Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 46 — JANUARY 2017

Critical Infrastructure and the Internet of Things

Tobby Simon

CRITICAL INFRASTRUCTURE AND THE INTERNET OF THINGS

Tobby Simon

CIGI

CHATHAM
HOUSE
The Royal Institute of
International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM
HOUSE
The Royal Institute of
International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Tobby Simon is the president and founder of Synergia Foundation, a think tank that works closely with academia, industry and government to establish impactful solutions in the areas of geo-economics and geo-security. He is a commissioner with the Global Commission on Internet Governance and a member of the Trilateral Commission. Tobby has a postgraduate degree in management and is a graduate of the Harvard Business School. He was a research affiliate at the Massachusetts Institute of Technology for five years and has served on the international advisory council of the Belfer Center for Science and International Affairs at the John F. Kennedy School of Government, Harvard University.

The Synergia Foundation is a Bangalore-based interdisciplinary think tank that works with industry, government and academia to establish leading-edge practices in the domains of geopolitics, geo-economics and geo-security. The foundation has multidisciplinary teams that pursue non-partisan research and draws on a global network of resources to offer research analysis and solutions.

ACRONYMS

CERTs	Computer Emergency Response Teams
CIS	critical infrastructure systems
DDoS	distributed denial of service
DoS	denial of service
ICS	industrial control system
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IT	information technology
SCADA	supervisory control and data acquisition

EXECUTIVE SUMMARY

Critical infrastructure systems — the assets and networks, be they physical or virtual, underpinning the functioning of an economy and society — determine the security, prosperity, well-being and resilience of an entire nation. In this regard, the Internet of Things (IoT) is an important concept embedded within a larger spectrum of networked products and digital sensors that has caused an explosion of applications, marking a fundamental shift in the way human beings interact with the Internet, and amplifying both opportunities and challenges — in particular with respect to critical infrastructure — across the globe. The IoT relies on progress in computing power and information technology (IT) to offer possibilities hitherto inconceivable: the IoT revolution — or the large-scale implementation of the IoT — is driving market opportunities and new paradigms in business and policy models each day, and transforming basic aspects of daily life.

The paper creates a framework to navigate the dialogue surrounding critical infrastructure and the IoT, addressing the emerging risks to critical infrastructure with the rise of the IoT, and toward explaining cyber threats to business and governments in the face of an expanding IoT. Presenting an overview of the basics of IoT and the technical processes and issues raised by it, and through landmark examples and references, a set of recommendations to overcome these risks are presented to create an informational resource regarding this growing pertinent conversation in light of competing information and forecasts.

INTRODUCTION

In November 2015, US prosecutors indicted three men in connection to the massive 2014 JPMorgan Chase cyber attack and the hacking of several other financial institutions. The vast, multi-year criminal enterprise centred on compromised private information involving 100 million institutional customers, which fuelled a web of stock manipulation, credit-card fraud and illegal online gambling. The globe-trotting conspiracy hacked servers in various countries, and in one instance exploited the notorious Heartbleed bug. With the stolen data, the group defrauded investors by criminally manipulating stocks, artificially inflating them. They deceived private companies into offering their shares publicly. The group then carefully manipulated the stock prices of the publicly traded companies, spammed email "tips" to institutional clients using stolen information, then quickly would sell off for profit, causing the stock values of the companies they had misled to collapse. The group illegitimately earned millions of dollars in this manner (Farrell and Hurtado 2015).

In a case study paper, Robert M. Lee, Michael J. Assante and Tim Conway (2014) provide an account of a cyber attack on a German steel mill:

> In December, 2014 the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) released their annual findings report. In one case they noted that a malicious actor had infiltrated a steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed advanced knowledge of ICS [industrial control system] and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.

There have been other cases where hackers have used printers, thermostats and videoconferencing equipment to breach security systems. Cybercrime costs the global economy some CDN$400 billion per annum (Desjardins 2015). In recent years, cyber attacks on Sony, the retailer Target and the Internet dating site Ashley Madison have shown that the technology that offers so many opportunities also brings with it significant threats. Data breaches are usually not identified immediately, as seen in the JPMorgan Chase case, where it was only much later determined that hacked contact information was used in stock manipulation. While details about the damage caused by the attack on the German steel facility are not known, the incident leads to speculation regarding the prospective impact of a larger, more organized cyber attack on the nation's critical infrastructure.

Internet-enabled infrastructure has transformed the boundaries of Internet technology, be it through home-automation concepts, energy-management systems and "smart homes"; wellness devices and network-enabled medical gadgets, which are revolutionizing health care sectors; intelligent vehicles, networked traffic systems and road and bridge sensors; or innovations in agricultural, industrial and energy production and distribution. The rise of "smart cities" has been increasing access to and the availability of information manifold. However, while this has opened up myriad avenues for efficiency, and is helping reap benefits to the tune of billions of dollars for the global economy, the unfettered rise of the IoT raises a plethora of issues: the IoT brings with it a concomitant set of concerns about the security and privacy of people, telecoms networks and power utilities, say, through illegitimate breaches of the networks undergirding critical infrastructure, as the efficiency of Internet connectivity also accelerates susceptibility to security violations through the misuse of IoT data. A "promise vs. peril" discussion has subsequently emerged within governmental and academic debates, which have begun to seek the best means to address the complex interdependence between critical infrastructure and IoT systems.

CRITICAL INFRASTRUCTURE

The term "infrastructure" is evolutionary and is often ambiguous. It is traditionally defined as any physical asset that is capable of being used to produce services or support the structure and operation of a society or an enterprise. Today, the notion of public infrastructure has broadened and encompasses such structures as roadways, bridges, airports and airway facilities, mass transportation systems, waste treatment plants, energy facilities, hospitals, public buildings and space or communication facilities, for example (Moteff and Parfomak 2004).

Critical infrastructure, on the other hand, includes physical and virtual facilities and services that form the basis for a nation's defence, a strong economy and the health and safety of its citizens. It is important as it provides necessities such as water and food, electricity and gas, telecommunications and broadcasting, health services, the financial system and the transportation system. They are essential for social cohesion and economic performance (see Figure 1).

At the heart of critical infrastructure is an ICS, which includes supervisory control and data acquisition (SCADA) systems, and other types of control systems that monitor processes and control flows of information. The functionality of an ICS is like the on or off feature of a light switch. For instance, an ICS can regulate the flow of natural gas to a power generation facility or the flow of electricity from a grid to a home.

An ICS is a proprietary and — most often — closed system. As an isolated, so-called air-gapped system, it is not vulnerable to virtual attacks, although it is susceptible to attacks by way of physical access, such as from infected removable devices (for instance, if an employee or supplier unwittingly uses an infected USB device within an air-gapped system). As technology continues to grow, more ICSs are connected to the Internet. This makes them vulnerable to multifarious attacks.

The operating environment for critical infrastructure is increasingly complex, driven by a number of factors, including globalization, the evolution of technology and the interconnected nature of critical infrastructure supply chains, networks and systems. This complexity, in particular, impacts the ability to understand and manage cross-sector dependencies (Brandis 2014).

Computers and communications, themselves critical infrastructures, are increasingly tying other infrastructures together. The growing interconnectedness from networking means that a disruption in one network may lead to disruption in another. This reliance on computers and networks increases critical infrastructure's vulnerability to cyber attacks (Moteff and Parfomak 2004).

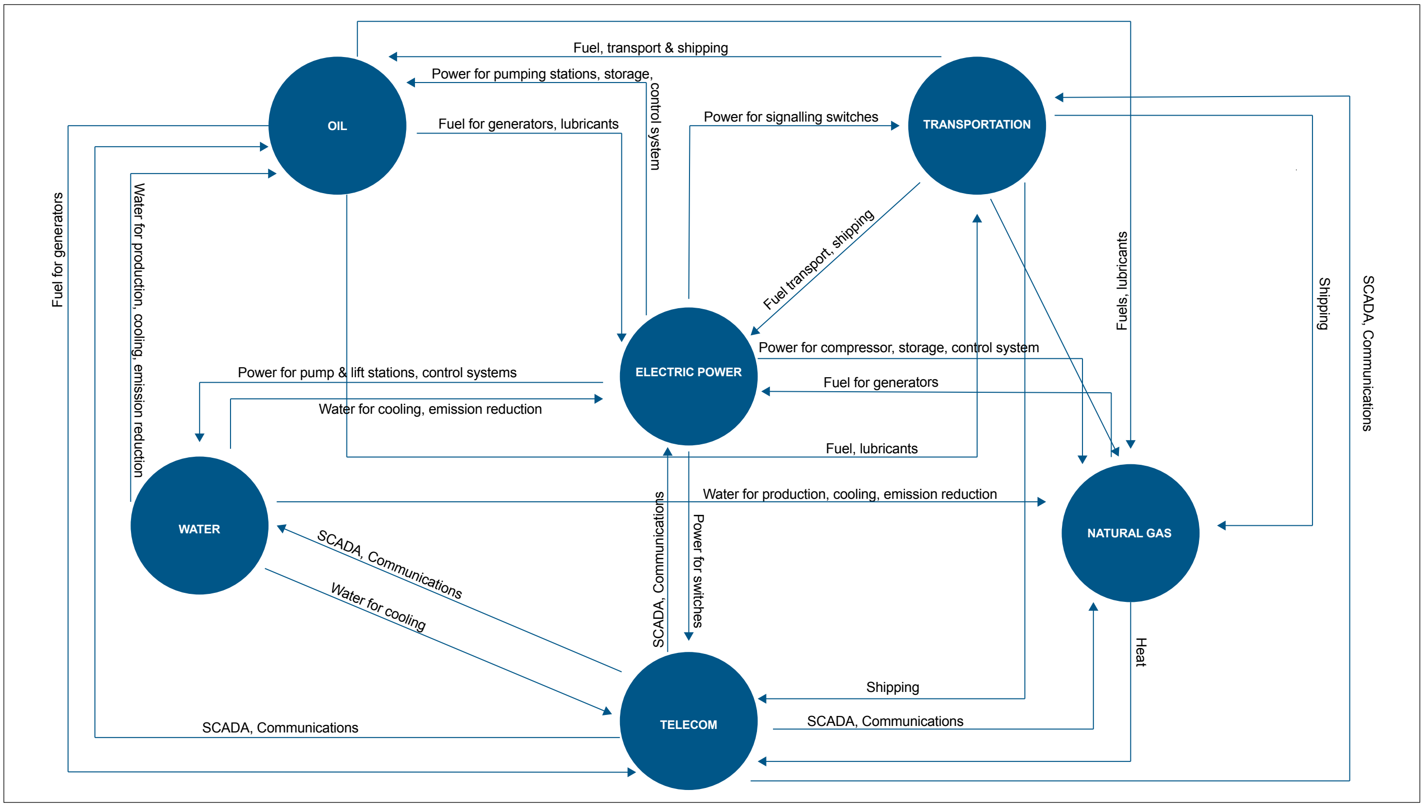
TYPES OF CYBER ATTACKS

Cyber attacks can be divided into four main groups — "hacktivism," cybercrime, cyber espionage and cyberwar, although the lines often blur — i.e., hacktivists may also engage in cybercrime or cyber espionage. Moreover, what may be considered hacktivism in one nation could be considered intelligence or cyberwar in another nation. It should, therefore, be noted that the categories intersect with each other despite theoretical delineation.

HACKTIVISM

Hacktivism emerged in the late 1980s in the form of Internet viruses and worms spreading political propaganda and messages of protest. The group Worms Against Nuclear Killers is an example of early hacktivism; in 1989, these Australia-based anti-nuclear hacktivists installed worms into the networks of NASA and the US Department of Energy to protest the launch of a space shuttle carrying radioactive plutonium. By the middle of the next decade, denial-of-service (DoS) attacks became common, often taking the form of message or traffic floods; for example, in 1994, the "Zippies" group spammed email accounts in the United Kingdom to protest against a bill that outlawed outdoor dance music festivals. Dorothy Denning (2015) writes that the term "hacktivism" was coined in 1996 by the Cult of the Dead Cow hackers' group, and the term picked up media momentum during the 1998-1999 Kosovo conflict, when DoS attacks were launched against websites in those member countries participating in the North Atlantic Treaty Organization's aerial bombardment of Yugoslavia. Hacktivism has become a common means of protest: groups exist worldwide, some associating themselves with a specific country, such as Anonymous Syria, others associate themselves with a particular government or a political group, such as Cyber Caliphate, while others express no particular allegiance, such as

Figure 1: Example of Infrastructure Interdependencies


OIL
TRANSPORTATION
ELECTRIC POWER
WATER
NATURAL GAS
TELECOM
Fuel, transport & shipping
Power for pumping stations, storage, control system
Fuel for generators, lubricants
Power for signalling switches
Fuel for generators
Water for production, cooling, emission reduction
Fuel transport, shipping
Fuels, lubricants
Shipping
SCADA, Communications
Power for compressor, storage, control system
Fuel for generators
Power for pump & lift stations, control systems
Water for cooling, emission reduction
Fuel, lubricants
Water for production, cooling, emission reduction
SCADA, Communications
Water for cooling
SCADA, Communications
Power for switches
Heat
Shipping
SCADA, Communications
SCADA, Communications

Source: Author.

Anonymous. Anonymous, a loosely organized group of hacker activists known for wearing Guy Fawkes masks, garnered popularity with the launch of Project Chanology, protests launched against what the group said was Internet censorship by the Church of Scientology. The group has since been responsible for cyber attacks and hacktivism against governments, terrorist organizations (including the Islamic State of Iraq and the Levant), corporations, religious groups and suspected sexual offenders, among others. Hacktivists, in addition to DoS attacks and defacing websites, often commandeer Twitter and Facebook accounts, make extensive use of social media to promote their actions and rally support, and steal and reveal sensitive information from the systems they penetrate (ibid.).

CYBERCRIME

Criminal hackers (motivated by economic gains through illegal penetration of computer networks, and relatively non-violent in nature) operate across the globe, replacing traditional forms of crime, costing the global economy an estimated CDN$445 billion annually (Morag 2014). Broadly, cybercrime includes fraud, sale in contraband and counterfeit items and online scams. Fighting cybercrime is particularly tricky because the crimes often challenge jurisdictional boundaries. A criminal hacker may sit in one country, use a server hosted in another and hack into systems housed in a third, rendering the legal and geographical components of the crime a challenge to investigate, let alone prosecute.

CYBER ESPIONAGE

Cyber espionage is a strategy aimed at obtaining critical governmental or corporate information by breaking into computer networks and systems. The strategy can be used to spy on any entity or group; for example, it is used for state-level purposes to understand rival country capabilities and attain classified information, or, in the case of industrial espionage, to gain access to rival business strategies and intellectual property. Cracking techniques and malicious software, such as a Trojan horse program, are employed to acquire personal, economic, military or political information through the Internet, computer networks or individual computers. Importantly, governmental or private actors sometimes undertake this even in the absence of hostilities. China has been particularly active in state-based hacking. According to one study, nearly half of all cyber-espionage attacks in the world originate from East Asia, in particular from China and North Korea (ibid.). North Korea, as mentioned in an example below, has waged distributed denial of service (DDoS) attacks on South Korea in the past decade. Also, Iran was blamed in 2013 for attacking Aramco, Saudi Arabia's oil company, by erasing data from roughly 30,000 computers and penetrating Royal Saudi Navy and Marine Corps networks. Such operations are typically illegal in the victim entity, but may be launched or supported by a foreign state or an entity from abroad.

CYBERWARFARE

Cyberwarfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption" (Clarke and Knake 2010), although the taxonomy has been widened to include non-state actors such as extremist groups, private firms, transnational criminal/terror groups and others. Countries are increasingly investing heavily in cyberwarfare technology, if not making cyber espionage a central aspect of their overall military strategy. This full-fledged threat to critical infrastructure is considered to have catapulted into a present danger with the discovery of the Stuxnet worm/virus in June 2010, and refers to any coordinated attacks waged against the critical infrastructure or control systems of a nation. Clandestine US attacks on the computer systems of Iranian nuclear enrichment facilities in 2012, as well as Russia's cyber attacks against the websites and network infrastructures of Estonia and Georgia, are classified as tactics of cyberwar (Edwards 2004).

Table 1 outlines the impacts and relative severity of the four categories of threats. Where critical infrastructure is concerned, cyber espionage and cyberwar are far more harmful than hactivism or cybercrime attacks, although they are perceived to be far less frequent (Morag 2014).

Table 1: Threat Categories versus Impacts

Threat Type	Impact Type
Hacktivism	The interruption of life-sustaining services (minor)
Cybercrime	Economic damages (minor)
Cyber espionage	Economic damages (major) Severe degradation of national security
Cyberwar	The interruption of life-sustaining services (major) Economic damages (intermediate)

Source: Edwards (2004).

THE IoT

Walt Mossberg (2014) has described the IoT as a "constellation of inanimate objects [that] is being designed with built-in wireless connectivity, so that they can be monitored, controlled and linked over the Internet" (cited in Cha 2015). The IoT "refers to the connection of everyday objects to the Internet and to one another, with the goal being to provide users with smarter, more efficient experiences" (Cha 2015).

The Internet revolution has redefined the modern landscape and introduced unprecedented opportunity. The IoT has heralded "smart" living and is transforming every aspect of modern living, industry and the economy. Internet connectivity is now being built into a wide range of non-computer products, including kitchen and home appliances, lighting and heating products and insurance company-issued car-monitoring devices. These products contain three important components: an Internet connection, either in the device itself or in a base station; a digital sensor, to collect incoming data; and a processor, like any computing device. However as IoT industry develops, the threat landscape also changes drastically, augmenting IT security concerns.

While the consumer IoT is set to revolutionize living, it comes with numerous risks. Recently, researchers from Proofpoint, a next-generation cyber-security company, reported that more than 100,000 smart TVs, refrigerators and other consumer items were compromised by hackers to transmit 750,000 malicious emails in a two-week period. Smart appliances are attractive to cybercriminals due to their 24-hour connectivity to the Internet and their poorly protected Internet environments (Prince Trust of India 2014). Researchers have shown how brakes in automobiles with on-board diagnostics, and other critical vehicular control systems, can be remotely controlled by virtually anyone with an Internet connection. One could take control of a such a vehicle by sending data to its interconnected entertainment and navigation system via a mobile phone network.

In December 2013, Target Corp's data breach rendered 40 million customers' banks accounts compromised. The source of the breach was found to be Fazio Mechanical, a small firm that has commercial relations with Target and whose network had been breached via email malware. The cybercriminals used this network breach to remotely connect to Target's network. This single and seemingly minuscule attack also managed to affect cash registers in more than 1,800 stores across the United States; it was subsequently found that Target's computer network was exposed to several vulnerabilities, such as missing patches in the operating system and outdated software, that were easily exploited.

Similarly, in March 2016, investigators at Verizon reported on several breaches against a water utility, referred to using the fake moniker "Kemuri Water Company," due to what was found to be poor security infrastructure and operational technology systems that were decades old. The SCADA system of the water company, which connected the main operational technology systems (such as valve applications and financial systems), was an IBM AS/400, introduced in 1988. Hackers managed to manipulate the weak system and impede on water treatment and production to the point that the entire process became impaired. Moreover, investigation reports found that the culprits were much less skilled than what one might have expected. According to Verizon's "Data Breach Digest," only a small number of security breaches constituted the vast majority of major cyber attacks in a three-year review (Kovacs 2016).

INDUSTRIAL INTERNET OF THINGS

For industry, the Industrial Internet of Things (IIoT) is altering manufacturing, energy, transportation, cities, medical and other industrial sectors, thereby driving a fourth wave of industrial revolution.

The IIoT describes machine-to-machine communications where machines interact and communicate with other machines and objects. These communications result in huge volumes of data that are intelligently generated, processed and analyzed, leading to efficient management. The increasing trend toward the IIoT is transforming industries such as transportation, entertainment, medicine, communications and industrial automation by optimizing operations (Lydon 2014).

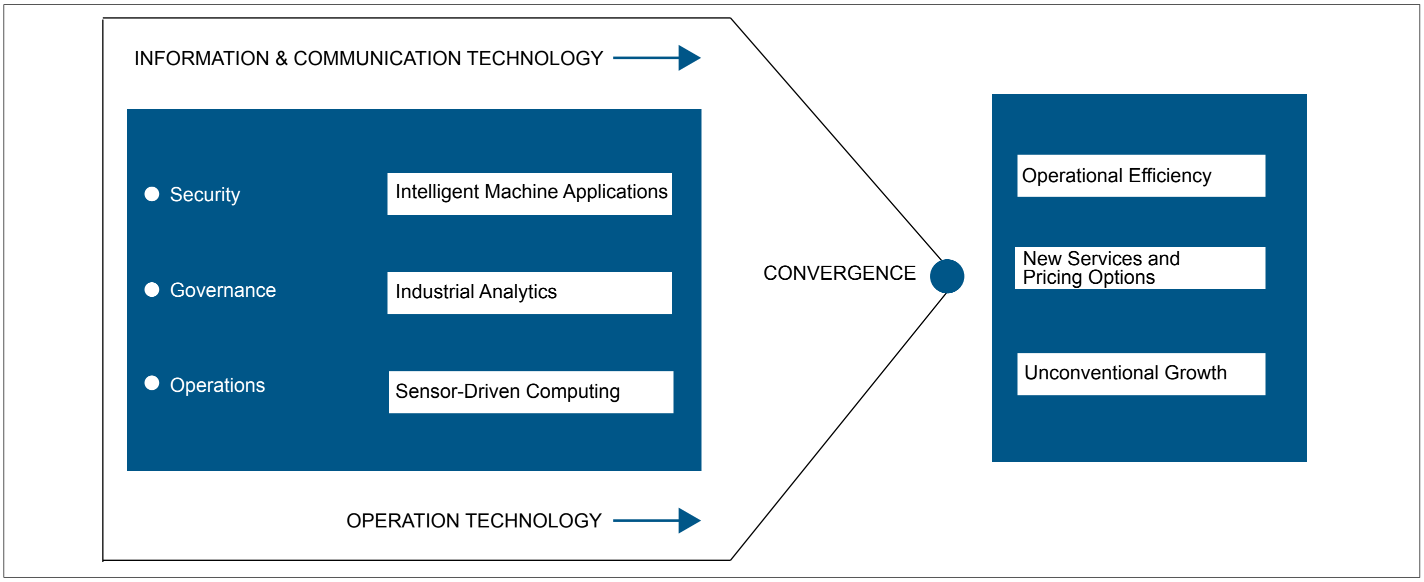
In the near future, "the intersection of people, data and intelligent machines will have far-reaching impacts on the productivity, efficiency and operations of industries around the world" (Shekhar 2016). The IIoT presents companies with myriad opportunities to upgrade, offer new services, improve products, increase production, create hybrid business models and enter new markets. To reap the full benefits of the IIoT, organizations will need to excel at exploiting three technology capabilities: sensor-driven computing, industrial analytics and intelligent machine applications.

The IIoT is transforming businesses by:

- optimizing asset utilization;
- reducing operational cost;
- improving worker productivity;
- enhancing worker safety;
- creating new revenue streams;
- improving sustainability; and
- enhancing customer experience (Daugherty et al. 2015).

According to a World Economic Forum (2015) report, examples of the IIoT "include using unmanned aerial vehicles…to inspect oil pipelines, monitoring food safety using sensors, and minimizing workers' exposure to noise, chemicals and other hazardous gases, especially in traditional heavy industries like oil and gas, manufacturing and chemicals." In the United Kingdom, a provider of drinking and waste-water services "is using sensors, analytics and real-time data to anticipate equipment failures and respond more quickly to critical situations, such as leaks or adverse weather events" (ibid.) (see Figure 2).

Figure 2: IIoT Convergence of Technology



Source: Author.

ICSs

Initially, "ICSs had little resemblance to traditional information systems" as "they were isolated systems running proprietary software and control protocols" (Ross et al. 2006). As these systems have increasingly been integrated "into mainstream organizational information systems to promote connectivity, efficiency and remote-access capabilities, they have started to resemble traditional information systems" and "in many cases, ICSs are using the same commercially available hardware and software components as in the organization's traditional information systems" (ibid.). According to the report by Ron Ross et al. (2006), "While the change in ICS architecture supports new information system capabilities, it also provides significantly less isolation for these systems from the outside world and introduces many of the same vulnerabilities that exist in current networked information systems. The result is a greater need to secure ICSs."

There are several drawbacks to traditional ICSs:

- Software, sensors and controls running many contemporary facilities and equipment are outdated and difficult to upgrade. Thus, organizations cannot readily incorporate new features and improvements.
- There is limited integration between internal systems (such as managerial apps, plant data sources) and external partners, which creates data silos.
- Aging operating systems and vulnerable operational technologies pose security risks because they cannot be easily retired or replaced.
- There is limited embedded computing or intelligence control at the device, product or plant level. (Daugherty et al. 2015)

Previous SCADA systems "took advantage of developments and improvement in system miniaturization and Local Area Networking (LAN) technology to distribute processing across multiple systems." According to Edvard Csanyi (2013), "the distribution of individual SCADA system functions across multiple systems provided more processing power for the system as a whole than would have been available in a single processor....Distribution of system functionality across network-connected systems served not only to increase processing power, but also to improve the redundancy and reliability of the system as a whole" (ibid.).

Traditional ICSs use an open-system architecture rather than a vendor-controlled, proprietary environment. They use Internet Protocol (IP) for communication and cloud-based services for agility and lower costs. Newer ICSs "have capabilities to monitor inventories, automatically send emails to order more raw materials, contact shippers of ready to ship product, and track product delivery" (Radvanovsky and Brodsky 2014), for example. Continued evolution of control systems with added emphasis on their cyber security is important and necessary for further automation.

The main advantages of new ICSs are:

- increased output or productivity;
- improved quality;
- increased predictability of quality;
- improved consistency of processes or product;
- reduced labour expenditures; and
- improved safety environment for production and operations (Hayden, Assante and Conway 2014).

RISKS AND CHALLENGES FOR THE IIoT

A great deal can go wrong when manufacturing plants, equipment or remote facilities are interconnected and online, including acute disruptions to operations; remote sabotage and loss of life due to impaired infrastructure; and cyber attacks and data theft by criminals, foreign governments and disgruntled employees (Daugherty et al. 2015). Recently, a floating oil rig's control systems were hacked and the rig shut down after the saboteurs tilted it, "while another rig became so riddled with computer malware that it took weeks to make it seaworthy again" (ibid.).

It is clear that the IIoT must be underpinned by a well-thought-out cyber/physical-security architecture. This goal can be augmented with the following actions:

- Apply non-invasive techniques to patch remote assets, and use industrial control and automation systems that cannot easily be shut down.
- Manage obsolete and legacy operating systems, hosts and devices that have limited or no security built into them.
- Detect and remediate counterfeit or compromised software and hardware.
- Safeguard the integrity of information and systems so that unauthorized access is detected and data that falls into the wrong hands is not corrupted and then reintroduced into critical processes.
- Control and monitor network connections to ensure that only appropriate ones exist between sensitive industrial equipment.

- Build in fail-safe mechanisms to ensure that compromised IT systems that run ICSs cause no physical harm to people and property, or other severe consequences.

- Understand adversaries' motivations and adapt risk-mitigation strategies to the main danger, such as one-time theft of records, sabotage or ongoing espionage. (Daugherty et al. 2015)

Ernie Hayden, Michael Assante and Tim Conway (2014) list the following challenges presented by new ICSs:

- Security vulnerabilities: An automated system may have a limited level of intelligence and therefore be susceptible to injects that could "confuse" or overwhelm processing capabilities.

- Research-and-development cost: The costs of automating a process may exceed the cost saved by the automation itself.

- High initial cost: The automation of a new product or plant typically requires large initial investment, in particular compared with the unit cost of the product.

CYBER THREATS TO CRITICAL INFRASTRUCTURE

Today, threats to critical infrastructure are increasingly through electronic, radio-frequency or computer-based attacks on the information components that control critical infrastructure. Cyber systems form the central infrastructure of critical sectors, nearly all of which use IT to facilitate core business processes. The cyber systems of critical infrastructure are thus high-value targets for attack, as disrupting them entails extensive economic, political and social effects.

Numerous kinds of threats exist with varying motivations and capabilities, but all breaches exploit certain kinds of cyber systems of critical infrastructure.

As identified in a study by Nadav Morag (2014), computer systems are generally vulnerable to six types of risk:

- risks due to IT (hardware, software, people, processes);

- risks due to interconnection with outside parties and providers (banks, other companies, and so on);

- risks due to outside suppliers (cloud providers, subcontractors, and so on);

- risks due to disruptions in IT equipment and logistics;

- new technologies (such as the IoT); and

- threats to upstream infrastructure (power supply, water supply, and so on).

There has been a dramatic shift toward engaging computer systems with various types of hardware (i.e., the IoT) — for instance, wireless cardiac pacemakers — rendering further vulnerability. Evolving risk areas include the disruption of cloud infrastructure; physical attacks; criminal data mining; digital fraud; and hijacking unmanned aircraft, vehicles and the like (drones, automated cars and so on).

All critical infrastructure systems have vulnerabilities that can be exploited through "threat vectors." Overall, vulnerabilities in critical infrastructure may be divided into two major subgroups: technical and non-technical (Edwards 2004).

Technical vulnerabilities can be basic vulnerabilities or application-based vulnerabilities. The former refers to the vulnerabilities of common Internet protocols. The core protocols such as IP, TCP (Transmission Control Protocol) and HTTP (Hypertext Transfer Protocol) were created and implemented without factoring in security features since the Internet was initially used to serve academic and governmental environments, wherein the users were trusted entities. Much later, security countermeasures were included in Internet protocols as add-ons with the proliferation of the Internet. Therefore, the Internet is still vulnerable to basic attacks, such as DoS, eavesdropping, hoaxing and packet sniffing. Apart from basic protocols, there are a number of applications, including operating systems, that run on top of basic protocols. These application vulnerabilities are exploited by attackers to gain access privileges to remote systems, steal information and interrupt service. Although a generalization, hacktivists and cyber warriors usually exploit basic protocols first, then application vulnerabilities, while cybercriminals often target application vulnerabilities.

In spite of state-of-the-art security systems — such as digital signatures, cryptography, biometric security, firewalls, intrusion-prevention systems and access-control systems — security breaches have increased over the years due to non-technical vulnerabilities relating to people and processes, and even closed systems are targeted and affected by viruses and worms such as Stuxnet. Security experts say that Stuxnet ultimately infected the closed network of the Natanz nuclear plant in Iran by means of USB thumb drives. The weakest link in cyber security is the human being: although technical countermeasures are vital for the security of critical infrastructure, they will not be as effective without the conducive and enabling behaviour of people and processes. Cyber spies usually exploit people and process vulnerabilities.

THE CYBER-SECURITY CRISIS

With Internet-based networks increasingly touching every aspect of an organization, a single vulnerability in the system can cause a catastrophic chain reaction. Traditional organizational perimeters are eroding, and existing security defences are coming under much pressure. Point solutions, such as "antivirus software, IDS, IPS, patching and encryption…remain a key control for combatting today's known attacks," even though hackers have found new ways to circumvent these controls (EY 2013, 1).

Although many of the initial cyber incidents impacting control systems were not directed at ICSs, wide-spreading Internet worms found their way into ICS networks through connections, remote access or by way of portable media. However, there have been examples of internal and external actors specifically targeting ICSs by exploiting vulnerabilities, commanding unauthorized actions or changing set points.

The 2015 "Dell Security Annual Threat Report" (Dell 2015) stated attacks against SCADA systems quadrupled from 2013 to 2014. Specifically, Dell saw worldwide SCADA system attacks increase from 91,676 in January 2012 to 163,228 in January 2013, and to 675,186 in January 2014.

Cyber attacks are increasingly a concern because of their catastrophic physical implications. The mysterious 2008 explosion of the majority BP-owned Baku-Tbilisi-Ceyhan pipeline in Turkey was only recently revealed to have been a digital attack. At the time, Baku-Tbilisi-Ceyhan was thought to be one of the most secure pipelines in the world. Still, unidentified hackers infiltrated the pipeline through a wireless network, tampered with the systems and caused considerable physical damage in an explosion.

One of the main examples, and a game changer for many organizations, was Stuxnet. It was credited as a precision attack causing physical damage to Iranian nuclear centrifuges by directing them to spin out of control while simultaneously playing recorded system values that indicated normal functioning centrifuges during the attack. This targeted sabotage made clear the potential of cyber attacks.

According to Hayden, Assante and Conway (2014, 20), "One of the most touted ICS cyber incidents involved the unauthorized release of sewage as the result of malicious operation.…Cyber incidents that impact or take command of the control system have raised the specter of consequences that are not shared by IT. In 2007, researchers at the Idaho National Laboratory (INL) demonstrated the ability of using cyber techniques to make unauthorized changes in ICS components which could result in physical damage." In 2012, a group calling itself "Cutting Sword of Justice" conducted an attack on Saudi Aramco, one of the world's largest oil companies. In a matter of hours, 35,000 computers were partially wiped out or totally destroyed.

In 2013, major South Korean banks and broadcasters were hacked, which resulted in bank clients being unable to withdraw money from ATMs and broadcasters' frozen computer networks (Sang-hun 2013). The attack is suspected to have originated in North Korea, with a malware known as "DarkSeoul," which paralyzed networks. At the end of the same year, DarkSeoul struck again, affecting 48,000 computers in South Korea, disrupting network systems and erasing hard disks, and attempting also to penetrate South Korea's nuclear operator, which was operating 23 nuclear power plants (Kwon 2015). The latter attack was described as a spear-phishing attack, in which unsuspecting employees of the nuclear operator opened maliciously coded documents in emails.

More recently, in December 2015, Russia-based hackers were alleged to have caused power blackouts across Ukraine in the first full-fledged attack on an electricity distribution network. Around two million people went without electricity for several hours, and experts say such cyber attacks could happen almost anywhere (Vallance 2016). Russian attackers began sending phishing emails to power-utility offices in Ukraine at least six months before the attack. The emails contained Microsoft Word documents, which, once opened, installed malware. Firewalls prevented the attacked computers from gaining control of larger systems, but the malware, known as "BlackEnergy 3," obtained access to passwords and login details, through which the hackers were able to launch another attack. Over time, they were able to remotely log into SCADA systems. By December 23, 2015, the attackers were remotely controlling SCADA computers and cut power at 17 substations, also jamming company communications so that engineers had difficulty gauging the extent of the blackout.

While there is a growing threat of cyber attacks on critical infrastructure, equally important is the rise of physical attacks on energy, transportation and communications. For instance, damage to undersea cables could significantly impede transactions such as the Society for Worldwide Inter-bank Financial Telecommunications, which transmits about 15 million messages a day via submarine cables to more than 8,300 banking organizations, securities institutions and corporate customers in 208 countries (Burnett 2011). In 2008, a broken submarine cable caused by a ship attempting to moor in bad weather off the coast of Egypt led to an Internet blackout that left 75 million people with limited Internet access. Phone and Internet traffic were severely reduced across a huge swath of the region, by as much as 70 percent in India, Egypt and Dubai (Johnson 2008).

The potential of both digital and/or physical attack on critical infrastructure, and the prospective cataclysmic consequences of such, should be a wake-up call for governments, industry and organizations. There is an urgent need for public and private entities to be aware of the risks and, further, be proactive in protecting their valuable information, thereby improving system performance, reliability and safety.

RECOMMENDATIONS

To realize the full potential of the expanding IoT, businesses and governments will need to first overcome a number of hurdles. Security and data privacy are the most important given increased vulnerabilities to attacks, espionage and data breaches driven by increasing connectivity and data sharing.

The following actions are required for an accelerated development of the IoT:

- **Share best practices:** "Operational safety and security practices vary greatly across industry domains. It is important to understand and document existing best practices across industries….This will help identify gaps and requirements for potential innovation, standards or new cybersecurity products" (World Economic Forum 2015).

- **Policies:** Organizations "need clear legal guidelines over data ownership, transfer and usage" to realize the full potential of the IoT. "Governments need to collaborate with each other and with industry to harmonize compliance requirements in data and liability laws… This will streamline data flows within a jurisdiction and across national borders" (ibid.).

- **Regulations:** For heavily regulated industries, such as utilities and health care, to truly benefit from the IIoT, policy makers "will need to revisit and possibly relax existing regulations to provide more flexibility and incentives" to drive innovation. "In the utilities industry, governments can now tap into the new power of transparency enabled by the IIoT to encourage more competition, market efficiency and better customer services" (ibid.).

- **Digital infrastructure:** The success of the IIoT "depends heavily on the presence of robust infrastructures, such as ubiquitous broadband connectivity and digital sensors." As emerging-market countries "continue large construction efforts, like roads, airports, factories and high-density buildings, they can avoid costly retrofitting faced by developed countries by installing state-of-the-art embedded sensors from the outset. These capabilities provide a foundation for smart cities, enabling more efficient use of natural resources and better public safety and citizen services. Industry can help government leaders to prioritize infrastructure investments that can provide long-term strategic benefits to economic growth, social impact and political success" (ibid.).

- **Role of manufacturers:** For the Internet to have a positive impact, there is a need for Internet service to be accessible, affordable, interoperable, secure and resilient. Today, virtually anyone can manufacture a connectable device. There are no standards for developing and incorporating safety aspects into these devices. Developing testing systems for existing industry and future products would help create a resilient ICS. Once manufacturers have made a connectable product — whether hardware or software — it is not enough to apply security as a veneer atop products that have already been manufactured. During the manufacturing process, security must be a built-in aspect of design for both hardware and software. Over time, these should evolve as standards that guarantee a certain level of default security to the systems. In the same way that quality benchmarks guide users to discriminate with respect to features, these security measures need to be a part of the embedded standards. For example, leading software manufacturers (product and custom) already have aspects such as software development life cycle as a standard input. This needs to become far more widespread — ubiquitous, in fact.

- **Role of Computer Emergency Response Teams (CERTs):** CERTs can play a major role in standardizing processes in the connected world. Standards must be developed toward the manufacture of IoT devices. Developing standard operating procedures for information sharing between governments and industry is also important. Repositories of vulnerabilities and laws should be created to be better prepared for future counter malicious activities against industrial systems. A global platform is one way to bring together industries by involving key stakeholders across the value chain. It "can help raise the collective security awareness by sharing threat intelligence. It can also ensure a unified industry voice when communicating with governments or agencies involving security" (ibid.).

- **Raise awareness among policy makers.** Many public policy makers are not well informed about the impact the IIoT might have on citizens, industry and governments. There is an urgent need for them to be better versed in the technology, its societal and policy implications (such as data security, privacy, education and employment) and the impact on government services (ibid.).

- **Cyber-security practices:** "Comprehensive, yet targeted, situational awareness is critical to understanding the wider threat landscape and how it relates to the organization. Cyber threat intelligence can bring this knowledge" as "it incorporates both external and internal sources of risk, and covers both the present and future while learning from the past" (EY 2015). Regularly rehearsing incident-response capabilities through "table top exercises [and] enacting complex incident scenarios" tests the organization's capabilities and provides better crisis management (ibid.). Cyber security "should become a standing boardroom issue — a vitally important item on the agenda. The organization's leadership should understand and discuss how cyber security enables the business to innovate, open new channels to market and manage risk" (ibid.).

CONCLUSION

The integration of the IoT with critical infrastructure means new growth opportunities for organizations and governments across the world. Although there are technological challenges and important hurdles to overcome, in particular concerning connectivity and security, the emerging technology will transform interoperability and efficiency in the modern world. According to Paul Daugherty et al. (2015, 17), "To be a viable stakeholder as well as partner in the digitally contestable future — and thus generate new revenues, governments and industries need to make the necessary changes." Of prime importance is ensuring data privacy, cyber security and accessibility to the global commons in order to drive innovation and growth. Knowing that attacks can never be fully prevented, organizations and governments should advance their cyber-threat-detection capabilities so that response to threat of attack is proactive and appropriate. Learning how to stay ahead of cybercrime will allow organizations to exploit the opportunities offered by the digital world, while minimizing exposure to the risks and costs of dealing with them.

WORKS CITED

Brandis, George. 2014. "Opening Address of the Critical Infrastructure Resilience Conference Melbourne, Victoria." May 22. www.attorneygeneral.gov.au/Speeches/Pages/2014/Second%20Quarter%202014/6June2014-OpeningAddressOfTheCriticalInfrastructureResilienceConference.aspx.

Burnett, D. R. 2011. "Cable Vision." *Proceedings Magazine*, August. US Naval Institute.

Cha, Bonnie. 2015. "A Beginner's Guide to Understanding the Internet of Things." Recode.net, January 15. http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: HarperCollins.

Csanyi, Edvard. 2013. "Three generations of SCADA system architectures." Electrical Engineering Portal, April 22. http://electrical-engineering-portal.com/three-generations-of-scada-system-architectures.

Daugherty, Paul, Prith Banerjee, Walid Negm and Allan E. Alter. 2015. "Driving Unconventional Growth through the Industrial Internet of Things." Accenture. www.accenture.com/in-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf.

Dell. 2015. "Dell Security Annual Threat Report." http://8f7ff0b2bdcb95e1cf03-005bbf273b9ee62b153151d15b71b4f0.r40.cf1.rackcdn.com/articles/2015-dell-security-annual-threat-report-white-paper-15657.pdf

Denning, Dorothy. 2015. "The Rise of Hacktivism." *Georgetown Journal of International Affairs*, September 8. http://journal.georgetown.edu/the-rise-of-hacktivism.

Desjardins, J. 2015. *The Cybersecurity Boom*. http://www.visualcapitalist.com/the-cybersecurity-boom.

Edwards, Matthew. 2004. *Critical Infrastructure Protection*. Amsterdam, NL: IOS Press BV.

EY. 2013. "Security Operations: Centers against cybercrime." www.ey.com/Publication/vwLUAssets/EY_-_Security_Operations_Centers_against_cybercrime/%24FILE/EY-SOC-Oct-2013.pdf.

———. 2015. "Cybersecurity and the Internet of Things." Insights on governance, risk and compliance." March. www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.

Farrell, Greg and Patricia Hurtado. 2015. "JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever." Bloomberg.com, November 10. www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds.

Hayden, Ernie, Michael Assante and Tim Conway. 2014. "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity." A SANS Analyst Whitepaper. https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

Johnson, Bobbie. 2008. "How one clumsy ship cut off the web for 75 million people." *The Guardian*, February 1. www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet

Kovacs, Eduard. 2016. "Attackers Alter Water Treatment Systems in Utility Hack: Report." SecurityWeek.com, March 22. www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report.

Kwon, K. J. 2015. "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes." CNN, April 23. http://edition.cnn.com/2015/04/22/asia/koreas-cyber-hacking/.

Lee, Robert M., Michael J. Assante and Tim Conway. 2014. "German Steel Mill Cyber Attack." ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper. SANS Industrial Control Systems, December 30. http://ics.sans.org: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Lydon, Bill. 2014. "Internet of Things: Industrial automation industry exploring and implementing IoT." InTech, March/April. www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/mar-apr/cover-story-internet-of-things/.

Morag, Nadav. 2014. "Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats." Colorado Technical University, October. www.coloradotech.edu/~/media/CTU/Files/ThoughtLeadership/cybercrime-white-paper.ashx.

Mossberg, Walt. 2014. "SmartThings Automates Your House Via Sensors, App." Recode.net, January 28. www.recode.net/2014/1/28/11622774/smartthings-automates-your-house-via-sensors-app.

Moteff, John and Paul Parfomak. 2004. "Critical Infrastructure and Key Assets: Definition and Identification." Congressional Research Service Report for Congress, Library of Congress, Washington, DC. October 1. www.fas.org/sgp/crs/RL32631.pdf.

Prince Trust of India. 2014. "Cyber criminals hack smart fridge to send out spam." *The Economic Times* (Mumbai), January 20. http://economictimes.indiatimes.com/industry/cyber-criminals-hack-smart-fridge-to-send-out-spam/articleshow/29110789.cms.

Radvanovsky, Robert and Jacob Brodsky, eds. 2004. *Handbook of SCADA/Control Systems Security*. Boca Raton, FL: CRC Press.

Ross, Ron, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner and George Rogers. 2006. "Recommended Security Controls for Federal Information Systems." National Institute of Standards and Technology. July. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/appendix-i.pdf.

Sang-hun, Choe. 2013. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." *The New York Times*, March 20. www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

Shekhar, Sidharth. 2016. "IoT Adoption in India: How to Take It Forward?" PCQuest, June 1. www.pcquest.com/iot-adoption-in-india-how-to-take-it-forward/.

Vallance, Chris. 2016. "Ukraine cyber-attacks 'could happen to UK.'" BBC.com, February 29. www.bbc.com/news/technology-35686493.

World Economic Forum. 2015. "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services." www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of Finance	Shelley Boettger
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief Operating Officer and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Sharon McCartney
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of
International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org