and internal review that went into building the strategy was the easy part. Now the government is faced with having to find effective and efficient ways to deliver on the priorities. To do this, the government should and must engage others who have the skills, expertise and tenacity needed to keep pace with a threat landscape that is increasingly pervasive and fluid.

The area of Public-Private Partnerships is not something the government has done overly well over the years, but it is one that this government acknowledges is needed. This is also a government from both the political and bureaucratic perspective that is more open and receptive to working closely with multiple stakeholders. The challenge is and will remain with finding a balance between the government's cautious and calculated approach to large-scale matters, with the need for progress, and the "time is money" mantra that the private sector aligns with.

BUILDING A SUSTAINABLE ECOSYSTEM

On a daily basis, there are discussions across media surrounding the growing and global labour shortage in the cyber security industry. In 2017, the number of unfilled cyber security jobs in the U.S. rose by 250%, exceeding 350,000 vacancies. In Canada, we are faced with a lack of national data to quantify the gap, yet there is no doubt when you speak with employers of these skills; the market is starved and becoming increasingly competitive both for those within and outside of Canada looking for expertise.

In 2017, CATA Cyber announced its national mandate. This came after almost 1.5 years of speaking with a cross section of public and private sector leaders to understand the areas of interest, opportunity, growth and risk. The consistent message heard, no matter what the industry or organizational size, was that finding and retaining cyber security talent was becoming very difficult. When we sat down to formulate the mandate, there was immediate and unanimous agreement that the development and delivery of a skilled labour market strategy was critical.

In late 2017, both Scotiabank and TD Bank announced that they were investing millions of dollars in Israel to develop cyber security innovation for the banking sector. TD noted in its media that they were finding it increasingly difficult to compete with Silicon Valley and others who were willing to pay staggering sums to recruit highly skilled cyber security expertise and that in Israel finding skilled talent was much easier. So in short, a country of 8.4 million people had more skilled cyber security labour than a continent of 340 million.

A labour strategy should take the following into consideration:

- Engagement with key stakeholders from government, industry and academia.
- Strategies for the "Now": apprenticeship, professional development programs.
- Strategies for the "Future": industry and government to engage and support the development of academic programs that speak to the current and emerging threat landscape.
- Engage them at a young age: programs to engage elementary and secondary school students are critical moving forward.
- Consider the often overlooked workforce: more and more programs are emerging where those with disabilities, military veterans and those re-entering the workforce are being trained and offered apprenticeship opportunities in cyber security with impressive results.

SHARING IN SILOS

The Canadian banking industry is one of the world's most respected and resilient financial services sectors in the world. In terms of cyber security posture and maturity, many would argue that it is also the most refined and sophisticated. Canadian banks spend millions of dollars each year on the protection of banking technology, infrastructure and personal information.

What the banking industry doesn't do is readily share just what and how they achieve this sophisticated security. Now, from a purely business perspective, I get it. No one wants to hear the institution they bank with and share their personal information with is constantly under attack from cyber criminals. It's certainly not good for consumer confidence and undermines a system that has become increasingly reliant on online technologies to conduct daily business.

The problem this creates is a siloed and shut off approach to sharing information and best practices. Many less mature sectors, such as healthcare and manufacturing, could greatly benefit from key learnings of the banking sector. This could avoid costly investments and security missteps that lead to disruptions in key services and the loss of personal information.

A more open and collaborative approach to information sharing will greatly benefit critical infrastructure going forward, but this will not happen unless we have a willingness to join the discussion.

Innovation Priority – Canadian Made

The decision Scotiabank and TD Bank made was predicated on two priorities: a skilled labour market and deep success in cyber security innovation. Both are well-deserved and even better marketed. Israeli-based companies currently control over 25% of global spending of cyber security products and services. The Israeli government has been extremely successful in integrating their mandatory military service programs into a sandbox for developing cutting edge innovation and delivering it to the global marketplace. They are also extremely efficient in creating public-private partnerships that benefit all involved.

For the past seven (7) months, Sir Terry Matthews (https://en.wikipedia.org/wiki/Terry_Matthews) has generously hosted industry dinners at his hotel, the Brookstreet in Kanata, Ontario. At the most recent dinner, Terry had just returned from a 3.5 week international business trip that took him to nine (9) countries. He commented that every country he visited was talking about cyber security and it was a red hot topic, yet no one was talking about what was going on in Canada. His summary for this was simple: ”we need to change this”.

Now, I don't disagree or blame TD or Scotiabank for their decision to invest in Israel, but I will argue that cyber security innovation in Israel is no better than what can be found in Canada. In fact, our advancements in others areas, such as quantum computing, artificial intelligence and blockchain only further benefit and differentiate what Canadian firms can bring to the global cyber security marketplace. Where we need to take a page from the Israelis is in the ways they support, grow and market their expertise worldwide.

While the government has acknowledged changes are needed in their procurement processes to allow Canadian firms better opportunities to compete and win government business, the private sector has a role to play in this as well. While I won't go as far as pleading the case for "Canada First", I will say Canadian-led firms need a better position at the starting gate.

Optimism and Action

While the threat to government, critical infrastructure and Canadians resulting from a cyber attack is significant and real, there is a strong argument to be made for optimism. Another mandate item of CATA Cyber is "economic prosperity for Canada through the development of the cyber security industry." A skilled cyber security labour force means jobs, industry and infrastructure security, and global recognition of Canada as a safe place to do business.
During the discussions surrounding Innovation, Science and Economic Development (ISED) Supercluster program, CATA Cyber recommended that no matter what projects were chosen, Security by Design should be a fundamental and foundational component of every technology innovation. If there is one thing to be learned from the Internet of Things (IoT), it is that security after-the-fact is costly, difficult to remedy and creates significant and widespread risk. The time for definitive action is now. Government and industry leaders must find ways to engage, support and collaborate if we are going to ensure the safety of our infrastructure and Canadians in the years to come.

About the Author

****Katherine Thompson** has taken a leading role in helping Canadians understand the risks and rewards associated with the digital economy. As Principal of Human Firewall Solutions, a Toronto-based market advisory and development firm and Founder-Chair of the Canadian Advanced Technology Alliance (CATA) Cyber Council, Katherine leads a national team of globally recognized cyber security experts focused on* *helping Canadian organizations better understand, secure and capitalize in the global digital marketplace.*

Katherine sits as board member of the CATA Public Safety Advisory Board and Cyber Titan, a collaborative with the US Air Force's Cyber Patriot program that seeks to engage young Canadians in a career in cyber security and other science, technology, engineering and math areas.

Microgrids Secure Energy During Disasters: An Emergency Management Perspective

*John A. Agostino**
Vice President, Adjusters International / Tidal Basin
Email: jagostino@aidrc.com

Over the past twenty years our experiences with super storms continues to increase. As our power infrastructure continues to age, its ability to function during these significant disasters continues to erode. Leaders in both government and the private sector continue to search for solutions that will provide sustained and resilient power sources during these events. More importantly, critical services cannot remain off-line waiting for major power sources to bring the power grid back to life. As part of the solution to the impacts of these super storms, we started taking a renewed and invigorated look at microgrids. The following article demonstrates the impacts and effects of disasters on our electric power sources, and how microgrids can become our sustained source of electric power.

The life of an emergency manager revolves around the four axioms of Readiness, Response, Recovery, and Mitigation. Now, in recent years, emergency managers find themselves dealing with the concept of resilience. As our natural disasters continue to increase in frequency and magnitude, the discussion continues as where to best place limited resources to address the essential requirements of each of these axioms.

We certainly know the need to prepare ourselves for the continued onslaught of natural disasters. Hurricanes, winter storms, forest fires, terrorism, and cyber attacks devastate our critical infrastructure and systems. In the past forty decades, natural disasters alone more than doubled. Yet, we continue to address these circumstances with the same inefficient rebuilt philosophy.

Let us briefly address the following Laws of Disaster Risk: Disaster risk grows exponentially with hazard risk; Disaster risk grows exponentially with urban density, even when hazard risk remains constant; Disaster risk is inversely proportional to resiliency capability; and emergency capacity required is inversely proportional to resiliency capability. The overwhelming driving forces behind these laws fall to two consequences, increase in the number and intensity of disasters, along with the urbanization of our society.[1]

If we intend to address these risks, then we must find a way to build our systems and infrastructure, with resiliency as the priority. However, meeting this goal seems more difficult than identifying the initiatives so critical to becoming resilient. One can argue that climate change continues to affect the number and intensity of our natural disaster storms. As that debate continues, we face the grim reality of super storms like Katrina and Sandy.

Most recently, the three successive storms of Harvey, Irma and Maria left major metropolitan areas devastated. Today, the Island of Puerto Rico still struggles to provide basic services to its citizenry.

The urbanization of our society greatly expands the potential for large populations becoming affected by a disaster. As we continue to quickly build infrastructure, such as housing, to meet the needs of our sprawling cities, the level of resilience in that planning process remains almost non-existent. For the most part, building quickly and cost effectively continues to dominate the industry.

If we follow the guidance of the U.S. Federal Emergency Management Agency (FEMA), citizens

[1] Resilience: The Ultimate Sustainability, Aris Papadopoulos, 2016

need to plan to sustain themselves from anywhere for 72 to 96 hours. So, let us examine some natural and man-made disasters that affected the Northeast United States and Canada. We all know about the super storms that devastated the East Coast, but what happens if we look at disasters that allowed the population to continue to reside in their homes.

In October 1987, the earliest snowstorm on record struck the Northeast United States. Up to a foot of heavy wet snow blanketed the Northeastern States. As the summer foliage remained on most of the trees, the heavy wet snow caused the trees to snap and break. As the trees fell on the power lines, it caused a massive power outage. The outcome of this unanticipated event left 317,000 citizens without power. Many people waited days to get their power restored. Without electricity, and generators hard to find, many people found themselves reverting to a pioneer spirit: reading by candlelight, putting food from the refrigerators into snowbanks, and cooking in fireplaces.[2]

On January 4, 1998, one of the worst ice storms in history struck both Northeastern Canada and the United States. This weather event left 4.7 million Canadians and 500,000 U.S. citizens without power. In fact, weeks after the ice storm, severely-effected populations waited for power restoration. One of the most affected industries was agriculture; dairy farmers, suffered significant losses. As an industry heavily reliable on mechanized operations, the loss of power paralyzed their milk producing capability. Approximately 5,500 farmers in Ontario and Quebec discarded 13.5 million litres of milk for loss revenue of $7.8 million. In New York State, then Governor Pataki, ordered 185 generators from across the country to help avert this crisis. Even with this effort, many of the cows became sick, produced less milk, or was useless. New York State farmers lost $4 million, dumping milk they could not properly refrigerate.[3] The recovery from this one event cost $3 billion to Canada and $1.4 billion to the U.S. Perhaps more importantly, 28 Canadians and 16 U.S. residences lost their lives.[4] This event caused such disruption in Canada, it brought about the largest mobilization of Canadian military forces since the Korean War to assist in the response and recovery operations.

Almost two years after the 911 Attacks on the World Trade Center Buildings, a great portion of the Northeast U.S. and Canada experienced another major power outage. Only this time a natural disaster did not cause the widespread power outage. On August 14, 2003, 50 million people found themselves in a complete blackout. Parts of Ohio, Michigan, New York, New Jersey, Pennsylvania, Massachusetts, Connecticut, Vermont, and the Province of Ontario lost power. Although power restoration successfully happened for most customers within hours, some waited two days for full restoration. Ontario experienced rolling blackouts for up to two weeks due to a generation capacity shortage. This technological disaster not only cost between $4 billion to $10 billion, but left millions of people in Manhattan and New York City initially wandering around in the streets wondering if another terrorist attack took place.[5]

The Washington Post recently published an article outlining how sophisticated cyber attackers can bring down an entire power grid. The energy sector sustains more cyber attacks than any other industry. The frequency and sophistication of these attacks continue to increase. Mounting and maintaining an in-depth defense remains a high priority. The U.S. Department of Energy in its 2016 Quadrennial Report stated that a cyber attack could weaken critical infrastructure,

[2] Times Union Newspaper, Albany, NY, Paul Grondahl, October 4, 2012

[3] Weather Volume 55. January 2000, Impacts and Consequences of the Ice Storm of 1998 for the North American Northeast, Lesley-Ann Dupigny, University of Vermont

[4] Weather Channel, Chris Dolce and Jon Erdman, January 2017

[5] August 14,2003 Northeast Blackout impacts and actions and the Energy Policy of 2005, North American Electric Reliability Council, David W, Hilt, P.E.

undermine the economy, and threaten the health and safety of millions of Americans.[6]

The power sector continues to digitize the electrical system to achieve better efficiency and reliability. The Federal Energy Regulatory Commission (FERC) maintains the mission to protect power systems against cyber attacks and enforce mandatory standards to ensure the continuous supply of electricity. Under this mandate, FERC endorsed the North American Electric Reliability Corporation (NERC CIP) cyber security standards for critical infrastructure protection. A 2017 report from the U.S. Department of Energy also recommends even more data collection and urges modernizing the grid. The estimated cost for such an effort falls between $350 billion to $500 billion.[7]

We now see how natural, man-made/technological, and cyber events can cause major disruptions to the infrastructure of our power sector. The outcome of these events leaves millions of people stranded without power. Billions of dollars in revenue are lost in these events and more (billions of dollars) are needed to protect and strengthen the power infrastructure. Emergency managers and first responders struggle to respond to and recover from all these types of events. The resources needed to manage the consequences of the increased number and magnitude of these disasters remain limited. Let us not forget, as part of these critical resources needed include the ability for critical facilities to continue their essential operations. These include military installations, hospitals/healthcare facilities, fuel producing refineries, fuel delivery services, communications centers, water treatment facilities, police, fire, and emergency medical services.

As we searched for solutions, one came to the forefront. One that already exist and proved very reliable. Microgrids, with the increase in the number and magnitude of disasters, became an excellent resource and solution to investigate.

The U.S. Department of Energy defines a microgrid as a group of one or more distributed energy resources with clearly defined electrical boundaries that act as a single, controllable entity with respect to the grid and can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode.[8]

Before we review examples of microgrid success stories, let's look at their widely accepted benefits as a complement to existing grid infrastructure along with the various types of microgrids:

Autonomy: Microgrids allow generation, storage and loads to seamlessly operate in an autonomous fashion, balancing out voltage and frequency issues with recent technology advance.

Stability: Control approaches remain based on frequency droops and voltage levels at the terminal of each device, allowing the entire network to operate in a stable manner no matter whether the larger grid stays up or down.

Compatibility: Microgrids remain completely compatible with the existing centralized grid, serving as a functional unit that helps build out the existing system, helping to maximize otherwise stranded utility assets.

Flexibility: Expansion and growth rates do not need to follow any precise forecast, since lead times remain short, and build-out incrementally. Staying technology neutral, they can tap into a diverse mix of renewable and fossil fuels.

Scalability: Microgrids allow many small generation, storage and load devices in a parallel and modular manner to scale up to higher power production and/or consumption levels.

Efficiency: Energy management goals, including economic and environmental, allow for an optimization in a systematic fashion.

Economics: Droop frequency control techniques allow for the programming of economic decisions into standard operating protocols.

[6] The Washington Post, February 15, 2018, content by Siemens

[7] The Washington Post, February 15, 2018, content by Siemens

[8] U.S. Department of Energy, 2018, Microgrids at Berkley Lab

> **Peer-to-Peer Model:** Microgrids represent a new paradigm, a true peer-to-peer model that does not dictate size, scale, peer numbers or growth rates.[9]

As previously mentioned, the military identified the value in using microgrids. Fort Carson, Colorado, currently participates as one of several microgrid projects underway on U.S. Bases under the Smart Power Infrastructure Demonstration for Energy Reliability and Security program. Fort Carson supports about 14,000 residents and covers approximately 342 miles with ancillary firing ranges.

The Fort Carson Sustainability Goal Plan Energy & Water Resources Vision Statement says: In support of the Sustainability and Net Zero Installation Initiatives, the Post will sustain all facility systems from renewable sources by 2020 and reduce the potable water usage intensity by 75% from the 2001 baseline by 2020. The desired end-state: secure energy sources; reduced dependence on fossil fuels and adverse air emissions; life cycle cost effectiveness; reduce reliance on petroleum imports and vulnerability; water conversation through efficient consumption reduced wastewater effluent treatment requirements, increased water re-use and development of sustainable water solutions. Achievement of this goal supports installation and force security. [10]

To achieve the goals of the Plan, the base undertook an ambitious plan to become a net zero facility using huge PV (solar) resources, potentially over 100 MW (Mega Watts), as well as wind, ground source heat pumps, biomass, and solar water heating. The microgrid project intended to keep a group of central base facilities operating without grid power as an island in the event of grid failure.[11]

New York University (NYU), one of the largest universities in the United States, started producing power on site since the 1960s. NYU installed a large oil-fired plant in 1980. At the end of that facility's useful service life, NYU made the transition from the oil-fired technology towards a modern natural gas fired combined heat and power facility with eyes towards microgrid capabilities, better reliability, and a better control of their energy expenditures.

The upfront capital cost of the upgrade cost a significant $126 million. However, working with the New York State Dormitory, NYU arranged for tax-exempt bonding. Also, NYU tuition and fees helped provide for low-cost financing sources.

The Combined Heating and Power (CHP) system provides an output capacity on 13.4 MW (twice the capacity as the previous plant) became fully operational 2011. It supplies electricity to 22 buildings, and 37 buildings across the campus. The microgrid consists of two 5.5 MW gas turbines for producing electricity coupled with heat recovery steam generators and a 2.4 MW steam turbine. The NYU microgrid connects to Con Edison distribution grid and purchases electricity when demand becomes superior to the on-site generating capacity.

NYU microgrid can function as a stand-alone island from the distribution grid. NYU successfully tested the microgrid during Superstorm Sandy. The NYU microgrid successfully islanded from the local distribution grid and continued to provide reliable power to much of the campus.

Now with more than 12,000 solar installations in the City, they turned their attention to storage. Hurricane Sandy showed the importance of integrating distributed generation and storage into emergency and resiliency planning.

The modernization of the plant presented impressive results both economically and environmentally. NYU evaluated savings on a total energy cost at $5 million to $8 million per year. The new facility drastically reduced NYU's local emissions with an estimated 68% decrease in the Environmental Protection Agency's criteria pollutants and 23% decrease in greenhouse gas emissions. This went a long way towards the University's commitment

[9] Renewable Energy Resilience, The Microgrid Revolution, Peter Asmus, November 6, 2009

[10] Fort Carson Sustainability Goals Update FY12

[11] U.S. Department of Energy 2018, Microgrids at Berkley Lab

to the City of New York to decrease its generation gas emissions by 30%. [12]

As a direct outcome from Hurricane Sandy, New York State offered $60 million in demonstration grants to identify microgrid projects that could provide continued power during major disasters.

Hurricane Maria devastated the Island of Puerto Rico. Before the Hurricane, Puerto Rico desperately needed grid modernization. The Island's power plants average about 44 years old. Puerto Rico Electric Company (PREPA) runs most of the power plants. Prior to the disaster the PREPA filed for bankruptcy with a $9 billion debt.

As Puerto Rico needs to start from scratch, the opportunity exits to solve many of its long-term energy problems and shift to a cleaner energy source that continues to drop in price. Microgrids look like the key to building a sustainable more resilient system.

The cost of renewables compares in price to what customers already pay for electricity. A new decentralized grid would become more conducive to integrating distributed energy. This could help raise the Island's renewable energy portfolio, which currently operates at 2%, and make it more resilient to future storms.

The interest from private companies already exist. Solar companies Sonnen and Sunrun already started partnering with local non-profits to provide battery and solar supplies. Tesla proved itself as one of the most ambitious with its efforts: in late September 2017, Bloomberg reported that Tesla shipped hundreds of Powerwalls, its home batteries that can store energy from rooftop solar, to the Island. Tesla, discussed with Puerto Rico's Governor Rossello to scale up the effort by sending Powerpacks, giant battery packages equal to 16 Powerwall batteries, to bring hospitals and city centers back online.

This battery technology, when used effectively, could restore electricity to rural and isolated communities first, where they could provide electricity well ahead of when grid rebuilding would likely reach those communities.

These new microgrids could work in tandem with the fossil fuel-powered centralized electricity grid, particularly in future storms like Irma and Maria. In fact, microgrids can provide individual pockets of power that could hugely support emergency relief and communications, to light and power tools for rebuilding. The goal now becomes to create a system of microgrids, small-scale power grids that operate independently of the centralized grid that can utilize renewable energy like rooftop solar.[13]

As emergency managers evaluate methods and systems to address the mandates of readiness, response, recovery, mitigation, and *resilience*, microgrids come to the forefront. Microgrids not only directly address these mandates, but effectively minimize the risks associated with the number and increasing magnitude of disasters.

One of the concerns emergency managers always need to address falls under the heading of public education. The emergency manager wants to make sure that the local population knows how to prepare for and protect itself during a significant disaster event. Always remembering FEMA's guidance to make sure you can sustain yourself for 72 to 96 hours.

As I drive through my own small neighborhood, I realize that many of my neighbors and I experienced the negative effects of long power outages from the 1987, 1998, and even the 2008 storm. Something looks significantly different after suffering through those events. Driving past my neighbors' houses (including my residence), I now see the sun reflecting off solar panels, and generators located along side our houses. Generators that not only can provide internal residential power, but also allows for external hookups to provide outside sources access to power. In our own way, we created a neighborhood mini-grid.

[12] U.S. Department of Energy 2018, Microgrids at Berkley Lab

[13] Inside Climate News, Puerto Rico's Solar Future Takes Shape at Children's Hospital, with Tesla Batteries, Lyndsey Gilpin, October 25, 2017

About the Author

***John Agostino** is currently in the position of Vice President, Field Operations, for Adjusters International/Tidal Basin. In this position, he maintains the responsibility to deliver all-hazards emergency programs to Adjusters International/Tidal Basin's clients. This includes preparedness programs, emergency response and disaster recovery operations, hazard mitigations programs, and community resiliency initiatives. Prior to his employment with Adjusters International/Tidal Basin, he worked at the New York State Emergency Management Office, retiring after thirty years of service. Prior to his retirement he served as the Deputy Director for Administration. In this position, he served as the Chief Financial Officer for the Emergency Management Office.* *His other responsibilities included the delivery of the disaster recovery programs for New York State. In that capacity, he served as the New York State's Governor's Authorized Representative for 57 federally declared disasters by the U.S. President. While serving at New York State, he received the Federal Emergency Management Agency's highest award for Outstanding Public Service. He also serves as Vice Chair of the Board of Directors for Family and Children's Services of the Capital Region in Albany, NY. John retired as a Major from the U.S. Army. He received a B.A. Degree from Siena College, Loudonville, NY and an MBA Degree from Rensselaer Polytechnic Institute, Troy, NY.*

Blast Mitigation Considerations and Industry (Best) Practices in Critical Infrastructure Protection

*Bert von Rosen**
Head, Explosion Effects Group
Canadian Explosives Research Laboratory
Natural Resources Canada
Email: bert.vonrosen@canada.ca

Samuel Maach, Ph. D.*
Director, Canadian Explosives Research Laboratory
Natural Resources Canada
Email: Samuel.maach@canada.ca

Abstract

Historically, Canadians have always considered bombings something that occurs elsewhere in the world, e.g., the Middle East or the U.K. However, since the events of September 2001, there has been an increased awareness that North American Industry might not be as secure as had been assumed. Since then, both government and industry have realized that the bomb threat is one which they must consider. This shift in awareness has made it necessary for security professionals to educate themselves in a new discipline.

The objective of this paper is to introduce the security professional, who may not be familiar with explosives and their effects, to some of the fundamentals of blast and to some of the blast-specific security measures that they can be implemented to help protect critical infrastructure.

The Threat

Types of Explosive

From a security perspective, explosives are often divided into three categories:

- Military explosives
- Industrial explosives
- Homemade explosives (HME)

Military explosives, such as TNT, PETN and RDX were originally designed to produce very high pressures in order to shatter bomb casings and produce high-velocity, lethal fragments. These explosives tended to be powerful and stable, difficult to obtain and expensive.

Industrial explosives are generally designed to produce a lower peak pressure, but more gas than the military explosives, making them better suited for moving rock. Similar to military explosives, they are relatively stable, but unlike military explosives, they are commercially available and inexpensive.

HMEs cover a very wide range of explosives: from the very stable to the highly volatile. What they have in common is that they can be made from commonly available materials, with unsophisticated tools such as one might find at home in a kitchen; hence the name, “homemade”. In general, they tend to be less powerful than either military explosives or industrial explosives. A wide variety of HME recipes may be found on the internet.

TNT Equivalency

The concept of TNT equivalency was introduced to simplify the life of safety and security practitioners and blast engineers. Instead of designing a facility for specific explosives, designs are generally based on a quantity of TNT and then converted to other explosives using TNT equivalency. For example, if a building had been designed to resist 100 kg of TNT detonated at the property perimeter, a security practitioner could use the TNT equivalence of ANFO to determine that the building was also capable of resisting the detonation of 120 kg of ANFO at the property limit.

Means of Delivery

Another useful way of defining an explosive threat is by its means of delivery. Two of the most common definitions are:

- HEIED or hand-emplaced improvised explosive device,
- VBIED or vehicle-borne improvised explosive device.

These designations are particularly useful because they not only describe the device, but to a large extent, they also describe the means by which they will be employed and the target they will be used against.

HEIEDs are usually used to target a specific piece of equipment, and occasionally people; the Encana bombings of 2008-2009[1] are good examples of the use of HEIEDs. As a blast weapon against people, HEIEDs are a threat only within a few metres of the device. To increase the range, the attacker builds fragments into the device. As a weapon to be used against equipment, HEIEDs are typically only effective when they are in direct contact with the equipment. Stand-offs as little as 100 mm can significantly reduce the efficacy of the device.

VBIEDs are typically used against structures or against large crowds in open spaces. Notable examples of VBIEDS include the Oklahoma City bombing (1995)[2], the Oslo bombing (2011)[3] and the Kabul bombing (May 31 2017)[4]. VBIEDS are usually considered to be blast weapons, as the body of vehicles usually makes for ineffective fragments. However, it should be noted that larger parts like axels, transmissions or engines may remain intact and become extremely hazardous fragments. As blast weapons, VBIEDS tend to cause significant damage to building envelopes, i.e. outer walls and windows. The failing building envelope results in hazardous debris which may lead to injuries or fatalities.

In rare cases, when the VBIED is very large and very close to structural components of the building, or when the building is extremely weak, the building may collapse. Load-bearing unreinforced masonry buildings are particularly vulnerable to collapse.

Blast 101

The detonation of an explosive charge which is placed on or near the ground produces a blast wave which spreads out from the centre of detonation as an expanding hemisphere. The pressure in the blast wave is known by several names: blast pressure, incident pressure, free-field pressure, overpressure, etc. Blast pressure decreases rapidly with distance, roughly following an inverse square law (Figure 1). This means that doubling the distance between the explosive and the target results in ¼ the pressure acting on the target. This is an extremely important point that should be considered when implementing a blast security plan.

When a blast wave meets an object, a part of the wave is reflected while the remainder of the wave passes over and around the object, enveloping it and then continuing. The pressure in the reflected portion of the wave is significantly higher (two to twelve times higher) than the remainder of the blast wave. This is the most damaging part of a blast wave, as is made evident by post-blast pictures of damaged buildings, in which it can often be observed that the wall facing the blast has been severely damaged, but the sidewalls, those at right angles to the front wall, are relatively unscathed.

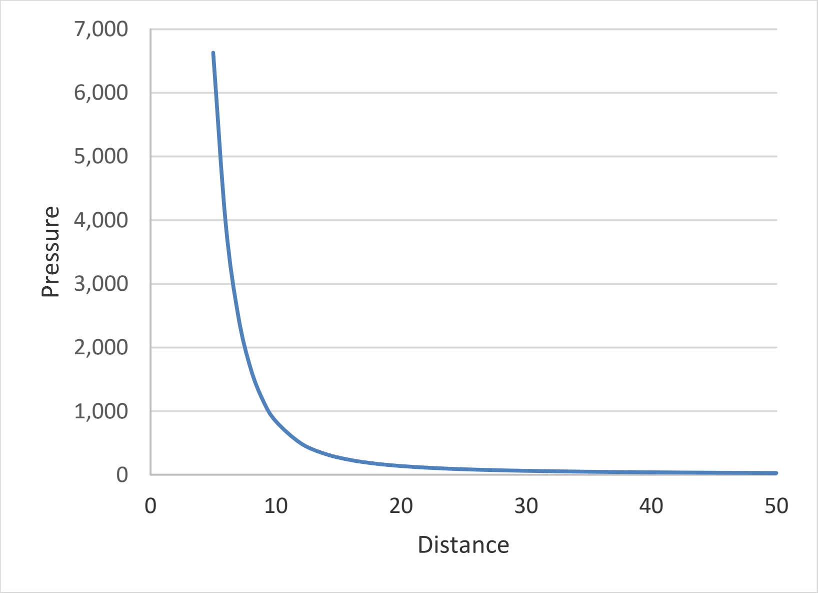

Figure 1: Decay of pressure with distance

Another key point to understanding the damage potential of a blast wave is the concept of impulse. The impulse, which is shown as the shaded area in Figure 2, is a measure of both the amplitude of the pressure and its duration. Impulse decays roughly linearly with distance, therefore if one doubles the distance between the explosive and the target, the impulse is halved. It is important to realize that both pressure and impulse are required to understand the damage potential of a blast wave.

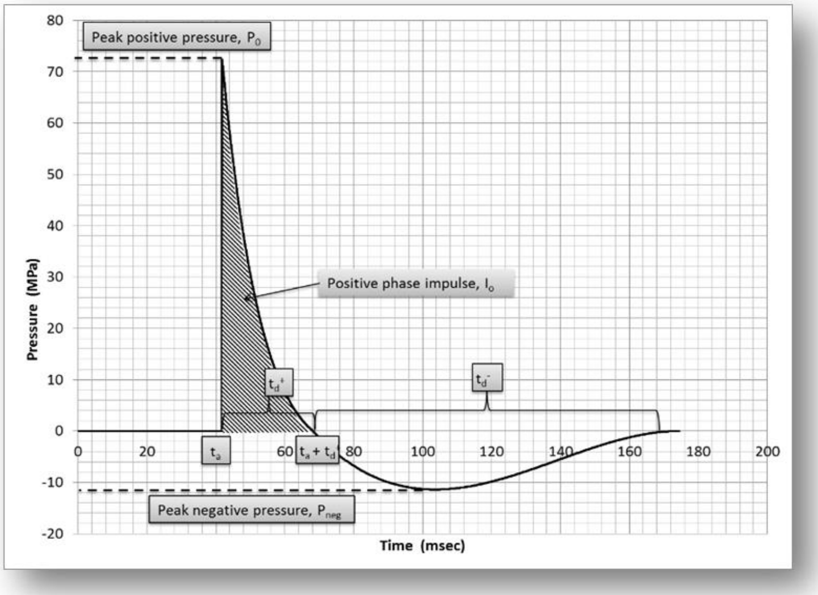

Figure 2: Pressure-time history of a blast wave. Impulse is the shaded area

Charges placed in direct contact with the target do not rely on air to transmit the pressure. Since air is a very poor medium for transmitting pressure, eliminating the air as a transfer medium greatly increases the transmitted pressure. This means that explosives in contact with their target have a greatly enhanced damage potential. The corollary to this is that the introduction of even a small air gap between an explosive charge and its target greatly reduces the efficacy of the charge. The security specialist can take advantage of this when protecting key assets.

Other Blast Effects

Other effects resulting from the detonation of an explosive device include: fragmentation, cratering, ground shock and fireball.

The ground shock, i.e. the shock propagating through the ground, is not usually considered when it comes to infrastructure protection as the effects are relatively weak. This is because the explosives in VBIEDs are not in direct contact with the ground (uncoupled) and the transfer of energy from the explosive to the ground is very inefficient. HEIEDs tend to be too small to cause any significant ground shock. Ground shock may be an issue near mining operations, where large quantities of explosives are placed in boreholes in the ground.

Cratering is not often considered in infrastructure protection either because it is a very localized effect. However, in cases where critical services such as electrical, gas or water enter a building near the ground surface, it may be necessary to consider the effect of cratering.

The fireball resulting from a detonation tends to have an extremely short duration, milliseconds. As a result, unless a material is extremely flammable, it is unlikely that the fireball will cause significant damage. In the case where there may be flammable gases such as natural gas or propane, the effect of the fireball should be considered.

Fragmentation is a significant hazard to people and equipment, but rarely to structures. Purpose-built fragmentation devices may produce fragments of several grams with velocities of up to 2000 m/s. Such fragments may penetrate through over 19 mm of steel or 100 mm of concrete and have a range of over 500 m through the air. Fragments from vehicles are generally much less effective because the vehicle body panels form light-weight fragments with very high drag, and as a result have a short range.

Blast Vulnerability Assessments

Blast vulnerability assessments are performed with the aim of determining the vulnerability of structures, personnel or assets to blast. The process comprises the following tasks:

- Formulation of the problem
- A site visit
- Identification of critical assets
- Scenario generation
- Review of relevant construction drawings
- Response calculation
- Determination of mitigation strategies
- Reporting

A detailed assessment requires a site visit. The visit helps to establish the location of critical assets, and locations which can be exploited by the attacker, i.e. access points, parking lots, nearest points of approach. The visit also allows the assessor to confirm details which have been identified in construction drawings. The assessor should be accompanied by both security personnel and an engineer responsible for the site, who can advise on procedures and provide details which may not be evident to someone unfamiliar with the site.

Construction drawings are required by the assessor to permit the blast response modelling of buildings and equipment. As-built drawings are preferred, although structural drawings may be sufficient. Architectural drawings rarely contain the necessary details. An assessment is only as good as the information upon which it is based.

Typically, the consequences of a blast are expressed in terms of damage to structures, assets, or possible fatalities to personnel. Once the vulnerabilities have been established, it is possible to design preventive measures.

A blast vulnerability assessment should be performed by a specialist, as it requires knowledge spanning several fields, including construction, dynamics and blast physics. In addition, the determination of the blast response of structures requires specialized software, much of which is not commercially available.

MITIGATION

General Security Measures

Blast is not a problem to be addressed in isolation from other security measures; good general security practices are also good blast hazard mitigation practices. For example, secure perimeter fencing, intended to reduce break-ins or theft, also makes it difficult to approach an asset with either a HEIED or VBIED. Good housekeeping reduces the probability of theft, but also eliminates locations to hide explosive devices. Other security measures which contribute to blast hazard mitigation include:

- Strong physical security posture
    - Security staff
    - Cameras
    - Alarms
- Controlled parking (underground should be eliminated if possible)
- Appropriate lighting
- Key control
- Identity badges
- Zoned approach to security
- Mail room procedures to deal with suspicious packages
- Staff training
    - Suspicious package identification
    - Responding to a bomb threat
- Exercises, preferably including first responders

FEMA 426 recommends the use of the four (4) Ds, Deter, Detect, Deny and Devalue as a basis for security. FEMA defines the terms as follows:

- Deter: The process of making the target inaccessible using tactics such as high fencing, electronic security systems lighting and security personnel,
- Detect: The use of intelligence and intelligence sharing to monitor and identify the threat before the attack occurs,
- Deny: The process of minimizing target damage by designing it or retrofitting it to be resistant to attack
- Devalue: The little value process of making the site appear of or consequence.

These principles also apply directly to blast security.

Blast-Specific Measures

If, after the general security measures have been put in place, there is still a concern that a blast hazard exists, blast-specific measures can be implemented. The specific measures are somewhat dependent on the target, but generally follow the principle of either reducing the pressure and impulse acting on the target or hardening the target.

The simplest way to reduce pressure and impulse on the target is to increase the stand-off distance. As was shown earlier, pressure drops rapidly with distance, therefore even a small gain in stand-off can have a significant beneficial effect. If the threat is a VBIED, then it is important that the vehicle be kept as far from critical assets as possible. This makes it imperative that the vehicle be prevented from entering controlled space. Access to the compound must be controlled using substantive vehicle barriers, preferably rated anti-ram barriers. Similarly, the perimeter fencing should be anti-ram rated. Testing agencies in the United States and the United Kingdom test and certify commercially available anti-ram barriers[5].

Visitor parking should be strategically positioned as far from vulnerable structures or assets as possible. Vehicles which must access the compound, i.e. delivery vehicles, should be vetted. The mailroom and loading dock should ideally be in a building which is separate and remote from other buildings.

The principle of increasing stand-off also works for HEIEDs. HEIEDs tend to be small devices, from less than one kilogram to a few tens of kilograms. As such, their effective blast radius is very small, and they are best employed as contact charges on specific pieces of equipment. This makes it important to keep such devices off critical equipment. Stand-off around equipment can be enforced through the use of additional fencing designed to make it difficult to place an explosive charge on the equipment. In some cases, fencing may be impractical, for example, in the case of very long pipelines. In these cases, it may be possible to wrap the equipment in a layer of material which enforces stand-off, for example 150 mm of insulation between an HEIED and a pipe may be sufficient to prevent a breach. Commercial products have been developed for this purpose, although caution is recommended because they are not all equally effective.

When it is not possible to increase the stand-off, blast shielding is an alternative. Blast shielding usually takes the form of a wall, placed either immediately in front of the potential target or immediately adjacent to the location of the threat, i.e. usually the perimeter of the property. The wall acts to deflect some of the blast effects, reducing both the pressure and the impulse on the target. The wall also has other benefits: it obscures the target and provides ballistic protection, which can be critical for sensitive equipment such as electrical transformers or high-pressure vessels. However, a blast wall must be designed by a qualified blast engineer to prevent the possibility of the wall failing and contributing to the debris field. In extreme cases, the debris from a failing blast wall can be more damaging than the blast pressure would have been without a blast wall.

To a limited extent, buildings and other structures can be hardened to resist blast. The most common retrofit involves the addition of a polyester film to the inside surface of window glazing or the replacement of the annealed glass with laminated glass. This is done to prevent the glass from shattering under blast load and forming hazardous high-velocity debris. Typical annealed glass windows shatter at approximately 3.5 kPa. With the appropriate window film, the capacity of the glass can approach 70 kPa, and in the case of laminated glass, much higher pressures can be resisted. Figure 3 compares the response of an annealed glass window and a filmed window as viewed from inside a building. When retrofitting a window, it is important to ensure that the window frame and the wall have the capacity to resist the additional load. There is little value in hardening a window only to have the wall fail instead.

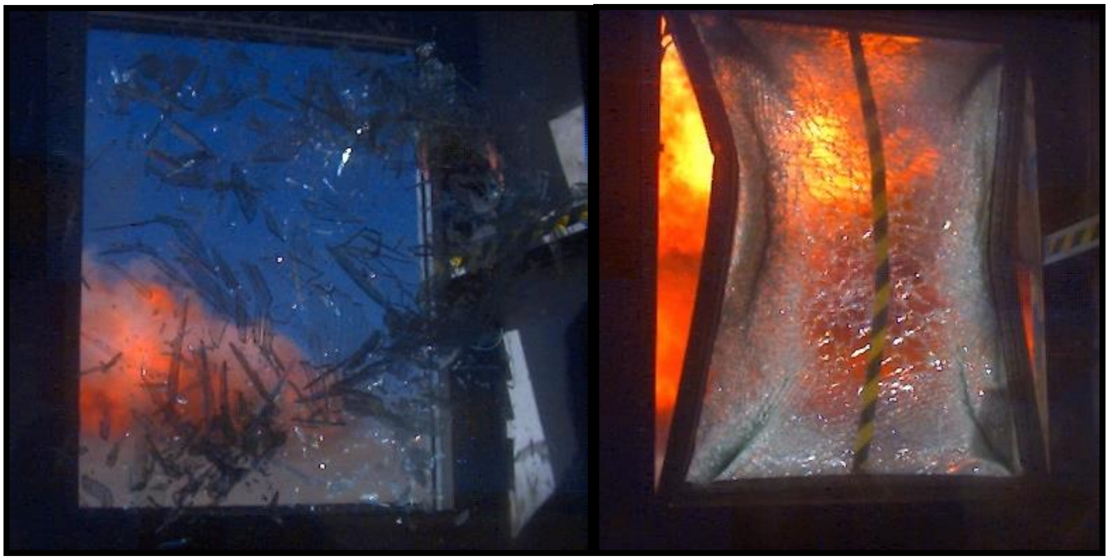

Figure 3: Response of unprotected annealed glass on the left versus filmed glass on the right as viewed from inside a building

The hardening of the walls of a building can also be achieved, although at a greater cost than the retrofitting of windows. Wall hardening is usually accomplished either by strengthening the wall itself, building a supporting structure behind the wall, or constructing a catchment system. Walls such as loadbearing or infill unreinforced masonry are particularly vulnerable to blast; unfortunately they are also common in industrial settings. These walls can be hardened by inserting rebar into the masonry and grouting it into place, or backing the wall with a structural steel frame as is shown in Figure 4. The backing frame must be anchored to the floor and ceiling slabs.

Regardless of the retrofit strategy, all blast retrofitting should be designed by a qualified blast specialist. Standard design practices do not apply to blast design; as a result, most architects and civil engineers would be unfamiliar with the design procedure.

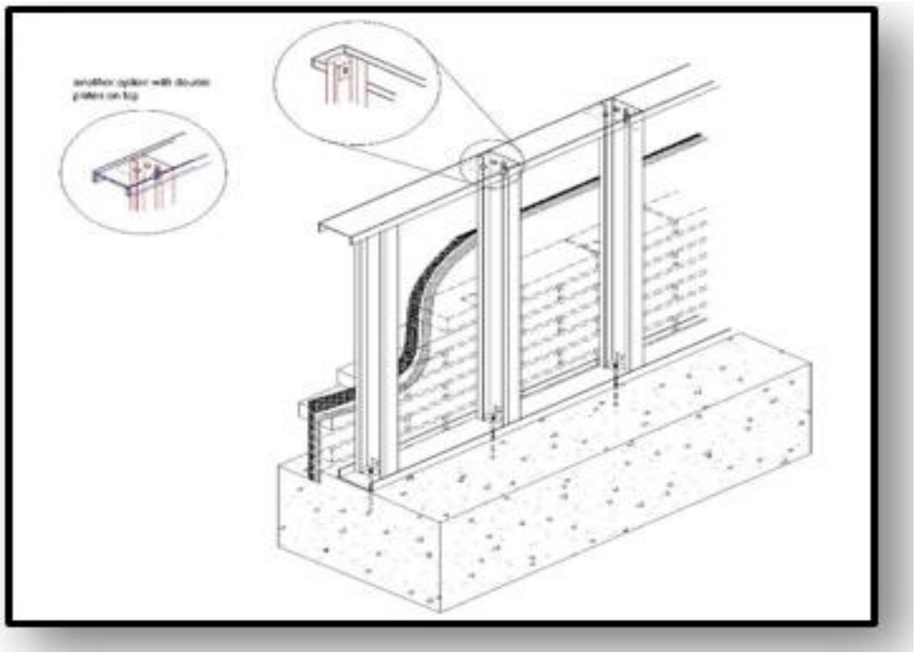

Figure 4 – Masonry wall retrofit

Conclusions

Over the past decade, the North American industry has become aware of the need to consider blast in their overall security plans. Designing a security plan around blast is not something that should be performed in isolation of other security requirements. Standard physical security practices intended to reduce theft and vandalism go a long way to reducing blast vulnerability.

However, if a blast specific security program is required, a blast specialist should be brought on board to conduct a blast vulnerability assessment and identify those assets which require protection. The assessment will also help determine whether asset vulnerability can be reduced by relatively simple measures, such as the installation of an additional security fence or blast wall, or whether it is necessary to design retrofitting to blast harden the asset.

REFERENCES

1. https://en.wikipedia.org/wiki/2008%E2%80%9309_British_Columbia_pipeline_bombings (accessed January 2018)

2. https://en.wikipedia.org/wiki/Oklahoma_City_bombing, (accessed January 2018)

3. https://en.wikipedia.org/wiki/2011_Norway_attacks, (accessed January 2018)

4. https://en.wikipedia.org/wiki/May_2017_Kabul_attack, (accessed January 2018)

5. https://www.dhs.gov/sites/default/files/.../Guide-to-Active-Vehicle-Barrier-2014-508.pdf (accessed January 2018)

USEFUL SOURCES OF INFORMATION

- FEMA 426, Reference manual to mitigate potential terrorist attacks against buildings

- Technical Support Working Group, Pipeline Mitigation Technologies, Final Technical Report, May 2011

- FEMA 427, Primer for design of commercial buildings to mitigate terrorist attacks

- Task committee on Blast Resistant Design, Design of Blast Resistant Buildings in Petrochemical Facilities, ASCE 1997

- UFC 3-340-02, Structures to Resist the Effects of Accidental Explosions, https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc, accessed Oct. 2017

Navigating Security Assessments: Tools and Methodologies

*Alexander St-Jacques**
Master's Student, Infrastructure Protection and International Security
Carleton University
Email: alexander.stjacques@canada.ca

Felix Kwamena, Ph. D.*
Adjunct Professor / Director, Infrastructure Resilience Research Group (IR^{2}G)
Carleton University
Email: felix.kwamena@canada.ca

*Andrew Lackey**
Master's Student, Systems and Computer Engineering
Carleton University
Email: andrew.lackey@canada.ca

Abstract

Security assessments are essential for energy infrastructure owners and operators, yet knowing what tools and methodologies to use and when is often difficult. This article explores the intended outcomes and limitations of four of the most common assessment practices, including risk assessments, vulnerability assessments, security audits and penetration testing. In highlighting their differences, it is argued that organizations should embed a security assessment framework into their security policy. In this way, owners and operators can ensure they use the right security assessment tool or method to receive the outcomes they need, when they need it.

A reliable energy supply is at the heart of the modern world, enabling society to produce the goods and services necessary for its health, safety and quality of life. As such, the security of critical energy infrastructure from natural hazards, accidents and malicious attacks is paramount. In order for energy infrastructure owners and operators to be confident that they have adequate security, they need security assessments that can provide assurance, and recommend improvements to their security posture. These assessments need to be based on their unique technologies, people and processes, the threat environment, and legal and regulatory obligations [1] [2].

Companies around the world often fail to address security concerns due to a general lack of agreement on how to address them and the necessary skills and knowledge to make informed decisions [3]. Tools and methodologies for assessing security, including vulnerability and risk assessments, security auditing and penetration testing, exist and are offered by plenty of consultants and security experts. The number of options available only adds to the challenge for owners and operators to select an assessment method or tool that suits their needs.

This paper seeks to provide clarity around four common tools and methodologies used for security assessments, and highlight their expected outcomes and limitations. These include risk assessments, vulnerability assessments, security audits, and penetration tests. While this paper does not seek to instruct owners and operators on which tools and methodologies to employ and when, it does seek to provide a clearer understanding of them. Once a clearer understanding of the assessment options available have been established, it is recommended that owners and operators establish a 'security assessment framework' to be embedded in their security policies to ensure they can select and utilize assessment activities that consistently and efficiently meet their needs.

Common Security Assessment Tools and Methodologies

Risk and vulnerability assessments are two of the most common security assessment methods – and two of the most commonly conflated. Even industry leaders like the American Petroleum Institute [4] [5] or the U.S. Department of Homeland Security [6] produce publications that use the terms interchangeably without explanation.[xiv] A risk assessment can be described as the calculation of the risk of security events in consideration of both the likelihood and potential impacts of the event. In its calculation, a risk assessment evaluates how the assets, threats (whether they be natural, accidental or human), vulnerabilities, and security measures already in place contribute to the likelihood and potential impact [7]. Once compared with the organization's security policy goals, including acceptable level of risk tolerance, the risk assessment can determine what the security needs are. Recommendations can then be developed in order to implement various countermeasures, while balancing the costs and benefits of mitigating the risks of security events.

A vulnerability assessment on the other hand, is used solely to identify and recommend fixes for system flaws and security gaps that can be exploited by a threat [7]. This requires an evaluation of the threats under consideration and the current security posture. In this way, vulnerability assessments can identify countermeasures to improve security by fixing flaws or introducing new countermeasures. However, unlike risk assessments, a vulnerability assessment does not produce risk-based priorities that consider the likelihood and possible consequences of security events occurring when making recommendations. Instead, they consider the target's "dynamic response and fragility to particular attack modes", [8, p. 3] of a given security event, and focus on addressing the greatest gaps and avenues of exploitation.

In short, a risk assessment can tell you if an asset requires security and to what degree, while the vulnerability assessment will tell you if there are issues with current security measures. Both risk and vulnerability assessments have important roles to play, and it should be noted that risk assessments actually have a vulnerability assessment as part of its process. For example, take the perimeter security of a physical facility and the possible security event of a thief breaching its fence. A risk assessment will evaluate the likelihood of a thief attempting to breach the fence, how they could breach the fence, and what could be stolen if the thief succeeds, helping you to determine if it is worth the cost to change or add different security measures that are necessary to lower the risk to an acceptable level. Alternatively, a vulnerability assessment can highlight ways the fence can be overcome by the thief, and recommend ways it could be fixed or improved. As such, a standalone vulnerability assessment should only be done if the need for the security measures under assessment has already been established.

In terms of cyber security, the nature of cyber assets means that security needs will always include a certain degree of access control. As such, standalone vulnerability assessments are much more common with cyber security assessments because the need for the access controls is already established. Moreover, the consequences of a cyber attack are often difficult to determine, making it difficult for a risk assessment to evaluate impacts, thus a vulnerability assessment is often the more practical option. Software tools known as 'vulnerability scanners' are frequently used for that purpose. While there is a use for both risk and vulnerability assessments over time, owners and operators need to understand their intended outcomes and limitations to know which to use their resources on: a determination of security needs and recommendations based on risk, or recommendations on how to fix vulnerabilities to meet previously determined security needs.

[xiv] The American Petroleum Institute and National Petrochemical and Refiners Association published the "Security Vulnerability Assessment Methodology," in 2003, then in 2013, they released the, "Security Risk Assessment Methodology, First Edition". By title alone, one would reasonably expect two different security documents: one focused on vulnerability, and the other on risk. Yet, the 2013 publication can be more accurately described as the 2nd edition of the 2003 publication, as both describe virtually the same risk assessment methodology. As another example, in the U.S. Department of Homeland Security, Office for Domestic Preparedness's 2003, "Vulnerability Assessment Methodologies Report," they set out to evaluate various vulnerability assessment methodologies. However, their evaluation criteria used was titled, "Ten Risk Methodology Evaluation Criteria."

A security audit is a third tool often used as part of security assessments that is offered by many security consultants and vendors. Security audits provide a technical and conceptual overview of an organization's security systems and practices to measure their security posture against a defined standard, generally for compliance purposes [7]. While they are important for legal and liability reasons, audits are not focused on improving security per say, like a risk or vulnerability assessment, but rather on whether policies and processes adhere to standards, and are being implemented and followed as intended. As well, audits do use risk and vulnerability assessments as part of their process, however the focus is generally towards protecting against non-compliance or poor implementation of policies, operating procedures, plans and controls [7].

As such, successful security audits provide assurance on compliance, but do not necessarily contribute to security. That being said, an audit can be used to evaluate the risk or vulnerability assessment process itself, or if security policies and mitigation measures are being implemented as intended. Therefore, they can fulfill an important role as a part of a larger security assessment process and serve the crucial function of maintaining compliance obligations. However, many auditing services will include security buzzwords in the description of their services. While some vendors may have the necessary expertise and methodologies to supplement their auditing services, owners and operators must be clear on what results they can expect from the audit (whether it actually goes beyond compliance), and any testing procedures they claim to be using.

A technique that is often associated with both vulnerability assessments and security auditing is penetration testing, or pentesting for short. Simply put, pentests simulate real-world security events to test the security of a target against a security event. What is important to note is that pentests in and of themselves do not comprise a risk or vulnerability assessment nor a security audit, as many vendors' description would lead one to believe, but are complementary tools. In contrast to other assessment methods, pentests test specific systems and configurations at a particular point in time, identify undiscovered vulnerabilities, and confirm or improve the security of systems, organizations or personnel [9]. They can also be used for testing response mechanisms, and creatively exploring the way an adversary may breach security and further exploit vulnerabilities once inside.

Penetration testing is a popular security buzzword, especially for cyber security assessments. Yet, like the other tools and methodologies above, owners and operators need to be aware of their intended outcomes and limitations. By emulating real adversaries, pentests can reveal vulnerabilities overlooked using other methods that are seemingly unrelated or minor, which can be used together to penetrate the target [2]. Moreover, they can reveal impacts and cascading effects not previously foreseen, and highlight unapparent ways security measures can be improved. However, pentests are not intended to find all available vulnerabilities, nor comprehensively prove a system is secure. Limited by time and resources, they can only demonstrate the use of vulnerabilities in one testing exercise at a time [9]. As well, while they can be useful for truly testing systems and employees, pentests can risk embarrassing employees or exposing assets to damage, making a reliable and respectful approach paramount to success [10].

Returning to the example of a fence for perimeter security around a facility, the intended outcomes and limitations of each of the aforementioned tools and methodologies can be demonstrated. A risk assessment will establish the need for a fence, a vulnerability assessment will search for the flaws in the fence, while a security audit will make sure that the fence was installed properly, as in if it is the correct height, or if it is inspected regularly according to industry standards. Both of these methods may deem the fence secure and compliant. As part of a supplementary pentest, a simulated adversary may creatively climb an adjacent tree close to the fence and jump over it. This basic example demonstrates how pentests can be useful for looking beyond what a vulnerability assessment and security audit can produce, and reflect the creative ways in which an adversary can use seemingly unrelated factors to reveal a vulnerability to exploit. The example also demonstrates the limitations of a pentest. For example, because the pentester found a way to overcome the fence, the pentest may not return to demonstrate other ways, such as using a vehicle to ram the fence. Therefore, while useful, owners and operators cannot rely on pentest results to highlight all possible ways the security measures may be breached.

Pentesting can be used for physical, cyber and personnel security purposes. Physical pentesting, often referred to as 'red teaming', can demonstrate the creative ways adversaries can overcome the physical security features, however it is often labor and resource intensive. Given the unique nature of cyber systems, as discussed above in relation to vulnerability assessments, pentesting is more routinely used for cyber security assessments. Using physical and cyber pentesting in tandem should also not be overlooked. For example, physically penetrating a facility could allow a threat actor elevated access to cyber assets that are normally considered secure. Penetration testing using social engineering techniques, wherein staff are targeted to be deceived or manipulated as a way to gain access, can also yield useful results.

Given limited resources, unlike the other tools and methodologies, there are important considerations that will limit a pentest. Prior to beginning, it must be determined if it will be testing for insider or outsider threats, how aggressive the pentest can be, and the level of risk and disruption the target will be exposed to. Lastly, choosing whether it ought to be covert or overt, pentesting has an effect on how the results can be used for training staff, planning for specific adversaries, and testing targets under regular circumstances or heightened alert [9] [11]. Owners and operators must also be cautious of maintaining the respect and dignity of staff while pentesting against them [11].

Overall, each of these four common tools and methodologies for security assessments can supplement each other and positively contribute towards better security. In brief, a risk assessment is a comprehensive overview that can determine prioritized security needs, vulnerability assessments identify flaws in the current security posture, security audits determine compliance against a given standard, and pentests conduct real-world simulations. Therefore, knowledge of their respective intended outcomes, limitations, and resource demands are crucial for planning and executing security assessments over the long term. It is especially difficult to do this when vendors use key terms interchangeably and mix the tools and methodologies together. While it is not necessarily detrimental for a vendor to mix assessment practices, owners and operators need to be clear from the outset what the expected outcomes are of the method or tool selected.

As such, it is highly recommended that infrastructure owners and operators create a security assessment framework that can be embedded in their security policy. In this way, any results or recommendations produced by an assessment process can coherently contribute towards achieving the security goals of the owner or operator. Otherwise, an assessment process that is not linked to a security policy with predetermined security goals risks wasting resources [9].

THE BENEFITS OF A SECURITY ASSESSMENT FRAMEWORK

While a security assessment framework should not prescribe the exact methodology or tool for each future assessment activity, a framework can broadly detail the timeframes and expected outcomes of different assessment tools and methodologies of varying rigor and scope that need to be conducted. In this way, the framework can drive a systematic process that coordinates the use of resources in an all-inclusive manner [1] [2]. The tailored framework will be able to increase efficiency, lower costs and ensure consistency over time and across the organization [2]. Additionally, with an established policy and framework, a healthier security culture can be fostered within management and staff to ensure their continued support, as the intended outcomes and limitations will be established and understood in advance [2]. Moreover, when selecting the right assessment methods or tools offered by vendors, they can be assessed against pre-established requirements based on intended outcomes, ensuring the right services will be procured consistently.

A security assessment framework should also address how the outcomes produced by assessment activities are to be handled. This includes how results, recommendations and action plans are tracked, reviewed and followed up on [11]. Without knowing how the results of an assessment activity are to be handled, management can be hesitant to undertake the activity out of fear they may lead projects or operations being halted, or that they will need to undertake expensive recommendations [12]. The framework can assure management that the purpose is simply to keep management better informed, with broadly established thresholds for when action is mandatory based on the security policy's goals and the acceptable level of risk tolerance. While issues do not always need to be addressed in the short or even long term, the framework can enhance accountability by requiring a record of justifications for not taking action, and establish timeframes for when they need to be revisited, serving to remind management of outstanding issues [12].

CONCLUSION

For owners and operators, deciding between the different tools and methodologies for a security assessment, choosing between a risk assessment, vulnerability assessment, a security audit, or a penetration test can be difficult. This paper has highlighted the key differences between the different tools and methodologies, as well as some of their intended outcomes and limitations. In recognizing the confusion around the different options, especially when offered by vendors, this paper recommends developing and embedding a security assessment framework into the security policy to ensure that assessment activities are used for the right reasons, have the necessary resources, and that results are used effectively. Depending on their security goals, regulatory demands, and resources available, each owner and operator will need to tailor a framework to their needs and how often the different tools and methodologies should be used.

REFERENCES

[1] T. Proffitt and A. Abdel-Aziz, "Scoping Security Assessments - A Project Management Approach", 2011. [Online]. Available: https://www.sans.org/reading-room/whitepapers/auditing/scoping-security-assessments-project-management-approach-33673.

[2] Joint Task Force Transformation Initiative, "SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans", 10 December 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[3] The Economist Intelligence Unit, "The Meaning of Security in the 21st Century", 2017. [Online]. Available: https://perspectives.eiu.com/sites/default/files/The-meaning-of-security-in-the-21st-century1.pdf.

[4] The American Petroleum Institute and National Petrochemical and Refiners Association, "Security Vulnerability Assessment Methodology", 2003. [Online]. Available: https://www.nrc.gov/docs/ML0502/ML050260624.pdf.

[5] The American Petroleum Institute and National Petrochemical and Refiners Association, "Security Risk Assessment Methodology", 2013. [Online]. Available: https://www.researchgate.net/publication/259137244.

[6] Office for Domestic Preparedness, "Vulnerability Assessment Methodologies Report", 2003. [Online]. Available: https://www.hsdl.org/?abstract&did=449166.

[7] M. Lupacchino, "Security Assessment vs. Security Audit", 2015. [Online]. Available: https://info.focustsi.com/IT-Services-Boston/topic/data-security/Security-Assessment-vs-Security-Audit.

[8] T. R. Brewer, J. E. Crawford, P. J. Vonk and L. M. Torres, "A quantitative approach to physical security assessments for power & energy infrastructure", in North American Power Symposium, Charlotte, NC, 2015.

[9] The German Federal Office for Information Security, "A Penetration Testing Model", [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile&v=1.

[10] T. Dimkov, W. Pieters and P. Harte, "Two methodologies for physical penetration testing using social engineering", 2009. [Online]. Available: https://research.utwente.nl/files/5097052/Pentesting_methodology.pdf.

[11] Souppaya, M. P. and K. A. Scarfone, "Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards and Technology", 2008. [Online]. Available: https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment.

[12] B. Hart, "Implementing a Successful Security Assessment Process", 2001. [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/implementing-successful-security-assessment-process-450.

Decarbonization of Heavy Industries: A Multi-Stakeholder, Multi-Disciplinary Approach to Addressing Challenges and Leveraging Opportunities

Felix Kwamena, Ph.D.*
Adjunct Professor / Director, Infrastructure and Resilience Group (IR2G)
Faculty of Engineering and Design, Carleton University
Email: felix.kwamena@canada.ca

Shahrzad Rahbar, Ph.D., ICDD*
President, Industrial Gas Users Association (IGUA)
Email: srahbar@igua.ca

There is a growing view that decarbonization of heavy industries in Canada – cement, iron and steel, mining, chemicals, and pulp and paper – means creating negative economic consequences and undermining their long term competitiveness.

This may be due to the fact that, unlike the electricity sector which is benefitting from the economics of wind and solar, cost effective technologies are not producing carbon dividends in other sectors.

What is not apparent is that decarbonization process is a set of wicked-interwoven challenges. Companies have focused on the use of technology-specific standards to address decarbonization and carbon emission control. This approach has not produced the expected results partly because emission trading strategies in theory and in practice are different issues. A review of the literature also indicates that policies have had limited results. In their recent study, Bataille and colleagues conclude that a broader social science framework requires the development of policy packages to inform a robust, fully decarbonized, energy intensive industry.

To build on the progress to date, a comprehensive multi-stakeholder, multi-disciplinary strategy and thinking is needed for full and active society-wide participation.

The questions that have to be addressed include:

- Is decarbonization really the answer to low carbon future?
- Will Canada still need the products of heavy industry?
- Can Canada's competitive advantages as a supplier of low-carbon be used to champion international leadership by using its heavy industries as examples?

Existing hydropower base, combined with wind, solar and ocean energy, biomass and natural resources, vast safely useable geological storage for carbon sequestration, and human resources, industrial base and technical research capabilities, give us a unique advantage.

The good news is that Canadian heavy industry is willing to partner and play a critical role.

On November 28-29, 2018, the authors will convene a workshop of representatives from academia, industry, government and non-governmental organizations to re-focus the discussion, and identify gaps in policy and research with a view to developing an integrated action plan.

The workshop will wrap up the evening of November 29th with the Dean's Annual Lecture – Infrastructure Security and Resilience.

The Dean's Lecture series is jointly sponsored by the Faculty of Engineering and Design and the Faculty of Public Affairs. It brings together distinguished speakers to address issues relating to infrastructure security and resilience before an audience of university faculty, post-graduate students, government officials, civil society and private sector representatives and selected diplomats. It is a landmark event which brings together experts from Canada and abroad to share knowledge with interested others. The Annual Lecture series is intended for panelists to look into their crystal balls and offer their vision of infrastructure security and resilience challenges and solutions for the next 5 to 10 years.

The theme of the 2018 Dean's Lecture is, "Economic Resilience of Canada's Heavy Industries: Transition to Decarbonization".

The panelists and topics are:

- Alan Young, Chair, International Institute of Sustainable Development: ***International Supply Chain Opportunities and Challenges***
- Chris Bataille, Author, Intergovernmental Panel on Climate Change: ***Heavy Industry and Decarbonization***
- Shahizad Rahbar, Ph.D. ICD.O President, Industrial Gas Users Association (IGUA): ***Paradigm Shift – Decarbonized Heavy Industry as a Competitive Long-term Advantage***.

We extend a warm invitation to all and look forward to your participation.

REFERENCES

Dale, A. (2017) How Do we Decarbonize [everything but electricity]? 1-8. https://solve.mit/edu/articles/how-do-we-decarbonize-everything-but-electricity.

Banks, J.P., Boersma, Tim; Ebinger, C.K. (2015) Does decarbonization mean de-coalification? Discussing carbon reduction policies. 19. https://www.brookings.edu/articles/does- decarbinzation-mean-de-coalification-discussion

Bataille, C., Ahman, M., Neuhoff, K., et al. (2018) A review of technology and Policy deep carbonization pathway options for making energy-intensive industry production consistent with the Paris Agreement. *Journal of Clean Production* 187. 960-973.

Meckling, J., Sterner, T., Wagner, G. (2017) Policy Sequencing toward decarbonization. *Nature Energy*, 2. https://www.nature.com/articles/41560.017.0025-8.

Levin, K., Cashore, B., Bernstein, S., and Auld, G. (2012) Overcoming the tragedy of super wicked problems: constraining our future selves to ameliorate global climate change. *Policy Science* 45. 123-152.

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*
Email: felix.kwamena@canada.ca

Divis, D. A. (2018), Congressional Mandate Means More Work on New Military GPS Receivers, Inside GNSS, January / February 2018 issue, http://www.insidegnss.com/auto/janfeb18-WV.pdf

Joerger, M., and M. Spenko (2017), Towards Navigation Safety for Autonomous Cars, Inside GNSS, November / December issue, http://www.insidegnss.com/node/5698

Klatt, C. (2017), Estimating Benefits to Canada and the World: the Canadian Spatial Reference System Precise Point Positioning Service, Geomatica, 71(1), pp. 37-44, https://doi.org/10.5623/cig2017-104

Klatt, C. (2016), Geodetic Technologies Enabling Innovation Part 1: Federal Government, Geomatica, 70(3), pp. 187-193, https://doi.org/10.5623/cig2016-304

McGranagham, R. M., A. Ghatt, T. Matsuo, A. J. Mannucci, J. L. Semeter, S. Datta-Barua (2017), Ushering in a New Frontier in Geospace Through Data Science, Journal of Geophysical Research – Space Physics, 122 (12), pp. 12586-12590, https://doi.org/10.1002/2017JA024835

Knipp, D. J. (2018), Advances in Space Weather Data Interpretation and Simulations, Space Weather, 16(3), pp. 198-199, https://doi.org/10.1002/2018sw001824

Quy-Toan Do, Jacob N. Shapiro, Christopher, D. Elvidge, Mohamed Abdel Jelil, Daniel P. Ahn, Kimberly Baugh, Jamie Hansen-Lewis, Mikhail Zhizhin, and Morgan D. .Bazilian, Terrorism, Geopolitics, and Oil Security: Using Remote Sensing to Estimate Oil Production of the Islamic State.

Energy Research & Social Science, 16 April 2018, pp. 1 - 8, https://reader.elsevier.com/reader/sd/B2E30FF4CAD50D136441DD37FF57040726FDB6BF4BA5F6A684630B40426EEA4B394343D013B093F7EC1ABEF0C4B97D2F

Ron Tira, Developing a Doctrine for Cyberwarfare in the Conventional Campaign.

Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice, by Matteo E. Bonfanti.

The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs, by David Siman-Tov & Noam Alon.

Germany's Cyber Strategy—Government and Military Preparations for Facing Cyber Threats, by Omree Wechsler.

Developing Organizational Capabilities to Manage Cyber Crises, by Gabi Siboni & Hadas Klein.

When Less is More: Cognition and the Outcome of Cyber Coercion, by Miguel Alberto Gomez.

Cyber, Intelligence and Security, Vol. 2, Issue 1 (May 2018), http://www.inss.org.il/publication/?ptype=456

Leslie Palti-Guzman, The Future of Asia's Natural Gas Market: The Need for a Regional LNG Hub, Asia Policy, volume 13, number 3 July 2018), http://asiapolicy.nbr.org

Jacqueline Westermann, Europe's Pipeline Politics, The Strategist, Australian Strategic Policy Institute [Australia], 30 April 2018, https://www.aspistrategist.org.au/europes-pipeline-politics/

CSIS Briefs, Mapping the U.S.-Canada Energy Relationship, Center for Strategic and International Studies – CSIS [USA], 7 May 2018, https://www.csis.org/analysis/mapping-us-canada-energy-relationship

Leslie Palti-Guzman, The Future of Asia’s Natural Gas Market: The Need for a Regional LNG Hub, National Bureau of Asian Research [USA], June 2018, http://nbr.org/publications/element.aspx?id=994

Fergus Hanson & Tom Uren, Australia's Offensive Cyber Capability**,** Australian Strategic Policy Institute [Australia], 9 April 018, https://www.aspi.org.au/report/australias-offensive-cyber-capability

Travelling abroad? Be Aware of the Risks of Espionage, General Intelligence and Security Service - AIVD (The Netherlands, 16 April 2018), https://english.aivd.nl/latest/news/2018/04/16/travelling-abroad-be-aware-of-the-risks-of-espionage

Ranjitha Shivaram & Adie Tomer**,** Do Our Infrastructure Systems Put People at Risk? Brookings Institution [USA], 10 May 2018, https://www.brookings.edu/blog/the-avenue/2018/05/10/do-our-infrastructure-systems-put-people-at-risk/

Lukáš Tichý and Jan Eichler, “Terrorist Attacks on the Energy Sector: The Case of Al Qaeda and the Islamic State”, the journal *Studies in Conflict & Terrorism Vol. 41,* No. 6, 2018, pp. 450-473, https://www.tandfonline.com/doi/full/10.1080/1057610X.2017.1323469

John Comiskey, Theory for Homeland Security, Journal of Homeland Security Education, Vol. 7 (2018), pp. 29-45, http://www.journalhse.org/v7-comiskey.html

David J. Mullan, “Developments in Administrative Law Relevant to Energy Law and Regulation” Energy Regulation Quarterly, Vol 6, Issue 1, 2018, pp. 19-36.

Stewart Fast “Who Decides? Balancing and Bridging Local Indigenous and Broader Societal Interests in Canadian Energy Decision-Making”, Energy Regulation Quarterly, Vol 6, Issue 1, 2018, pp 37- 46.

Pipeline Security Guidelines, March 2018, Transportation Security Administration.

Tomas Havranek, Dominik Herman, Zuzana Irosava, “Does Daylight Saving Save Electricity? A Meta-Analysis” The Energy Journal, Vol.39, No.2, pp. 35-61.

Christopher Sands, “Tax Debates Create Certainty and Uncertainty for North American Energy” Energy Issue 1, 2018, pp. 9-14.

Samarth Kumar, Dirk Hladik, and Philipp Hauer, “Challenges in Measuring Security of Supply in Changing Electricity and Natural Gas System” International Association for Energy Economics (IAEE) First Quarter 2018, pp. 15 – 20.

Prudence Dato, “Investment in Energy, Adoption of Renewable Energy and Household Behavior: Evidence from OECD Countries”, The Energy Journal Vol 39, No. 3, May 2018, pp. 213- 244.

***Felix Kwamena**, *Ph.D.*

Adjunct Professor/Director
Infrastructure Resilience Research Group (IR^{2}G)
&
Director, Energy Infrastructure Security Division
Energy Sector, Natural Resources Canada

INFRASTRUCTURE RESILIENCE RESEARCH GROUP (IRRG)
UPCOMING EVENTS

SPRING / FALL 2018

EVENT	DATE / LINK
Fall 2018 Training Courses	January to December 2018 https://carleton.ca/irrg/training/
Workshop: Economic Security, Resilience and De-Carbonization of Heavy Industries: Theme: A Multi-stakeholder,Multidisciplinary Approach to Addressing Challenges and Leveraging Opportunities for the De-Carbonization of Heavy Industries, Quebec Suite, Fairmont Chateau Laurier Hotel, 1 Rideau Street, Ottawa, Ontario	November 28 - 29, 2018 https://carleton.ca/irrg/cu-events/2016-symposium-on-critical-infrastructure-and-resilience/
The Dean’s Annual Lecture Series – Infrastructure Security and Resilience: Economic Security, Resilience and De-Carbonization of Heavy Industries , Quebec Suite, Fairmont Chateau Laurier Hotel, 1 Rideau Street, Ottawa, Ontario Ottawa, Ontario	November 29, 2018 (Evening) https://carleton.ca/irrg/cu-events/2016-the-deans-annual-lecture-series-infrastructure-security-and-resilience