VOL 1 ISSUE 6 **December 2017**

IR³ FEATURE ARTICLES

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 sixth issue of IR^3 shows that infrastructure resilience requires not only a knowledge of possible threats, but the tools available to aid in resilience.

Gaétan Houle urges power utilities to expand their resilience beyond the critical infrastructure protection (CIP) standards mandatorily required by the North American Electric Reliability Corporation (NERC). In addition to security threats targeted by the CIP standards, utilities face challenges imposed by a shortage of talent, largely due to an aging workforce; an increase in the sophistication, magnitude, and frequency of cyber attacks; aging infrastructure which must compete with increasing demands; and a demand for new technologies in response to, for example, the Internet of Things. Houle stresses that increased resilience requires a strong security culture.

In the article *Innovation in Security*, **Ross Johnson** describes his experience with cybersecurity in Israel. Johnson acknowledges the Internet as the latest great innovation, but points out that the opportunities provided by this technology are balanced by the vulnerabilities imposed by it. Recognizing the potential of the internet, as well as its inherent downfalls, has led to the development, now need, for cybersecurity. Israel understands both the advantage and threat imposed by the Internet and has become a leading nation in cybersecurity.

Wildfires pose a potential risk to nearby infrastructure, and resilience requires accurate knowledge of the location of vulnerable areas. **Lynn Johnston** describes the development of maps indicating the location of the interfaces where human-built structures are at risk. These maps are a valuable tool for improving community, industrial, and infrastructure resilience.

Doug Powell closes Issue 6 by introducing social media as an effective tool for countering social activism. Technological advancement has led to the development of social media as a means of supporting social activism and protest. Social media and web-based monitoring has therefore become necessary to define the risks associated with such activism to adequately mitigate potential impacts. Industry can, in turn, use social media as a tool to engage with protest groups and leaders, openly and publicly, as a means of countering potential risk.

Next Issue:

Issue 7 will focus on cybersecurity. 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 March 02, 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.

The 21st Century Electrical Grid: Security Beyond Compliance

Gaétan Houle, PEng, MBA
Principal Security Architect, Critical Infrastructure Protection
SNC-Lavalin
Email: gaetan.houle@snclavalin.com

Abstract

The Critical Infrastructure Protection (CIP) standards developed by the North American Electric Reliability Corporation (NERC) are mandatory requirements for power utilities that generate, transport or distribute more than 300MW of electrical power. With increasing and ever-changing security threats, the rapid evolution of technology and new business drivers, regulators are struggling to keep the standards up to date. Some updates can take up to two years to be formally approved, with an additional 18 months granted to power utilities to implement the corresponding compliance measures. The world of cyber-security changes at a much faster pace and could leave NERC CIP compliant power utilities exposed. While the CIP standards establish a good baseline for the industry, power utilities must go beyond mandatory requirements and base their security program on a series of best industry practices and a strong corporate security culture if they wish to minimize their security risk exposure.

I. NERC CIP

NERC is the electric reliability organization for North America [1], whose fundamental mission is to ensure the reliability and security of the bulk power system in North America. Among other responsibilities, they develop and enforce the application of the CIP standards. Subject to the oversight by the Federal Energy Regulatory Commission in the USA and the Department of Natural Resources in Canada, NERC's area of responsibility includes the continental United States, Canada, and the northern portion of Baja California, Mexico.

The NERC CIP standards are a set of mandatory requirements designed to secure the infrastructure supporting North America's bulk electric system. While the CIP standards have varied over the years, the basic requirements have remained the same: identify critical cyber assets, then implement electronic and physical procedures to protect them.

The CIP standards establish a baseline for the North American power system's security and apply to entities that "materially impact" the reliability of the bulk power system.

For over 10 years, the electric industry has been subject to mandatory compliance to the NERC CIP standards. Entities can be subject to penalties of up to $1,000,000 per day per violation for violating the NERC CIP standards [2].

II. THE PERFECT STORM

The power utility industry in North America is heading toward a "perfect storm", with many demographic, technological and security trends deeply affecting the way it will need to operate in the future.

Shortage of Talent

In accordance with a recent survey published by the Center for Energy Workforce Development [3], the power utility industry still employs a high number of workers who could leave at any time. In fact, as depicted in Figure 1, it is estimated that 62% of the power utility workforce will retire in North America over the next five years.

If we narrow this talent shortage to cybersecurity personnel, the ISACA, a non-profit information security advocacy group, reports that there will be a global shortage of two million cybersecurity professionals by 2019. Every year in the U.S., 40,000 information security analyst jobs go unfilled [4].

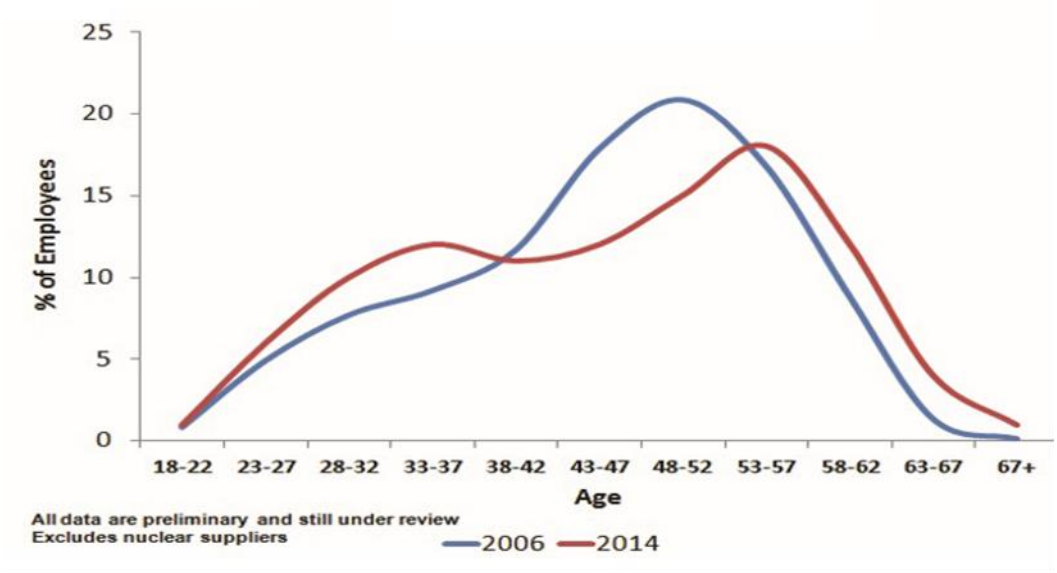

Figure 1 - Age Distribution Electric and Natural Gas Utilities [3]

Increasing Cyber Threats

In accordance with the US Department of Energy's Quadrennial Energy Review, cyber threats to the electricity system are increasing in sophistication, magnitude, and frequency [5]. Although cyber attacks occur with greater frequency and intensity around the world, many either go unreported or are under-reported, thus creating a false sense of security. We are no longer talking about the teenagers working from their bedroom in their parents' home; the main threats are now state-sponsored hackers, who attempt to infiltrate the critical infrastructures for geopolitical reasons. During his testimony before Congress in 2017, the US Director of National Intelligence, James Clapper, confirmed that more than 30 countries are developing offensive cyber attack capabilities [6].

As a prime example, on 23 December 2015, skilled Russian hackers successfully brought down a control center in Ukraine, leaving 225,000 customers without power for up to 6 hours [7]. This marked the first time that a cyber attack was successfully used against a nation's power grid. Investigations revealed that the attack had been planned over many months, first by obtaining system administrator credentials through a phishing attack, then by launching a synchronized assault using malware developed specially to target the technology specific to the power utility industry (dubbed CrashOverride). Among other things, the malware can manipulate the settings on electric power control systems by scanning for critical components that operate and open circuit breakers. It continues to keep them open even if a grid operator tries to close them, to create a sustained power outage. The malware, which is undetectable by conventional antivirus, also has a "wiper" component that erases the software on the computer systems that control the circuit breakers, forcing the grid operator to revert to manual operations, which means physically going to a substation to restore power.

Furthermore, in 2017 Symantec uncovered Dragonfly, a cyber espionage group that has been in operation since at least 2011, whose purpose is to perpetrate attacks, with the potential for sabotage, against the energy sector in Europe and North America [8].

Nowadays, this is the type of sophisticated threat that power utilities must be prepared to fend off.

III. A Fast-Changing World

Historically, utilities have been able to invest heavily in generation and delivery infrastructure because a steady growth in demand maintained affordable prices for customers and generated reasonable returns. However, changing consumer

habits, combined with conservation efforts and alternative power sources have eroded demand growth from about 7% annually (1949 to 1973) to about 2.5% (1974 to 2013). The projected growth from now until 2040 is less than 1% [9].

This level of growth is not sufficient to maintain the current system without raising rates. Yet, tighter emission regulations, greater security threats, and the aging transmission and distribution system require more than maintenance; they need expensive upgrades and replacements. Raising rates is not always attractive, as both utilities and their regulators are charged with keeping rates affordable, and higher rates increase the competitiveness of alternatives to utility-provided power, such as micro grids [10]. The industry must then look beyond its traditional cost-of-service model and look for operating efficiencies. Technology, particularly Internet of Things (IoT) applications, offers a wide range of possibilities for how electric utilities can reduce their operating costs.

The Internet of Things

IoT technology is now accelerating the digitalization of the power grid as it is seen as an effective tool to reduce the damage and impact of natural disasters to transmission lines, improve the reliability of power transmission, and reduce economic loss. However, many IoT devices are wireless, meaning they are more subject to intrusions than wireline sensors. In fact, many IoT devices being introduced into smart grid environments were not developed with security in mind and could be subject to various types of attacks, namely:

- Identity spoofing
- Eavesdropping
- Data tampering
- Password cracking
- Malicious code infection
- Denial of service

Do you remember the shortage of cybersecurity professionals discussed earlier? Cybersecurity professionals now need to develop expertise on how to secure IoT devices, or protect against them should they become compromised and used by hackers to attack the infrastructure. For example, over the past couple of years, hackers have infected security cameras with malware that allowed them to saturate computer networks with large video streams. Given the afore-mentioned shortage of professionals, developing security expertise of IoT devices is particularly challenging

Bi-directional Flow of Power and Information

As depicted in Figure 2, the grid is evolving from a one-way system where power flows from centralized generation stations to consumers, to a platform that can manage decentralized consumption and production systems so that power and information can flow as needed in multiple directions.

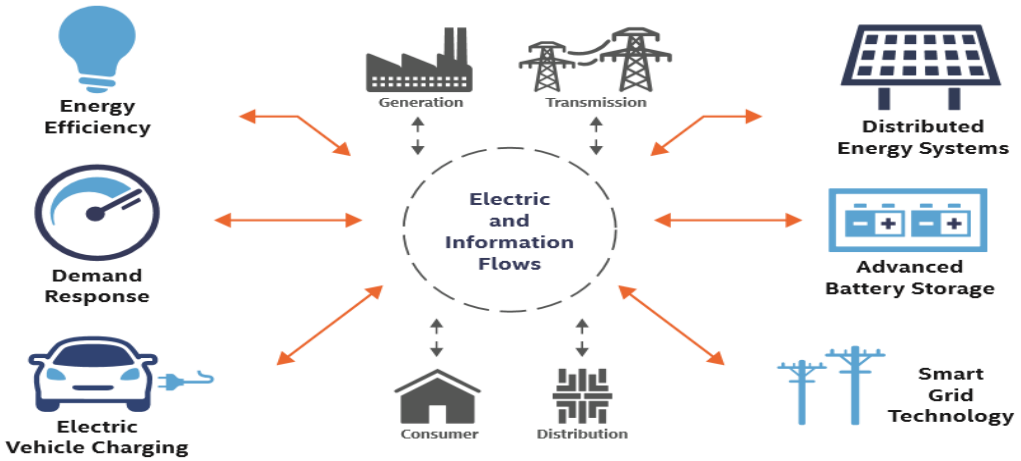

Figure 2 – 21st Century Energy Infrastructure [10]

At the heart of these advances are technologies like sensors and big data analytics, which together form interconnected systems capable of quickly analyzing large amounts of data. This new capability promises power utilities the ability to provide a more reliable and customized service to consumers at a lower operating cost.

For the consumer, this new technology is great. For the Chief Security Officer (CSO) at the power utility, the smart grid has exponentially increased the number of entry points and devices to protect.

Unlike the world of Information Technology (IT) where Microsoft and UNIX are the dominant operating systems, so far there is no standard operating system for IoT, which means that CSOs are struggling to standardize security procedures such as access control, patch management, antivirus, etc. across all these new devices.

Smart Meters

The smart grid initiative aims at transforming today's public power grid into a flexible and intelligent energy entity. New technology will provide detailed monitoring of the grid status and energy consumption behavior of connected customers to implement control mechanisms, flexible billing processes, and more cost effective services. However, these advantages do not come without costs; the increasing integration of advanced metering infrastructure (AMI) with information and communication technology leads to new security and privacy challenges.

According to the industry, the firmware running in smart meters will have to be upgraded regularly during its normal lifespan, which could be up to 15-20 years. Designing a security system that will be effective over such a long period of time is a complex task. Among others, the management of cryptographic keys over the entire life cycle of the meters is of particular concern for security practitioners. What happens if the key used to sign firmware upgrades is compromised?

Manufacturers need to balance between time-to-market and the reliability of their product, which is why software often needs to be patched after it has been released. The mechanism used to perform such upgrades could also be used to update meter configurations to support modifications to tariff plans, alarm and alert, network functionality, communication features, and much more. A scenario where a field technician physically plugs in his laptop to install new firmware in each of the millions of smart meters is simply not a cost-effective option. Accordingly, an over-the-air upgrade, where smart meters can be programmed with new firmware remotely, is the approach elected by power utilities. However, this much wanted feature does come with its share of potential security risks. If proper security measures are not taken, attackers could patch a meter with their own malicious firmware. The utility could probably manage a localized compromise of a single meter. However, if the attack can be propagated to a larger install base, it could lead to serious problems.

Ontario's Long Term Energy Plan [11] promises to leverage all sorts of smart meter related technologies, all of which, if not secured properly, could cause havoc to the electric grid. Here are smart grid initiatives currently being deployed:

- Smart grid technology platform connected to a network of large-scale commercial and industrial electricity users to automatically increase or decrease electricity consumption in response to moment-by-moment changes in the electricity needs of the grid.
- Programmable communicating thermostats for commercial properties, which provide automated energy conservation through demand response programs.
- Mobile applications and devices, such as smart thermostats that make it easier for consumers to monitor and manage their home energy use and costs.

Resilience Through Inter-Connectivity

The North American ice storm of 1998 caused massive damage to trees and electrical infrastructure, leading to widespread long-term power outages in the northeastern regions of the USA and Canada, and particularly the Montreal area. Millions were left in

the dark for periods varying from days to several weeks, and in some instances, months [12]. More recently, Puerto Rico was hit by hurricanes Irma and Maria, leaving 3.5 million people without power. Global climate change is forcing power utilities to be more resilient and have access to alternate sources of power during situations of natural disasters where main power distribution lines are damaged.

There are close to 3,000 power utilities operating in Canada and the USA, ranging from large provincial or state utilities to small municipal entities. To provide a resilient service to their customers, neighboring grids, as well as numerous utilities integrated through acquisitions, need to be interconnected. If not properly secured, this level of interconnectivity could be leveraged by intruders to cause massive blackouts. For the CSO of a power utility, this interconnectivity represents another potential source of security challenges. This is especially true since power utilities producing less than 300 MW are not mandated to comply with NERC CIP security standards.

IV. Impact on Security

The need for electric grids to be interconnected, as well as the deployment of new technologies, has a profound impact on power utilities' security programs.

IT and OT Convergence

Operational Technology (OT) consists of devices such as Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, Safety Instrumented Systems (SIS), etc., that monitor sensors, pressure meters, thermometers, electric power meters, etc., and control physical equipment such as valves, pumps, power breakers, etc. Old industrial control systems were primarily designed with safety and reliability in mind, not necessarily security. Accordingly, old PLCs often have passwords hard-coded in the firmware of the devices.

Historically, however, IT and OT systems have been kept separate, the later operating over serial communications protocols, using proprietary systems, which are difficult to scale across multiple technologies and providers. In order to reduce development and support costs and decrease time-to-market, OT equipment vendors have integrated many IT-derived developments, such as an Internet Protocol (IP) network interface and software that requires periodic updates. This new approach means that OT systems may need to be upgraded or patched to address security flaws, and be protected against malware infiltration. Operators will need to be connected to a local area network, and be integrated with a central identity and access management system to perform such updates. Gradually, the procedures and technology used to support OT are becoming very similar to those used to support IT systems.

Not surprisingly, the deployment of smart grid technology is forcing a marriage between IT and OT functions in an effort to concentrate the scarce resources needed to support the infrastructure. That being said, OT and IT come from very different cultures and have significant hurdles to overcome in pursuit of collaboration to achieve security and interoperability without disrupting critical services. A recent Gartner survey [13] found that organizations are keen to integrate IoT and IT technologies into OT systems. However, most organizations do not yet have the skills, expertise or time to drive the IT/OT alignment requirements.

Increased Attack Surface Area for Hackers

One of the key principles in security is to reduce the attack surface area that could be exploited by hackers. Attack surface area is defined as the reachable and exploitable vulnerabilities that a system has. Attack surface areas are not limited to equipment, they are also comprised of software (the larger the number of lines of code, the higher the probability of a security flaw) and people (the more people needed to support complex infrastructures, the higher the probability of human error).

Formerly, industrial control systems were isolated, disconnected from the Internet or from corporate networks, and were managed by a limited number of operators. With all of the interconnected technology being deployed by power utilities, maintaining a true network isolation between the OT environment and

the rest of the world is becoming untenable. In effect, the attack surface area that can be exploited by hackers is increasing considerably. The cyber attack against the Ukrainian power grid in 2015 is a prime example of what could happen.

Regulators are Struggling to Keep-Up

Given the rapidly increasing security threats and emerging technology being deployed by power utilities, the Federal Energy Regulation Commission (FERC) is struggling to keep the NERC CIP standards up to date. The development and approval of new versions of the CIP standards generally take up to two years to materialize. Once these standards are approved, power utilities are then given a reasonable period of time to comply with the new standards. Typically [14]:

- Six months to evaluate and purchase automated data collection tools for NERC reporting; and,
- One year to implement and operationalize systems, and ensure adequate compliance documentation before the standard becomes effective.

Given the speed at which technology and security threats evolve, it is abundantly clear that being compliant to NERC CIP alone is nowhere near sufficient to keep power utilities' infrastructure secure.

V. SECURITY CULTURE

Power utilities' security programs should not be built on security compliance requirements alone; they must also take into account:

- The evolving threat landscape;
- Changing operational and business requirements; and,
- Technological evolution.

As stated by Timothy E. Roxey, VP and Chief E-ISAC Operations Officer at NERC, "we have a culture of compliance when we should really have a culture of security" [14].

What is a security culture? The Centre for the Protection of National Infrastructure defines a security culture as a "set of values, shared by everyone in an organization that determines how people are expected to think about and approach security" [15]. Proactivity and responsiveness are key attributes.

A strong corporate security culture starts from the top, at the Board and C-suite level. One cannot expect a security culture to be driven by the firewall administrators. Here are initiatives that can be taken by top executives to support a security culture within their organization and to effectively manage security risks:

- Ensure that security risks are on the agenda of their meetings by default;
- Track a risk register comprised of the top 10 most significant security risks and the mitigation strategy; and,
- Invite the CSO to brief the Board and the Executive Committee on a regular basis. During the presentations, ensure that reliable security metrics are used to demonstrate trends.

Top management should not assume that their employees and subcontractors are aware of all the security procedures that need to be followed. In fact, phishing is now the preferred attack vector used by hackers to infiltrate an organization's IT infrastructure. Accordingly, a comprehensive mandatory security awareness program is essential to a strong corporate security culture.

CSOs should support an holistic and proactive program where they are ahead of the game, including:

- Staying abreast of new security threat vectors and how they could impact their organization;
- Coordinating with their peers in the industry to exchange best practices;
- Keeping senior management apprised of the security risks and seek the necessary funding to mitigate risks instead of waiting for a breach to occur; and,
- Not limiting their activities to the minimum security compliance requirements.

IT / OT convergence is inevitable. The sooner the two groups start working together, the more they will be able to learn from each other on the best ways to tackle new threats, compliance requirements, and new business drivers.

VI. Conclusion

Emerging technology is rapidly evolving to address new business drivers and security threats are increasing at an alarming rate. Although NERC CIP compliance is essential to ensure a common baseline across the industry, it cannot be the only measure used by power utilities to manage their security risks. Complete security risk management extends from technical staff and security professionals into the C-suite, boardroom, and beyond. To keep the electric grid secure and reliable, the responsibility of security must ultimately be proactively shared by everyone in the power industry.

About the Author

Gaétan HOULE, Peng, MBA is the Principal Security Architect, CIP at SNC-Lavalin. SNC-Lavalin is the largest engineering firm in Canada with offices and operations in over 160 countries. SNC-Lavalin is constantly ranked among the top engineering design firms in the world.

Gaétan has held several senior positions in the Canadian Federal Government, including Chief Engineer, Communications Security with the Department of National Defence; Director, Corporate Security with the Department of Foreign Affairs and Consul at the Canadian Embassy in Peru, following the 1996-97 terrorist crisis in Lima.

In the private sector, he has worked as Chief Security Officer for several multi-national corporations, including Bombardier Aerospace, Airbus Group (Paris, France) and Bell Canada, where he personally crafted the security plan to protect the telecom infrastructure for the 2010 Winter Olympics in Vancouver. In 2016, having worked for four years as the National Cybersecurity Practice Leader for Ernst & Young Canada, Gaétan joined SNC Lavalin as the Principal Security Architect CIP where he and his team help clients in the energy industry protect their critical infrastructure.

Gaétan has a bachelor's degree in Electrical Engineering from the Royal Military College of Canada and an MBA from the Jones International University. He is a member of the order of Professional Engineers of Ontario.

References

[1] About NERC (2016). Retrieved from http://www.nerc.com/Pages/default.aspx

[2] NERC (December 2012) Sanction Guidelines of the North American Electric Reliability Corporation. Retrieved from http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4B_SanctionGuidelines_20121220.pdf

[3] Center for Energy and Workforce Development (2017) Five Things You Need to Know about Energy Workforce Development. Retrieved from http://www.cewd.org/Documents/5Things-SlideBooklet-Feb2017.pdf

[4] ISACA (January 2016) 2016 Cybersecurity Skills Gap. Retrieved from https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

[5] US Department of Energy (January, 2017) Quadrennial Energy Review

[6] Steve Ranger (2017, January 5) US intelligence: 30 countries building cyber attack capabilities. Retrieved from http://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities

[7] E-ISAC (March 2016) Analysis of the Cyber Attack on the Ukrainian Power Grid. Retrieved from http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[8] Symantec (Sep 2017) Dragonfly: Western energy sector targeted by sophisticated attack group. Retrieved from https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

[9] Karl McDermott (2016) Cost of service regulation in the investor-owned electric utility industry—A history of adaptation, Edison Electric Institute

[10] Intel (2016) Transforming Utility Grid Operations with the Internet of Things. Retrieved from https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/transforming-utility-grid-with-iot-brief.pdf

[11] Ontario Department of Energy (December 2013) Ontario's Long-Term Energy Plan

[12] U.S.-Canada Power System Outage Task Force (April 2004) Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations

[13] Gartner (June 2017) Redefining ITAM for the Digital Age

[14] Kitchel J. (January 2013) NERC CIP v5 is Coming. Get Ready. Retrieved from http://www.isssource.com/nerc-cip-v5-is-coming-get-ready

[14] Davis K (August 2011) The NERC CIP Evolution. Retrieved from http://www.elp.com/articles/powergrid_international/print/volume-16/issue-8/features/the-nerc-cip-evolution.html

[15] Center for the Protection of Critical Infrastructure (2017) Developing a Security Culture. Retrieved from https://www.cpni.gov.uk/developing-security-culture

Innovation in Security

Ross Johnson
Senior Manager, Security and Contingency Planning
Capital Power
Email: rossintx@gmail.com

What is innovation? A Google tour of the subject shows that there are many different views of what the word means. According to the Merriam-Webster dictionary, it means '*the introduction of something new' or 'a new idea, method, or device*.' To President Barack Obama, "*Innovation is the creation of something that improves the way we live our lives.*" To the Organization for Economic Co-Operation and Development, "*Innovation can be defined as 'new products, business processes, and organic changes that create wealth or social welfare*."

History has shown us that the greatest innovations accelerate the development of our civilization. Gutenberg's printing press allowed ideas and knowledge to be stored in books and collected and shared; the industrial revolution harnessed energy in the production of goods, vastly increasing output; and the Haber process turned atmospheric nitrogen into ammonia, creating a new source of fertilizer which fuelled a population increase from 1.6 billion in 1900 to 7.4 billion today.

The latest great innovation is, of course, the Internet. All of the great innovations in the past have served to help us get to this point, so arguing which is the most important is pointless. The value of the Internet is the way it can use information and communications to control processes, monitor the environment, and inform people, globally, in real or near-real time. From this capability, almost anything is possible.

With great power comes great potential for disaster, though. The Internet can also provide unprecedented opportunities to steal secrets or money or things that can be sold for money; to destroy equipment and lives and reputations; to turn data into hostages; and to sow propaganda and lies to a credulous public. It can provide the tools to both unite and divide, and accelerate the pace of events beyond the capability of governments or other organizations to respond.

Israel recognized the potential of the Internet to boost their economy, and a host of Internet-related software and hardware followed. Israelis invented the USB stick; the first personal computer microprocessor, the Intel 8088; RSA public key encryption; Waze, the navigation app; the Iron Dome antimissile system; and many more innovative solutions to some of the Internet's most intractable problems. Israel was recognized as an innovation leader long before the Internet: in 1974, Intel established their first R&D plant outside of the United States.

Prime Minister Netanyahu recognized that while the Internet provided Israel with great opportunities, it was also a great vulnerability. In 2014, he announced the creation of a National Cyber Defense Authority. He said, "This new authority is an 'Air Force' against new threats which will not solely rely on existing defense teams. We are in a new world, we are organizing new forces, [and] it [has] great significance for Israel's defense in the future."

Today there are more than 300 cybersecurity companies operating in Israel – as an industry, second only to the US in size. Their 2014 exports of $6 billion represent 10% of the global market for cybersecurity products. Over 25 multi-national corporations have R&D centers in Israel, including household names such as IBM, Microsoft, Intel, McAfee, Intuit, and PayPal. Lockheed Martin announced recently that they would be establishing an R&D centre there as well.

In cybersecurity, the engine of Israel's innovation is their near-universal military service. High school students with an aptitude for cyber are selected and given additional training while still in school. When they graduate, they are recruited into military intelligence where they are trained to operate in offensive and defensive cyber warfare units. When they leave military service, they have several options: join other government security services in their cyber units; go for advanced education at Ben Gurion University; join private industry; or start their own company.

The process of taking an idea to market includes meeting with an incubator company, which will evaluate their idea, introduce them to a venture capital company, and guide them through the first two years of the start-up business cycle. This process is being enhanced even further through the creation of CyberSpark at Ben Gurion University in Be'ersheva. When complete, it will be a cybersecurity innovation campus that includes education, military intelligence, industry, venture capital firms, and government. Close proximity will reinforce the sharing of ideas and people. Based in the Negev desert south of Tel Aviv, it will have the additional advantage of offering housing at much more competitive prices than Tel Aviv, which will help to attract young people trying to get their start in life.

Canada and Israel have a special relationship in the arena of research and development. Led by Canadian scientist Henri Rothschild, who holds a masters and a doctorate in bio-nucleonics from Purdue University, the Canada-Israel Industrial Research & Development Foundation (CIIRDF) works to partner collaborative R&D between private sector companies with the goal of commercializing new technologies. The CIIRDF promotes the benefits of the relationship; offers a service to pair Canadian and Israeli companies who are seeking R&D partners; and invests in bilateral R&D initiative with high commercial potential.

In May 2016, I was invited to travel to Israel by a company called AWZ Ventures, based in Toronto. AWZ imports knowledge, know-how and technology from Israel, to advance and implement state-of-the-art, integrated, customized and comprehensive cyber intelligence, and physical security solutions and services for business and government in North America and globally. Their Advisory Board includes Stockwell Day, former Public Safety Minister in Canada and Avi Dichter, a former Public Safety Minister in Israel, and former senior intelligence executives from Canadian and Israeli agencies and military units. (I act as a compensated consultant for them as their critical infrastructure advisor. I first met AWZ Ventures in 2015 when I attended a cyber-security conference in Israel as part of a Canadian Electricity Association delegation). They are investing in a number of cyber intelligence and physical security companies, and requested my advice on which ones would likely do well in North America. We visited a number of companies in the 11 days we were there.

Our visit started with a meeting with Dr. Tal Steinhartz, the Chief Technology Officer of the Israel National Cyber Bureau (INCB), who explained how the Israeli cybersecurity ecosystem was founded, and how they grew into the center of excellence they have become. The INCB, comprised of 35 cyber experts, reports to the Prime Minister of Israel, ensuring that the full support of the government is behind them. Dr. Steinhartz describes cybersecurity as a "domain of problems," and explained how Israel's strategy rests on three pillars:

- **Robustness**: the capacity to perform without failing; repelling and containing cyber threats; an activity that organizations 'do' and governments 'promote'
- **Resilience**: a system's capacity to handle threats in order to regain normal functioning; event driven
- **Defense**: starting with the premise that 'you've already been hacked,' they seek to minimize the effect of the attack

The remaining time in Israel, we visited a number of companies that are developing products that help Israel to achieve its strategy.

Octopus Command & Control is an innovative command-and-control solution that provides users with a holistic view of their unconnected physical security, cybersecurity, health & safety and facilities technology, sensors, devices, data sources and applications. It is the only Cloud-enabled and mobile device-ready system of its kind on the market.

Octopus offers a unified and converged platform that is specifically tailored to the user's needs, integrating technology, procedures and personnel into one command & control capability in order to manage safety and security operations, improve decision-making and responsiveness, and reduce costs. Among many other features, Octopus allows users to swiftly and accurately obtain information about unwanted incidents, which allows faster and better decision-making and deploying of resources.

Octopus was developed by security industry experts and has already been successfully deployed in critical infrastructure, government, financial services, manufacturing, transportation and other sectors around the world. It currently carries four ISO certifications for quality management, information security, software engineering and IT service management.

SIGA is an end-point SCADA security system that will defeat any known attack. It works by monitoring the behavior of the end-point equipment you are protecting by analyzing the analog signals, rather than digital, and reporting anomalous readings, allowing operator intervention before damage occurs. Developed with the support of an incubator company funded by Alstom, it is particularly well-suited to use in the energy sector.

Most Internet intelligence services work by monitoring open source reporting and aggregating information. Senpai Technologies' creation – RogueEye - allows the user to create and manage espionage avatars, deploying them in the Dark Web to gain access to chat rooms and channels where our adversaries plan their campaigns. (We received a live demonstration of this product by a young man in a bank security operations center. He has one of the most interesting jobs I have ever seen.) RogueEye can help protect your company from direct action radical groups, criminals, and insiders who may be using their position to sell proprietary or personal company information.

Another intelligence service we looked at is BICI. Their CEO, Shai Braitner, served in the Israeli Defense Forces as a naval commando, and now heads an organization which largely serves the legal industry by locating evidence and assets. His company has developed an engine which finds linkages and associations between individuals or individuals and objects – particularly helpful if you are tracking down and recovering stolen assets.

MinerEye was recognized as a Gartner 'Cool Vendor' on their 2016 list. (40% of Gartner 'Cool Vendors' are from Israel.) Their product, VisionGrid™, allows you to see where your data is. Or, as MinerEye says, "Providing scalable analysis and governance of unstructured data across disparate and distributed file shares, desktops and collaboration sites, VisionGrid enables companies to discover, analyze and act on data to increase data privacy, data protection and overall compliance." It will show you where all your sensitive information is stored, and help you to protect it. During the demonstration, the enthusiasm and excitement for this product increased quickly as we realized how powerful it was, and useful it would be for data security, data classification, regulatory compliance, investigations, and many other functions.

Almost all cybersecurity training is conducted at the individual level. This is good for improving individual skills, but when your company is being attacked by cyber criminals or hackers, you respond as a team. CyberGym, a joint venture with the Israel Electric Corporation, will train your entire cyber incident response team and senior cyber management. Your team is in a room with computer equipment configured to emulate the system you use at home. Exercise controllers and your company's senior management is in another room watching skilled hackers trained by the Israeli Defense Force's offensive cyber warfare group attack 'your' computer systems. (There are real-world consequences to these

attacks; part of the configuration is a water pump, and if the hackers gain access to it you can end up with water on the floor. They can also turn off your lights.) Training typically lasts four to five days, and by the end of the week your employees have learned to operate as a tightly-knit team, experienced in defending your systems against a wide variety of attacks.

L7 Defense is a company which has developed a product that protects applications on websites. Application-layer DDOS attacks are complex: most webpage DDOS attacks are now handled by the Internet Service Provider, but normally a company only finds out that their application has been attacked when their customers contact them to tell them that something on their website is not working, like a payment module. An application can be down for hours before the company realizes they have a problem. L7 Defense has created a product that will halt an application DDOS attack in under *20 seconds*.

Insider threats are a lot like the weather: everyone talks about them, but few have figured out what to do about them. Fortscale (another Gartner 'Cool Vendor') has created a User & Entity Behavior Analytics (UEBA) product which detects insider threats. According to Fortscale, "82% of attacks use your own credentials against you." These attacks could be based on 'stolen credentials, rogue users, or careless employees.' It looks for abnormal account behavior which would indicate credential theft or abuse. As Fortscale says, "It's not magic, it's just really good math."

Another company to watch is SecBI. Security Business Intelligence is a Security Incident Event Management (SIEM) tool which allows you to prioritize events, investigate their cause and effects, and shows you the effects and impact of various defensive strategies. They are described as an 'adaptive investigation platform that combines advanced machine-learning capabilities, cybersecurity expertise, and user feedback.'

Our trip wasn't limited to cybersecurity. We met with Shafran, a global security consultancy and management company led by former Israeli Security Agency members. They have a number of core competencies: security systems design; background checks and employee vetting; and close protection. Their vetting process was particularly interesting; it combines the usual police and credit checks with a questionnaire and a session with a professional security interviewer. The questionnaire is designed with check questions; someone giving untruthful answers is highly likely to be tripped up, which is then followed up by the security interviewer.

I believe that there are several reasons why Israel has become a powerhouse in the cybersecurity domain: universal military service which gives them the opportunity to select the best and the brightest in cyber, and start them on an organized career path; a strong venture capital base; and centralized government policy-making which recognizes cyber-security as a strategic national goal. They are a good example of what a nation can do when everyone is rowing in the same direction.

About the Author

Ross Johnson, CPP - is the Senior Manager of Security and Contingency Planning for Capital Power, based in Edmonton, Canada. He served in the Canadian Forces as an infantry and intelligence officer for 24 years. Since leaving the service in 2001, he has been employed in several security-related leadership positions in aviation security, the offshore oil industry, and the electricity sector. He is also the infrastructure advisor for Awz Ventures of Toronto, Canada.

Ross is the author of Anti-terrorism Planning and Threat Response, a book on the prevention of terrorist attacks.

He is a member of the North American Electric Reliability Corporation's Critical Infrastructure Protection Committee, where he sits on the Executive Committee. He is also a member of the Electricity Information Sharing and Analysis Center's Physical Security Advisory Group.

He recently represented Canada on the Standards Drafting Team for the new critical infrastructure protection standard on physical security of large switchyards and substations.

Ross is also a Past-Chair of the Canadian Electricity Association's Security and Infrastructure Protection Committee, and Chair of ASIS International's Petrochemical, Chemical, and Extractive Industries Security Council. He is the current Chair of the Provincial Electricity Sector Physical Security Group, based in Alberta.

Ross can be contacted at rossintx@gmail.com.

Some material from this article appeared previously in the July 2016 newsletter of the ASIS International Utilities Security Council, of which Ross is a member.

Wildland Fire and the Infrastructure Interface

Lynn M. Johnston, MSc.
Forest Fire Research Specialist, Great Lakes Forestry Centre
Canadian Forest Service, Natural Resources Canada
Email: lynn.johnston@canada.ca

Abstract

This article presents some recent research focused on mapping wildland fire "interface" areas in Canada. These "interface" areas are stretches of forests or other burnable wildland fuels which are located near potentially vulnerable human-built structures or infrastructure. National maps of where these areas are located have not existed previously, and are necessary for community, industrial, and infrastructure resilience. Overall, Canada was found to have 116.5 million hectares of interface areas. These areas indicate the locations that fire suppression and mitigation activities would likely be necessary to protect the structures or infrastructure values from destruction by wildland fire. The interface maps are available for use in research or for a variety of applied uses.

I. BACKGROUND

Sparked by lightning or humans, wildfires (Fig. 1) in Canada burn more land than the area of Lake Ontario (> 2 million hectares) every year (CIFFC 2013). Though wildfires are a natural and necessary part of Canadian ecosystems, they can also cause significant destruction when they burn communities, industrial structures, or infrastructure. Wildland firefighting does provide some protection, but not all fires can be controlled and they can quickly devastate a community – for example what was seen in Slave Lake, Alberta in 2011 and again in Fort McMurray, Alberta in 2016 (Fig. 2).

Just accounting for the direct costs of suppression, evacuation, insurance, and recovery, the fires in Slave Lake came to over $1 billion (Flat Top Complex Wildfire Review Committee 2012). The direct costs of the Fort McMurray fire will likely end up being over $4 billion, taking place as the most costly insurable loss in Canada's history (exceeding the 2013 southern Alberta flooding and the 1998 Ontario/Quebec ice storm), and will also be among some of the most expensive wildfires in the world (Insurance Bureau of Canada 2015; Aon Benfield 2016). These types of fires may become even more of a concern in the future for two primary reasons: 1) human development is expanding further into wildland areas; and 2) it is anticipated that future wildfire activity will increase under climate change (Flannigan et al. 2009; Wang et al. 2015; Flannigan et al. 2016).

The fires in Slave Lake and Fort McMurray are both referred to as "wildland-urban interface" fires. The "wildland-urban interface" is the area of vegetated land which borders a community or isolated buildings (Fig. 3). Despite containing "urban" in the term, the wildland-urban interface does include isolated structures (e.g. Fig. 3b), cottages, reserves, and small communities that traditionally would not be considered "urban" areas. The vegetated land bordering these potentially vulnerable communities or structures may be any type of wildland fuel that can be burnt by a wildfire, including: forests, shrublands, and natural grasslands.

Fig. 1 Wildland fire in Canada. Photo: Lynn Johnston / Canadian Forest Service.

Fig. 2 Destruction due to wildfires in a) Slave Lake, Alberta and b) Fort McMurray, Alberta. Photo: (a) Mike Flannigan, University of Alberta; (b) Brian Wiens, Canadian Forest Service

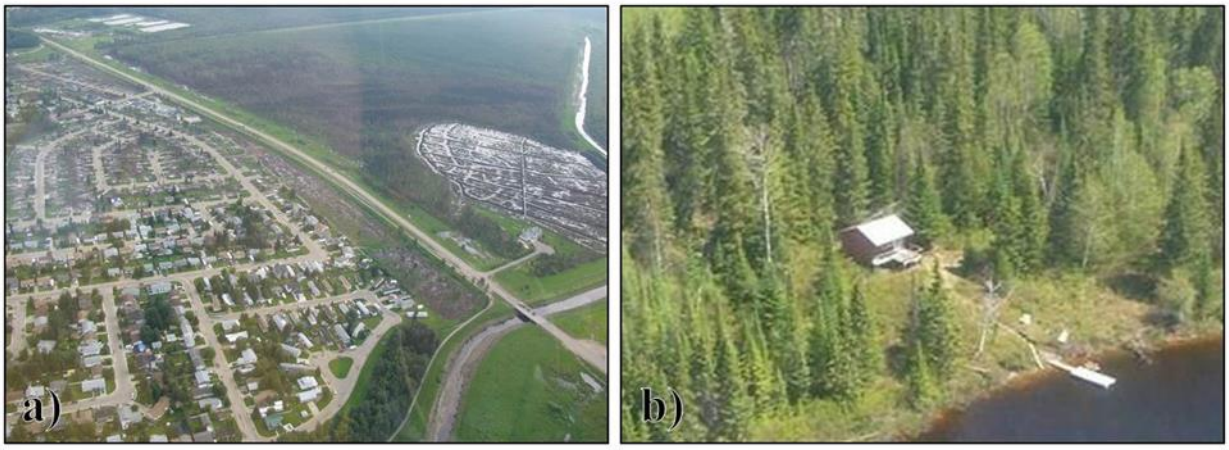

Fig. 3 Photos showing typical wildland-urban interface areas, with a) a community bordering a forested area, and b) an isolated cabin amongst a forested area. Photo: (a) Mike Flannigan, University of Alberta; (b) Jeremy Johnston, Ontario Ministry of Natural Resources and Forestry.

II. PROJECT OBJECTIVES

The wildland-urban interface has been mapped and studied in other areas of the world. In particular, in the United States there is a significant volume of information on interface areas (e.g. Radeloff et al. 2005; Caballero et al. 2007; Hammer et al. 2007; Theobald and Romme 2007; Zhang et al. 2008; Haas et al. 2013; Chuvieco et al. 2014; Thomas and Butry 2014; Fox et al. 2015; Martinuzzi et al. 2015). However, in Canada there is very limited information on this topic. The research project discussed here begins to address this knowledge gap by providing the first national map of wildland-urban interface areas for Canada.

This study also expands the concept of the wildland-urban interface to industrial structures (i.e. the "wildland-industrial interface") and potentially vulnerable infrastructure (i.e. the "infrastructure interface"). These novel concepts were introduced in this study to address the implications of the destruction of these industrial areas and infrastructure for firefighting, the economy, and our communities. Though generally there is priority placed on homes and community buildings (i.e. the wildland-urban interface), industrial structures and infrastructure often require fire protection when under threat from fire. In addition, to direct fire threat, industrial structures are also important from an economic standpoint; shutting down operations due to direct fire threat or evacuation of workers can quickly result in millions of dollars of lost revenue for a company and can affect local and even national economies. Infrastructure features are crucial during wildfire situations; for example, water and electrical shut downs can be a challenge for community protection, and roads can be important escape routes for communities or industry employees. Infrastructure features can also be a source of wildfires; railways can cause fires from the sparks created from trains or rail grinding, and human access along roads provides many opportunities for fire ignition.

This study produced three national interface maps: one for the traditional wildland-urban interface (focusing on homes, public and commercial buildings), one for the wildland-industrial interface (focusing on industrial structures related to oil and gas, mining, or other industrial operations), and one for the infrastructure interface (focusing on roads, powerlines, railways, and other infrastructure features).

III. METHODS FOR MAPPING THE INTERFACE

There are a wide variety of ways of defining and mapping interface areas (see Mell et al. 2010; Platt 2010). This study selected a fuels-focused definition of the interface areas, using a buffer around each potentially vulnerable feature. A brief summary of the methods used to map the interface will be covered here, but for more information see Johnston (2016).

Mapping the interface areas required data on both structures/infrastructure and on wildland fuels (Fig. 4a). Structure/infrastructure locations were taken from the CanVec+ (Natural Resources Canada 2015a) dataset, and each potentially vulnerable feature was included in calculations of the wildland-urban interface, wildland-industrial interface, or infrastructure interface, depending on if they were primarily urban/community features, industrial features, or infrastructure.

Relevant fuels data were extracted from the Land Cover circa 2000 (Natural Resources Canada 2015b) dataset. The fuels were then classified according to the relative fire hazard they may impart to structures (similar to the methods of Theobald and Romme [2007]). A "high hazard" fuel would be something like a continuous conifer forest, which can have potentially extreme fire behaviour and could

impart extreme fire risk to nearby structures. A "low hazard" fuel would be something like a sparsely vegetated shrub land, which has low potential for fire spread and would impart a much lower risk to nearby structures.

To produce the actual interface areas, a buffer of vegetated areas was calculated around each potentially vulnerable structure. The size and shape of the buffer was dictated by the type and arrangement of surrounding fuels. A large buffer (and therefore a large interface area) would be produced with higher hazard fuels, and smaller buffers (small interface areas) where there is less fuel or lower hazard fuels. The maximum distance the buffer could extend was limited to 2400 m[1]. Non-fuel areas were removed from the buffered areas, resulting in the final interface areas (Fig. 4b).

IV. MAPS

The national interface maps produced in this study are shown in Fig. 5. All three interface "types" (i.e. the wildland-urban, wildland-industrial, and infrastructure interface) are shown together in Fig. 5a. The three interface types do overlap quite a bit, and in total they cover 116.5 million ha, or 13.8% of the total land area of Canada. This is an area equivalent to almost twice the size of the province of Alberta. Individually, the wildland-urban interface covers 32.3 million ha (Fig. 5b), the wildland-industrial interface covers 10.5 million ha (Fig. 5c.), and the infrastructure interface covers 109.8 million ha (Fig. 5d).

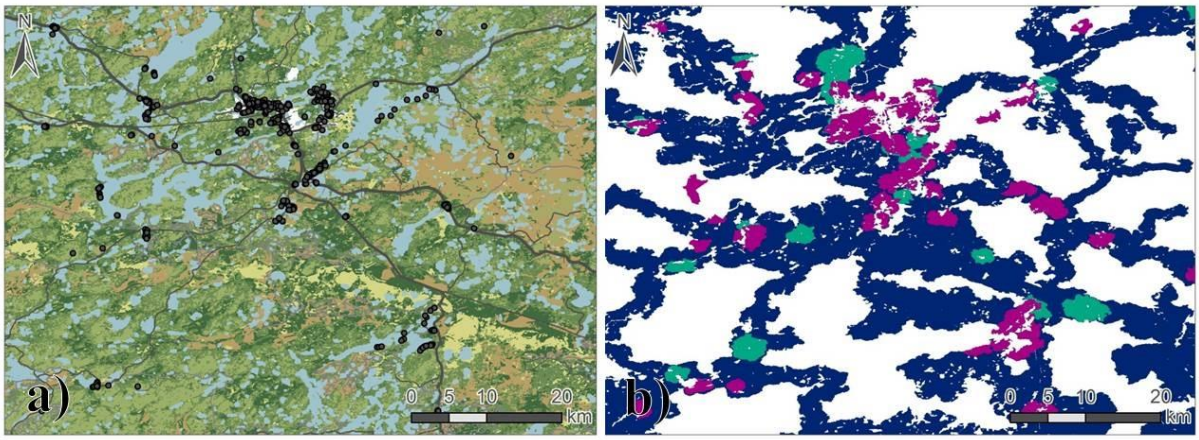

Fig. 4 Maps showing a) the data inputs; the fuels (greens, browns) and values (black), and also water is shown in blue; and image b) shows the wildland-urban interface (magenta, wildland-industrial interface (cyan), and infrastructure interface (navy)

[1] The maximum 2400 m buffer was used in this study for two reasons: 1) this is the most frequently used distance for interface mapping since it is the generally accepted distance an ember can travel from a wildland fire and ignite a structure (Radeloff et al. 2005; Hammer et al. 2007; Stewart et al. 2007; Theobald and Romme 2007; Zhang et al. 2008; Platt 2010; Bar-Massada et al. 2013; Thomas and Butry 2014), and 2) because the distance matches the intended scale and uses of the interface maps within fire management.

The areas indicated as "interface" may potentially be at risk from wildfire, though the maps do not indicate a full picture of fire risk. Risk requires much more information and considers both the probability and consequence of fires (Fried et al. 1999; Lein and Stump 2009; Haas et al. 2013; Chuvieco et al. 2014). The maps here simply indicate where, given the correct conditions, structures or infrastructure may be threatened by wildfire burning in nearby wildland fuel.

Following the population distribution of Canada, interface areas are more concentrated in the southern parts of the country, with generally more sparse areas to the north. Provincially, the provinces with the largest interface areas are Quebec, Alberta, Ontario, and British Columbia. These four provinces are also the most involved in fire management, with 80% of the money spent in Canada being within those four provinces (Stocks and Flannigan 2013). The eastern provinces of Nova Scotia, Prince Edward Island, and New Brunswick have much less fire activity and generally lower fire risk (Stocks et al. 2002), but a surprisingly high density of interface can be found in these areas. This result indicates that if these provinces have a fire, it is most likely going to be an interface fire.

Of past fires recorded in Canada from 1980-2014, many could be considered "interface fires". For the wildland-urban interface, 17% of all fires burnt in the country intersected, at least in small part, with a wildland-urban interface area, thus are considered wildland-urban interface fires. For the wildland-industrial interface, this value goes down to 6%, mostly due to the fact that there is less industrial area. For the much larger infrastructure interface, 38% of the fires were found to be infrastructure interface fires. Overall, many fires have burnt within interface areas, at times resulting in damage or destruction of structures and infrastructure. Despite the large number of human-caused fire ignitions near interface areas (Wotton et al. 2003; Price and Bradstock 2014), it appears effective fire detection and suppression has resulted in significantly lower[2] area burned within interface areas as compared to outside these areas.

V. Potential Applications

Practical applications of the interface maps include a variety of topics within wildfire management, wildfire mitigation, and long-term planning. The three interface maps can be used together or individually, and can be combined with other spatial information, depending on the needs of the application.

Wildfire management can benefit from the use of these maps to improve decision support activities when protecting communities, industrial structures, and critical infrastructure. Specific activities that may benefit include values protection, prepositioning of resources, and prioritizing fires.

Mitigating wildfires near communities, industrial structures, and infrastructure is very important and can reduce destruction of these values when a wildfire occurs. Wildfire mitigation planning applications of these interface maps include FireSmart activities (see www.firesmartcanada.ca), fuel treatments (i.e. removing or modifying wildland fuels to make firefighting easier and reduce fire risk), prescribed burning, improving building codes or municipal bylaws, industrial fire mitigation regulations, and infrastructure fire mitigation (e.g. railway fire prevention, powerline clearance, powerline or pipeline fire policy).

[2] For the wildland-urban interface, there is 4.0 times less fire inside wildland-urban interface areas vs. outside. For the wildland-industrial interface it is 2.0 times lower, and for the infrastructure interface it is 1.5 times lower.

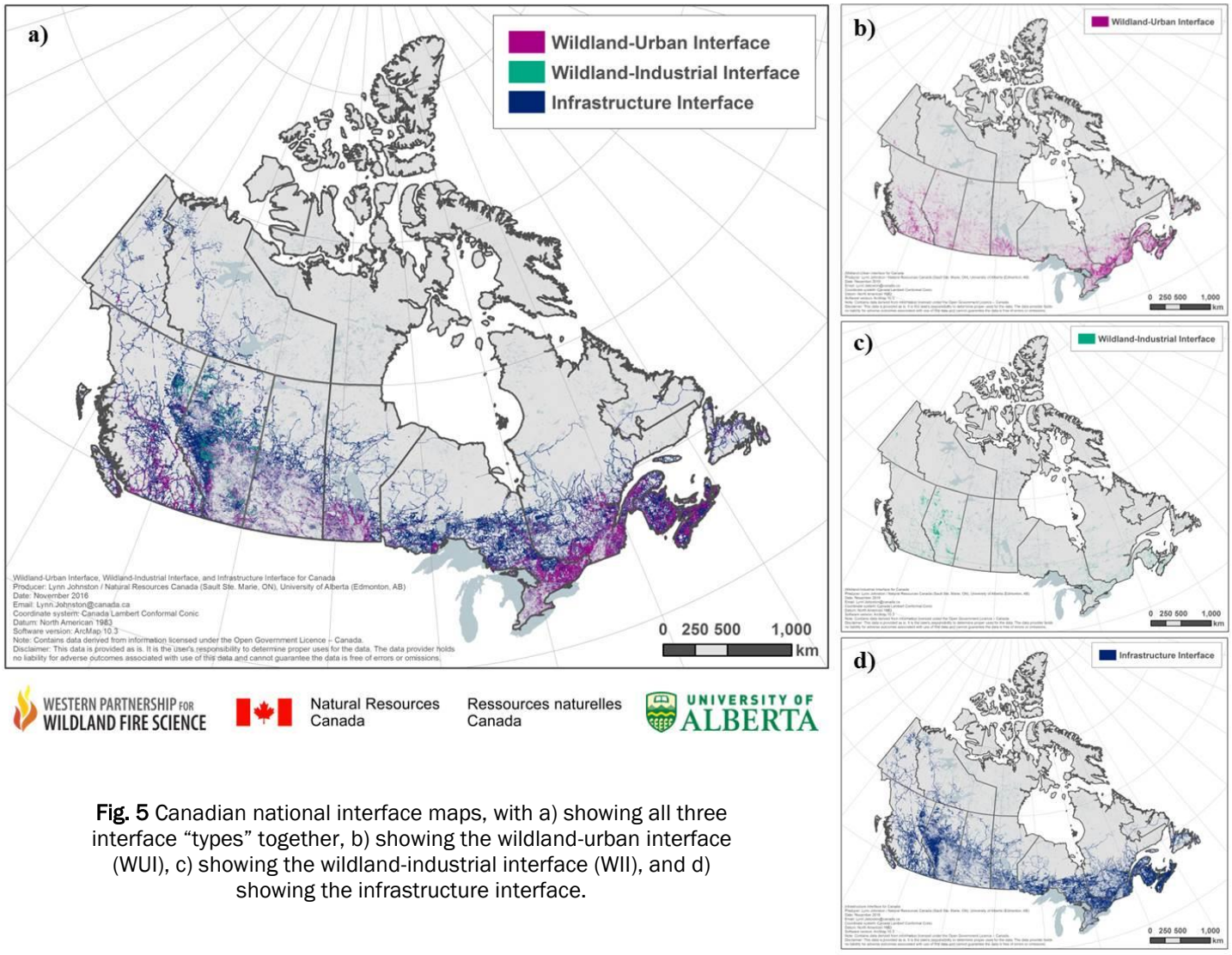

Fig. 5 Canadian national interface maps, with a) showing all three interface "types" together, b) showing the wildland-urban interface (WUI), c) showing the wildland-industrial interface (WII), and d) showing the infrastructure interface.

Long-term planning activities may benefit from the use of these interface maps. City planning and development could use the maps to improve community wildfire resilience by reducing the expansion of interface areas by using "infill development" (i.e. reducing fuel areas and filling in areas that are already "interface"), or limiting growth in areas that would create new areas of interface. Insurance companies may also be interested in this type of information as part of a larger-scale risk assessment or implementing insurance rebates (e.g. for implementing FireSmart principals). Individually, the infrastructure interface map has a variety of long-term planning applications, including: 1) railway policy and planning activities, such as limiting rail grinding activities near interface areas when fire hazard is high; 2) policy involving fire mitigation or fuel clearance around pipelines/powerlines; 3) evacuation planning; and 4) pipeline/powerline shutoff policy during wildfire events.

VI. Conclusion

The results of this study show that Canada has a substantial amount of interface area. This area has the potential to be at risk when a wildfire occurs, and would likely require firefighting action when a fire is approaching. These interface areas should also be considered priority areas for risk assessment and fire mitigation activities.

The maps produced here are available for use in research or applied purposes. Overview maps for general interest (e.g. Fig. 5), higher resolution maps, or the full resolution data are available upon request (contact the author).

In Canada, we have very effective fire suppression capabilities, and many communities, industrial structures, and critical infrastructure have been saved from destruction due to quick detection and suppression of wildfires. However, it is not possible to stop every fire that threatens values. Having the best tools and information for improved resilience of our communities, industries and infrastructure is crucial.

.

The research discussed here is ongoing, with future work to include map updates (e.g. are more detailed/recent input data becomes available), mapping risk within interface areas, and predictions of the growth of the interface in the future.

About the Author

Lynn JOHNSTON is a Forest Fire Research Specialist with the Canadian Forest Service at the Great Lakes Forestry Centre in Sault Ste. Marie, Ontario. She has worked with the CFS since 2007 on a variety of wildland fire topics, including fire behaviour, fire risk, and fire and climate change.

Lynn obtained a BSc. at the University of Guelph in 2007, and recently completed her MSc. at the University of Alberta in Forest Biology and Management, focusing on wildland fires.

References

Aon Benfield (2016) Global Catastrophe Recap. Aon Benfield. 15 pgs. Available at http://thoughtleadership.aonbenfield.com/Documents/20160608-ab-analytics-if-may-global-recap.pdf [Accessed June 21, 2016].

Bar-Massada, A, Stewart, SI, Hammer, RB, Mockrin, MH, Radeloff, VC (2013) Using structure locations as a basis for mapping the wildland urban interface. *Journal of Environmental Management* **128**, 540-547. DOI: 10.1016/j.jenvman.2013.06.021.

Caballero, D, Beltrán, I, Velasco, A (2007) 'Forest fires and wildland-urban interface in Spain: types and risk distribution' IV Conferencia Internacional sobre Incendios Forestales. Seville, Spain.

Chuvieco, E, Aguado, I, Jurdao, S, Pettinari, ML, Yebra, M, Salas, J, Hantson, S, De La Riva, J, Ibarra, P, Rodrigues, M, Echeverria, M, Azqueta, D, Roman, MV, Bastarrika, A, Martinez, S, Recondo, C, Zapico, E, Martinez-Vega, FJ (2014) Integrating geospatial information into fire risk assessment. *International Journal of Wildland Fire* **23**, 606-619. DOI: 10.1071/WF12052.

CIFFC (2013) CIFFC Canada Report 2013. Canadian Interagency Forest Fire Centre Inc. Available at http://www.ciffc.ca/images/stories/pdf/2013_canada_report.pdf [Accessed July 17, 2015].

Flannigan, M, Wotton, B, Marshall, G, de Groot, W, Johnston, J, Jurko, N, Cantin, A (2016) Fuel moisture sensitivity to temperature and precipitation: climate change implications. *Climatic Change* **134**, 59-71. DOI: 10.1007/s10584-015-1521-0.

Flannigan, MD, Krawchuk, MA, de Groot, WJ, Wotton, BM, Gowman, LM (2009) Implications of changing climate for global wildland fire. *International Journal of Wildland Fire* **18**, 483-507. DOI: 10.1071/WF08187.

Flat Top Complex Wildfire Review Committee (2012) Flat Top Complex. 95 pgs. Available at http://wildfire.alberta.ca/wildfire-prevention-enforcement/wildfire-reviews/documents/FlatTopComplex-WildfireReviewCommittee-A-May18-2012.pdf [Accessed July 4, 2016].

Fox, D, Martin, N, Carrega, P, Andrieu, J, Adnès, C, Emsellem, K, Ganga, O, Moebius, F, Tortorollo, N, Fox, E (2015) Increases in fire risk due to warmer summer temperatures and wildland urban interface changes do not necessarily lead to more fires. *Applied Geography* **56**, 1-12. DOI: 10.1016/j.apgeog.2014.10.001.

Fried, JS, Winter, GJ, Gilless, JK (1999) Assessing the benefits of reducing fire risk in the wildland-urban interface: A contingent valuation approach. *International Journal of Wildland Fire* **9**, 9-20. DOI: 10.1071/WF99002.

Haas, JR, Calkin, DE, Thompson, MP (2013) A national approach for integrating wildfire simulation modeling into Wildland Urban Interface risk assessments within the United States. *Landscape and Urban Planning* **119**, 44-53. DOI: 10.1016/j.landurbplan.2013.06.011.

Hammer, RB, Radeloff, VC, Fried, JS, Stewart, SI (2007) Wildland–urban interface housing growth during the 1990s in California, Oregon, and Washington. *International Journal of Wildland Fire* **16**, 255-265. DOI: 10.1071/WF05077.

Insurance Bureau of Canada (2015) Facts of the Property and Casualty Insurance Industry in Canada 2015. Insurance Bureau of Canada (IBC). 68 pgs. Available at http://assets.ibc.ca/Documents/Facts%20Book/Facts_Book/2015/FactBook-2015.pdf [Accessed June 21, 2016].

Johnston, Lynn M. (2016) Mapping Canadian Wildland Fire Interface Areas. MSc thesis. Department of Renewable Resources. University of Alberta. 161 pgs. doi: 10.7939/R3GT5FR9Z

Lein, JK, Stump, NI (2009) Assessing wildfire potential within the wildland–urban interface: A southeastern Ohio example. *Applied Geography* **29**, 21-34. DOI: 10.1016/j.apgeog.2008.06.002.

Martinuzzi, S, Stewart, SI, Helmers, DP, Mockrin, MH, Hammer, RB, Radeloff, VC (2015) The 2010 wildland-urban interface of the conterminous United States. Research Map NRS-8. U.S. Department of Agriculture, Forest Service, Northern Research Station, Newtown Square, PA. 124 pgs. Available at http://www.fs.fed.us/nrs/pubs/rmap/rmap_nrs8.pdf [Accessed July 4, 2016].

Mell, WE, Manzello, SL, Maranghides, A, Butry, D, Rehm, RG (2010) The Wildland-Urban Interface Fire Problem Current Approaches and Research Needs. *International Journal of Wildland Fire* **19**, 238-251. DOI: 10.1071/WF07131.

Natural Resources Canada (2015a) CanVec+. Dataset. Used under the Open Government Licence - Canada. (EaSS GeoGratis Client Services. Natural Resources Canada, Canada Centre for Mapping and Earth Observation). ftp://ftp2.cits.rncan.gc.ca/pub/canvec/archive/canvec+_archive_20151029/doc/CanVec+_en_release_notes.pdf.

Natural Resources Canada (2015b) Land Cover, circa 2000 - vector. Dataset. Used under the Open Government Licence - Canada. (EaSS GeoGratis Client Services. Natural Resources Canada, Canada Centre for Mapping and Earth Observation). www.GeoGratis.gc.ca.

Platt, RV (2010) The Wildland- Urban Interface: Evaluating the Definition Effect. *Journal of Forestry* **108**, 9-15.

Price, O, Bradstock, R (2014) Countervailing effects of urbanization and vegetation extent on fire frequency on the Wildland Urban Interface: Disentangling fuel and ignition effects. *Landscape and Urban Planning* **130**, 81-88. DOI: 10.1016/j.landurbplan.2014.06.013.

Radeloff, VC, Hammer, RB, Stewart, SI, Fried, JS, Holcomb, SS, McKeefry, JF (2005) The wildland-urban interface in the United States. *Ecological Applications* **15**, 799-805.

Stewart, SI, Radeloff, VC, Hammer, RB, Hawbaker, TJ (2007) Defining the wildland-urban interface. *Journal of Forestry* **105**, 201-207.

Stocks, BJ, Flannigan, M (2013) Chapter 4: Current Fire Regimes, Impacts and the Likely Changes – I: Past, Current and Future Boreal Fire Activity in Canada. *In* 'Vegetation Fires and Global Change: Challenges for Concerted International Action. A White Paper directed to the United Nations and International Organizations.' (Ed. JG Goldammer.) pp. 39-50. (Kessel Publishing House: Germany).

Stocks, BJ, Mason, JA, Todd, JB, Bosch, EM, Wotton, BM, Amiro, BD, Flannigan, MD, Hirsch, KG, Logan, KA, Martell, DL, Skinner, WR (2002) Large forest fires in Canada, 1959-1997. *Journal of Geophysical Research* **107/108(print)**, 8149.1-8149.12. DOI: 10.1029/2001JD000484.

Theobald, DM, Romme, WH (2007) Expansion of the US wildland-urban interface. *Landscape and Urban Planning* **83**, 340-354. DOI: 10.1016/j.landurbplan.2007.06.002.

Thomas, DS, Butry, DT (2014) Areas of the US wildland–urban interface threatened by wildfire during the 2001–2010 decade. *Natural Hazards* **71**, 1561-1585. DOI: 10.1007/s11069-013-0965-7.

Wang, X, Thompson, DK, Marshall, GA, Tymstra, C, Carr, R, Flannigan, MD (2015) Increasing frequency of extreme fire weather in Canada with climate change. *Climatic Change* **130**, 573-586. DOI: 10.1007/s10584-015-1375-5.

Wotton, BM, Stocks, BJ (2006) Fire management in Canada: vulnerability and risk trends. *In* 'Canadian Wildland Fire Strategy: Background Synthesis, Analysis, and Perspectives.' (Eds K Hirsch, P Fuglem.) pp. 49-55. (Canadian Council of Forest Ministers. Natural Resources Canada, Canadian Forest Service, Northern Forestry Centre: Edmonton, Alberta).

Zhang, Y, He, HS, Yang, J (2008) The wildland-urban interface dynamics in the southeastern U.S. from 1990 to 2000. *Landscape and Urban Planning* **85**, 155-162. DOI: 10.1016/j.landurbplan.2007.11.007.

Social Media Monitoring As An Effective Tactic to Counter Social Activism

Doug Powell, CPP, PSP

I. INTRODUCTION

A paradigm shift has taken place, world-wide with respect to the manner in which votes are cast and approvals are given for natural resource development and energy sector projects. Most often referred to as "the new reality", it can be simply described as a shift in societal acceptance and tolerances for controversial projects, usually referencing the environment as the primary concern. Controversy has always been shaped by societal norms, but the new shift seems to be taking us beyond reasoned debate and due process to something like an adhoc political system. The "adhoc" nature of the protest vote refers specifically to a social empowerment where opposition to any issue, for any reason seeks out iconic leadership to coalesce a variety of social concerns and ills for the purpose of non-political, direct action. Indeed, if the political system worked the way it is intended (acknowledging that politics by nature is imperfect), the popular vote would govern the day, and those in opposition would always maintain a diligent, but respectful opposition based on political views, ideologies and differences of opinion. The party holding the majority would, through popular support, good government and/or effective compromise, guide a system of public hearings, academic and expert input, judicial process and good old-fashioned debate in order to move all national interests forward on behalf of the electorate. And, it is reasonable to assume this happens, every day. However, this system is only one of two systems in effect today relevant to natural resource project approvals in recent history.

The "protest vote" is not unique to North American culture, is not unique to natural resource development, and is not uncommon in a variety of settings. Much like union organization over the decades, too, protest has helped to call attention to many social injustices, human rights issues, environmental concerns, inhumane acts and a variety of other social concerns; and rightfully so. Even protest that failed to end particular concerns ultimately brought attention to issues and created meaningful social shifts to correct imbalances or change social norms. While protest has erupted over the centuries in the form of wars, uprisings, strikes, solidarity movements, riots and a variety of other newsworthy and compelling actions, the protest movement today, as it pertains to natural resource development, seems to have shifted yet again to something more like a new political vote. This new adhoc political process has contributors like NIMBY (Not In My Back Yard) and BANANAS (Build Absolutely Nothing Anywhere Near Anything (Anyone) and CAVE (Citizens Against Virtually Everything). The protest movement generally seems to have morphed into something far more general and wider reaching than these isolationist perspectives.

II. RESOURCE-BASED INDUSTRY PROJECT APPROVALS

A reasoned opinion about government process, in democratic society at least, is that due process rules the day. It may not be perfect, but it allows for disparate opinions, educated discourse, opposing ideology and varying theories to come together in ways that provide for effective decision-making by those elected and/or appointed to make the decisions they are authorized to make. Yet, despite years of review process and judicial oversight, once approval is given to any project, protest has become the next layer of "approvals" needed before industry can commence to deliver what the legal process has granted them the rights to do. It is fair to say that regulatory approvals for any resource-based project should always be subject to review and accountable to deliver that which was approved, with all conditions applied. The application of the protest vote, however, is now adding

layers of cost, legal processes, schedule delays and project-related concerns for those working in this new reality. Whether one agrees or disagrees with the protest voice most prevalent on any issue, it is a common and consistent project risk that now requires careful planning in order to effectively mitigate it.

III. MANAGING SECURITY RISK FOR RESOURCE-BASED PROJECTS

The New Global Focus

Managing security risk for planned energy projects requires having a comprehensive understanding of those involved in the global environmental movement. The journey to understanding the full protest risk picture begins with understanding who the stakeholders are at the local level and their concerns and grievances. Ultimately, while resource-based projects come under the larger, more socially acceptable environmental protest movement, First Nations (FN) issues are now becoming equally prevalent for a number of important reasons (unceded lands, consultation and negotiation requirements, land claims issues, land use issues, etc.), which encompass environmental stewardship as FN stakeholders hold themselves out to be stewards of the water and land in many protest actions. As a result, these two more established movements are often front and centre in most energy sector project debates. When environment and FN issues are not front and centre, there is a tendency for smaller, less recognized groups to seek an environmental or FN focus to oppose energy development projects in order to have a more stable platform for their own grievances. For example, private land owners, anarchists, anti-government groups, NIMBYs and BANANAs will often coalesce under an environmental or FN support banner in order to give legitimacy to their grievances, and to be part of a more sustained and well-funded protest process. So, managing the protest risk relies on understanding all the players and how they are connected even before the resource project begins.

Understanding the Actors

Knowing where local protest entities will potentially derive support requires understanding who they are talking to and who is talking about the project. Therefore, it is important that those managing critical infrastructure risks understand that successful protest, protest culture and direct action against any project has a proportional relationship to presence in social media, mainstream media and web-based content. In order to fully understand and appreciate any protest potential and protest impacts, a social media monitoring and analysis requirement is necessary in order to define the risk and plan mitigation. Sufficient experience has been acquired that we know well how protest power bases can speak into issues globally with effect. This is true for US-based, European and Canadian protest entities, etc. Just as in business, those with profile and a good financial base can dominate the world stage. Resource-based projects in the most remote parts of the planet are no longer immune from mainstream protest. One individual in close proximity to any project (including the workers at the project), can initiate global awareness and ignite protest activity via social media with a little persistence. Once initiated, a general call for support over social media can bring together disparate "concerned" protest voices whether or not they have any relationship to the primary cause of protest, in order to increase the voice and "virtual" presence of the protest focus. A local concern over a river can easily accommodate additional protest concern over land use, animal rights, FN interests, human rights and a variety of other "insert name here" interests. Gone are the days when one, lone protest voice needed to write hundreds of letters to government leaders, news outlets and advocacy groups to get support. A well placed social media broadcast can often ignite entire virtual communities for global support. That support can come in many forms, including: branding (giving the protest movement a theme), labeling (environmental, FN, poverty, etc.), petitioning, fund raising, rallies (in communities far and removed from the project site), activism, media canvassing, etc.

Monitoring Social Media for Great Understanding

To monitor and mine social media in order to understand and manage protest potential is a necessary function of protection planners today. Even understanding who the identified leaders are within the

protest community allows companies to engage these individuals and groups openly and publicly to hear their concerns and attempt to share information to defray some of the more heated protest. Engaging protest groups to separate the various interests and work with them individually is a good, proactive strategy at times. In many instances, protest movement is supported by an uneducated media who, for various reasons will print stories that promote additional unrest. This is accomplished by writing the protest side of the story and not providing equal time for the company to speak to the issues. Protest entities will often speak from a position of worst case or worst fear in order to garner support and elevate their concerns. Media coverage on this basis will likely reach more members of the public because of the sensationalistic aspect of the story. Controversy sells news! An effective strategy for companies facing protest is to understand the protest messaging and issue their own messages, buying air time on television and radio, if necessary, to promote project benefits, to discuss the regulatory process that led to required approvals, and to counter false or misleading information from protest entities by putting facts in front of the public. This tact requires careful and studied media monitoring in order to assess priority messaging and target audiences. Certainly, more reasoned individuals will always filter out sensationalism and extremist viewpoints, and not all protest rhetoric need be countered.

Assessing Actor Capabilities

Assessing protest entities as adversaries in security management is also important. We also know from history that some entities have used dangerous and deadly tactics to further their causes. Opportunists bent on extremism will at times grab onto protest issues in order to further their own malevolent behavior or to usurp the protest platform for ideological reasons. Thankfully this is rare, but needs to be factored into protest environments where more heated opposition is prevalent. Looking for these extremists amidst the protest environment requires some skilled research, assessment and study. In bigger stakes projects where very high risk is involved, extremism and terrorism (even domestic terrorism) needs to be considered. Social media monitoring, to assess main actors, hangers on and player association, including dark web activity are required in order to draw a full picture of the project security risk. As a word of caution, this includes filtering out those who posture as extremist, but are only living out an alter-ego as part of their virtual existence on line. These individuals may incite extremist behavior, but are not themselves active in this area.

Once the players are well understood (and sometimes this evolves over time), capabilities of the actors can be determined. There is a big difference between a protest that continually calls for support (money, food, boots on the ground, etc.) and entities that are well known to have deep war chests, proven tactics and many resources when they enter into the protest climate. There is a huge difference between local land owners opposed to a project who want to have their discontent understood, and militant groups who chain themselves to gas valves and work to intimidate company executives and workers. Understanding tactics and capabilities leads to an effective means to mitigate more extreme protest potential.

In addition to social media monitoring, there are many online web-based resources as well as published materials and industry experts who have compiled thousands of pages of background information and historical references about protest movements, protest entities and protest tactics. Having this type of information and the skill set to accumulate and understand it is an important component of security planning in the current social climate. It is unlikely that any resource-based project today has a unique protest associated with it. Since protest entities evolve and learn from one another, an important counter-measure for industry is to also understand that historical component and evolution, and how it has been impacting industry over the past decade, at least.

IV. ADAPTING AN EFFECTIVE MEDIA MONITORING MODEL

Once a company has determined the need for effective information and intelligence gathering, a means to accomplish this need is the primary focus. Few companies have the resources or skills needed to build in-house social media and web monitoring. While it is true that many individuals or business groups (like a corporate communications department) already provide some media filtering services, the deeper dive, broader application of monitoring, especially the experience needed to overlay monitoring with good analysis, is not readily available. External agencies have begun to offer this solution for a fee. Like all services, vendor capability can be quite varied. If a company elects to go with a third party solution for media monitoring, it will be very important to vet the supplier and seek out samples of their work product, as well as to contact vendor references to understand how the product is perceived and utilized by others. Like all services, the better ones cost more money. So, it may be more appropriate for most companies to seek out good analysis only at times when the threat level is higher or when particular situations require more focused attention on the protest community. It may also be effective to "sample" social media from time-to-time just to understand who is saying what, and where most of the focus and attention of various protest entities are. Like a health check-up, a comprehensive report, periodically, delivered by a competent resource should become part of the company's regular business updates, even in times of relative calm, and should also formulate part of the executive team and Board reporting periodically since it responds to key company risks. Additionally, seeking out this type of analysis reporting in the midst of a crisis is important, but seeking it out and using it to plan security risk mitigation far in advance of any project or conflict is an important part of security planning.

Police and Intelligence Community Information Sharing

Looking to the police and intelligence community for this kind of help has some benefit. It is unrealistic to think that the policing community or the intelligence community has the resources, the time or the inclination to serve industry with ongoing social media and web monitoring services. It is true that valuable relationships need to be fostered and formed between industry and policing agencies in order to share critical information at critical times, and for ongoing threat environment awareness. These two communities (industry and policing) are good examples of entities that can perform better when some symbiosis exists. However, they are hard-pressed to serve one another's day-to-day interests and this has been proven out in many instances. While this article advocates a continued path toward more open, meaningful and deliberate sharing of information between industry and policing agencies, the path forward is challenging and has several more hurdles to clear before it can become a reliable replacement for comprehensive social media monitoring services. Such a forum should definitely form part of the supplemental sharing for industry and police, and maintaining effective liaison relationships is critical for both in the present security environment. Better relationships are needed to ensure better understanding of each other's issues and limitations when it comes to addressing protest, activism, terrorism and other interdictions. Almost as a second imperative to good social media and web monitoring, police and intelligence community relationship for industry has become integral to the industry security plan, and vice versa.

Academic Institutions Opportunities

Interestingly, one voice in this area of endeavor has begun to raise itself in the ongoing national dialogue on intelligence services and information dispensing, and for very good reason. Academia is offering another viewpoint and option for these services. This voice is a reasoned one, although no less cumbersome to get traction than the relationship with police and intelligence communities. But even on the surface, this idea makes sense. Schools of study already exist for the national security, intelligence services and similar academic endeavor. Universities are extended communities of accomplished researchers that openly share information for the purpose of further study and

advancing ideas. Universities build environments where information can be stored, analyzed and manipulated for new and important results to take shape. Academics are paid to ponder ideas, research, and write on particular specialized areas of focus and study. Universities provide an environment where anyone can join in dialogue, debate, study and topical discourse. Laboratories can be set up and torn down in quick order using proven methodologies, with skilled technical resources guiding this work. Universities provide a staging area for information gathering, creative analysis, information dispensing, and other opportunities and products that are not readily available in industry or government. There is a reason why industry and government continually turn to academic institutions to lead or guide new research and to problem-solve in complex situations. So, perhaps turning this into an environment for information management, including study for the purposes of better social media and web-based monitoring, in particular for good analysis, is a very good idea to pursue.

There are challenges to be overcome. While academic institutions may very well be able to provide comprehensive reporting on protest and activism in a manner that assists industry to plan defensive measures and pre-emptive tactics, providing industry with information from industry security databases so as to help facilitate meaningful information gathering and analysis may be no less problematic for industry than it is to facilitate police agency sharing. In order for industry to agree to provide raw data reporting to an academic institution, even if the institution is a think tank or dedicated working group within the academic institution, a process for confidential data transfer, as well as for data storage and handling is needed before industry will sign onto the sharing process full scale. There are two key factors at play, here. Industry will not readily share information that has the potential to impact the reputation of the organization if leaked, or has the potential to otherwise negatively impact profit or share-holder value. Naming security incidents and actors involved have these potentials in some instances and the inadvertent release of information like this would be embarrassing to the owner of the information if not strategically ill-advised. One area where policing agencies somewhat trump academic institutions is in the ability to keep information secret in most cases. If the academic partner(s) in such arrangements are able to build a system of anonymity for data received without jeopardizing the integrity of the information conveyed, then this would solve most of the problem.

Challenges with the Academic Model

If information sharing and protection protocol can be successfully addressed, including an impressive program for protecting IT systems and data storage, records, etc., then without a doubt, academic think tank type information and intelligence environments could be the answer to more far-reaching and comprehensive information analysis and reporting, in addition to research in this important area. Nothing in this model prevents law enforcement from also having some kind of stake in the game, either. In fact, there is opportunity for additional symbiosis between policing, intelligence and academic facilitation in this concept. Funding can also become much more available to schools that specialize in this area. There is opportunity for ongoing financial support in a number of areas, including payment for special reports, journals, commissioned research, consulting services, etc., as well as subscription based services for routine weekly, monthly, quarterly and annual analysis reporting and similar research-based products. There is also opportunity to engage industry at a higher management level than the security group. Executive level players might be more readily amenable to receiving information from credible universities and think-tank groups, and to supporting that output than to supporting, for example, private institutions laboratories and working groups. Engaging the executive in this type of dialogue can influence decisions about security planning and funding, overall.

The notion of an academic intermediary, with a research and analysis base, being the purveyor of information and intelligence products seems to have a number of positive if not exciting opportunities for companies in the resource sector. In fact, this concept is not a new one and is already successfully applied in

the United States and the United Kingdom as examples where the academic community has stepped in to fill a need where industry and government have been encumbered in their efforts to create a meaningful information sharing practice. Canadian entities working to the same end can also learn from our economic partners and international allies and even improve on something that already works.

V. SUMMARY

Industry operates, today in an era where public opinion – not to be confused by popular opinion – has adapted social media very effectively to support social activism and protest. The energy sector is under close scrutiny in all it does. Regulatory approval process is costly and time intensive. Achieving government approval for large-scale natural resource projects is taxing and does not come with any guarantee of success. The new paradigm, however, is that even with that approval in place, the hurdles associated with beginning and completing projects now requires another form of approval which plays out in the very public protest-charged arena of activist participation. Companies now need to plan and prepare their project teams for work to take place in that environment which can run the full spectrum from peaceful demonstration to planned and coordinated attacks. In this environment, project success is at risk, but most importantly, so are lives as the safety of workers becomes a leading concern.

Industry can apply many proven defensive strategies to their security planning, and there are many experts who have already worked successfully in this environment who can be important resources to security leaders today. Equally important is knowing who is in opposition to any given project, tracking their involvement and understanding the capabilities and tactics of these opponents. For this purpose, social media and web-based monitoring is valuable for a variety of reasons. Developing or acquiring this kind of analysis and reporting is also challenging, but many companies are already finding success in this area. Developing professional networks that can help direct information sourcing is also important. In every respect, good information leading to effective intelligence is likely the most valuable tool security practitioners have to combat the protest environment today. To this end, while policing and intelligence agencies working closely with industry has tremendous benefits, there is also an opportunity to develop an academia focused solution by utilizing schools of focused study, research and reporting to address information sharing and intelligence reporting related to protest and activism. Certainly, having an academic solution to information sharing and intelligence services makes a lot of sense for a variety of reasons. This idea is well worth exploring given successful think-tanks providing this service are already in place globally. Industry and policing will certainly benefit in the end with better information and solutions being brought forward by dedicated experts using an academic focus for analysis and research output reporting. The stakes for resource-based industry projects are high. A studied tactical response is now required to counter the risk presented.

About the Author

Doug is a security professional with more than 34 years' experience managing security, and considered an expert, internationally, in several disciplines. Doug has worked for BCH since 2006 where he has managed critical infrastructure security through three major projects: the 2010 Winter Olympics; smart grid deployment; and, presently with the Site C dam construction. Doug demonstrates leadership serving professional committees and organizations, internationally. Doug has served ASIS International as a Council Vice President and as Chair of the Critical infrastructure Working Group. Doug was also 2nd Vice-Chair of the Utilities Security Council of ASIS. Doug has served with IRRG since 2014 as an advisor to the organization and on the Steering Committee for IRRG's *International Urban Security & Resilience Conference*.

Doug holds two professional security certifications, Certified Protection Profession (CPP) and Physical Security Professional (PSP).

Doug is an accomplished speaker and educator, internationally, and has authored 15 white papers, as well as having several articles published in professional journals. Doug has won awards, including *CSO of the Year* (2010), *Security Program of the Year* (2011) and was named recipient of the prestigious ASIS *Roy Bordes Award* for volunteer leadership in 2017.

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*

"Canadian Security Intelligence Service Public Report " 2014-2016 (Ottawa: February 2017) https://www.csis-scrs.gc.ca/pblctns/nnlrprt/2014-2016/index-en.php#cyber

Report: Counterterrorism Yearbook 2017 (Australian Strategic Policy Institute) The ASPI Counterterrorism Yearbook 2017 (8.8 MB) is freely accessible at: https://www.aspi.org.au/publications/counterterrorism-yearbook-2017

Tiered Response Pyramid: A System-Wide Approach to Build Response Capability and Surge Capacity, by Joseph W. Pfeifer & Ophelia Roman. Homeland Security Affairs Vol. 12, Article 5 (December 2016) https://www.hsaj.org/articles/13324

National Cyber Crisis Management: Different European Approaches, by Sergei Boeke http://onlinelibrary.wiley.com/doi/10.1111/gove.12309/abstract

Unpacking and Exploring the Relationship Between Crisis Management and Social Media in the Era of "Smart Devices", by Eric K. Stern. Homeland Security Affairs Vol. 13 (June 2017). The Journal of the NPS Center for Homeland Defense and Security, Cyber Journal 12 https://www.hsaj.org/articles/13986

Cyber Journal 12, Edition 12 (October 2017) https://www.cse-cst.gc.ca/en/node/2287/html/28058

Threat Assessment – The cyber threat against Denmark. Threat Assessment Branch under the Centre for Cyber Security (January 2016). https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20%20The%20cyber%20threat%20against%20Denmark.pdf

The NHS trusts and hospitals affected by the Wannacry cyberattack. WIRED. By Victoria Woollaston, 15 May 2017. http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack

Russian World-Views - Domestic power play and foreign behaviour. Highlights from the Workshop =-*World Watch: Expert Notes* series publication No. 2017-06-02 https://www.csis.gc.ca/pblctns/wrldwtch/2017/2017-06-15/20170615-en.php?=undefined&wbdisable=true

What Comes After Daesh? Highlights from the Workshop. World Watch: Expert Notes series publication No. 2017-05-01 https://www.csis-scrs.gc.ca/pblctns/wrldwtch/2017/2017-05-09/What-comes-after-daesh_report_EN.pdf

New Federal Government Space Weather Website and Document Repository Launched, by Michael Bonadonna, Seth Jonas, and Erin McNamara (November 2017), Space Weather, Vol. 15, Issue 11 doi:10.1002/2017SW001746. http://onlinelibrary.wiley.com/doi/10.1002/2017SW001746/full

Extreme Events in Geospace: Origins, Predictability, and Consequences, by Natalia Buzulukova. Oxford, United Kingdom: Elsevier. https://www.elsevier.com/books/extreme-events-in-geospace/buzulukova/978-0-12-812700-1

The challenge posed by geomagnetic activity to electric power reliability: Evidence from England and Wales, by Kevin F. Forbes and O. C. St. Cyr (October 2017). Space Weather, Vol. 15, Issue 10. http://onlinelibrary.wiley.com/doi/10.1002/2017SW001668/abstract?campaign=agupersonalchoice

State-of-the-art research on electromagnetic information security, by Yu-ichi Hayashi. Radio Science, 51(7), doi:10.1002/2016RS006034. http://onlinelibrary.wiley.com/doi/10.1002/2016RS006034/full

***The future of Russian Gas Exports, Economics of Energy & Environmental Policy**, by* Finn Roar Aune, Rolf Golombek, Arild Moe, Knut Einar Rosendahl and Hilde Hallre Le Tissier, Volume 6, Number 2, September 2017, pp 111-136.

How does Canada Respond to Stranded Asset Risk, by Amy Myers Jaffers. The Global Exchange, Special Edition: Energy Series 2017, pp 18-22.

Understanding the Shift in Energy Security, by Petra Dolata. The Global Exchange, Special Edition: Energy Series 2017, pp 23-25.

Big Projects, Big Politics, Big Policy: Strengthening Public Confidence in Energy Decision-making in Canada, by Monica Gattinger. The Global Exchange, Special Edition: Energy Series 2017, pp 26-29.

With the latest Developments on the North American Pipeline Landscape, is Energy East Necessary? By Kelly J. Ogle, The Global Exchange, Special Edition: Energy Series 2017, pp 30-35.

Can Canada Restore a Functional Regulatory Process for Major Infrastructure Projects? By Dennis McConaghy, The Global Exchange, Special Edition: Energy Series 2017, pp 36-42.

Energy as a Service: Going Beyond Energy Supply, by Normand Mousseau. The Global Exchange, Special Edition: Energy Series 2017, pp 43-46.

More Hydro Power in Canada: Tapping our Potential, by John Haffner and Jim Burpee. The Global Exchange, Special Edition: Energy Series 2017, pp 51-54.

What Will Happen if Gazprom Stops Transiting Gas Across Ukraine? By Robert E. Brooks, IAEE Energy Forum, First Quarter 2017, pp 23-26.

Energy Efficiency and Jobs – a case Study of Israel, by Ulrike Lehr, Anke Moning, Rachel Zaken and Edi Bet-Hazadi. IAEE Energy Forum, First Quarter 2017, pp 27-29.

Spatial Dependence in State Renewal Policy: Effects of Renewable Portfolio Standards on Renewable Generationwithin NERC Regions, Eric Bowen and Donald J. Lacombe. The Energy Journal, Vol. 38, Number 3, 2017, pp 177-234.

The Report of the Expert Panel on Modernization of the National Energy Board and the Response of the Government of Canada, by Nigel Bankes. Energy Regulation Quarterly, Vol. 5, Issue 3, 2017, pp 11-24.

Federal Environmental Assessment Reform: A Practitioner's Perspective, by Michael Fortier. Energy Regulation Quarterly, Vol. 5, Issue 3, 2017, pp 25-28.

The Mandate of the National Energy Board, by Peter Miles. Energy Regulation Quarterly, Vol. 5, Issue 3, 2017, pp 29-32.

Winter Residential Optional Dynamic Pricing: British Columbia, by Chi-Keung Woo, Jay Zarnikau, Alice Shiu and Raymond Li. Canada Energy Journal Vol. 38, Number 5, 2017, pp 115-124.

The CO2 Content of Consumption Across U.S. Regions: A Multi-Regional Input-Output (MIRO) Approach, by Justin Caron, Gilbert E. Metcalf and John Reilly. The Energy Journal Vol. 38, Number 1, 2017, pp 1-22.

A Top – Down Approach to Evaluating Cross-Border Natural Gas Infrastructure Projects in Europe, by Andras Kis, Andrienn Selei and Bobala Takacsne Toth. The Energy Journal, Vol 37, Special Issue 3, 2016, pp 61-80.

***Felix KWAMENA**, Ph.D.*

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

INFRASTRUCTURE RESILIENCE RESEARCH GROUP (IRRG)

UPCOMING EVENTS

WINTER / SPRING / FALL 2018

EVENT	DATE / LINK
International Urban Security and Resilience Conference, Workshop and Exhibition, The Sheraton Centre (Toronto, Ontario)	Tuesday, May 8th , 2018 to Thursday, May 10th , 2018 https://www.eiseverywhere.com/ehome/2018internationalurbansecurityandresilience/642621/

EVENT	DATE / LINK
Fall 2018 Training Courses	January to December 2018 https://carleton.ca/irrg/training/
Symposium on Security and Infrastructure Resilience, " The Challenges of Dealing with Natural Resources Development Projects and Activism", Fairmont Chateau Laurier Hotel, Ottawa, Ontario	November 14 – 15, 2018 https://carleton.ca/irrg/cu-events/2016-symposium-on-critical-infrastructure-and-resilience/
The Dean's Annual Lecture Series – Infrastructure Security and Resilience, Carleton University, Ottawa, Ontario	November 15, 2018 https://carleton.ca/irrg/cu-events/2016-the-deans-annual-lecture-series-infrastructure-security-and-resilience