CYBER SECURITY FOR THE GOVERNMENT OF CANADA

THE CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE

L'INSTITUT DE LA CONFÉRENCE DES ASSOCIATIONS DE LA DÉFENSE

EDITED BY CHRISTOPHER COWAN AND EVA LUC

JULY 2018

INTRODUCTION

by Craig Leslie Mantle, PhD

Canadians are inseparable from their electronic devices. Smartphones, laptops and all manner of objects connected to the "internet of things" permeate our daily lives from the moment we wake to the moment we fall asleep again. And it is easy to understand why: the devices that keep us connected in an increasingly wired world keep us informed, entertained and productive. In the course of human history, few other technologies have revolutionized and simultaneously made more convenient our habits of work, play and rest in so short a time. But all of this has come with a cost: our security. As we rely more and more on devices to simplify and enrich our daily experience, we also expose ourselves to nefarious agents who seek to exploit our electronic dependency for their own gain. All who capitalize on the benefits afforded by connected devices – from individuals who read the online news while riding the bus, to state governments that rely on computers to keep the personal information of their millions of citizens safe, to transnational companies that run worldwide supply chains – are to lesser or greater degrees at risk. Whether we recognize it as such or not, we are locked in a vicious cycle, with patches and updates being released to address system weaknesses (or, at significant expense, designing robust systems and the means to protect them) and cyber criminals adjusting their tactics in a seemingly never-ending game of cat-and-mouse.

Against this backdrop, IBM hosted a cyber security event in Ottawa, Ontario that addressed many of these issues and more. The CDA Institute provided five graduate students to act as rapporteurs, to capture the essence of each speaker's comments; one student was able to go beyond passive listening and actively engage with subject matter experts in the field of cyber security in order to obtain a deeper understanding of relevant issues as they pertain to the Government of Canada. Their summaries follow. ■

CONTENTS

*Cover image courtesy of Flickr user Blogtrepreneur

WELCOMING REMARKS BY BOB KALKA, VICE-PRESIDENT OF IBM SECURITY

by Mikaela Lichty

Bob Kalka offered welcoming remarks. He introduced to the audience the top thought-individuals from around the globe who came to speak at the conference and set the stage for the upcoming panels. While cyber security receives a significant amount of attention, there is still a skills shortage with over 300,000 cyber jobs remaining unfilled, a number that could climb to over two million by the end of the decade.[1] This pertinent issue, along with topics on how to improve intelligence, would be discussed in the following remarks. The panelists would also delve into how cyber threats are viewed and how cognitive computing and machine learning are being applied against cyber threats. This is not a futuristic ideal—this is all happening right now! ■

Notes

1. For further information, see Bob Kalka, "Returning From Coventry: The Crisis of Consumability", IBM *SecurityIntelligence*, 30 March 2016, https://securityintelligence.com/returning-from-coventry-the-crisis-of-consumability/.

Image courtesy of Flickr user Blue Coat Photos

IBM SECURITY STRATEGY AND OVERVIEW

by Mikaela Lichty

Superintendent Mark Flynn, Director, RCMP Federal Policing Cybercrime Operations

The discussion began with remarks from Superintendent Mark Flynn. He specifically manages cybercrime within the Royal Canadian Mounted Police (RCMP) and he provided an understanding of how the RCMP and federal policing programs view cybercrime. Within the RCMP, technology is both a target and an instrument: Not only is technology a target for attack, it is also serves as a motive and means of achieving criminal aims as well.

Today, there are new criminals who have new tools with which to commit crime. The rate at which criminals are adopting cyber methods to commit these new crimes and to facilitate traditional crimes is unprecedented. These criminals would likely never commit a physical crime if presented with an opportunity to do so, but are now capable of causing an unimaginable amount of harm to others thanks to technology. For example, Flynn stressed that the damage criminals can cause to individuals by sharing private information online is substantial and is the type of threat that needs to be addressed with significant resources. Thus, strategies need to be implemented that enable investigative units to address both traditional crimes with cyber elements and to extend their capacity to target key cybercrime actors. To accomplish this, the RCMP has identified three key cybercrime strategic pillars:

(1) To identify and prioritize threats through intelligence collection and analysis;

(2) To pursue cybercrime through targeted enforcement and investigative action; and

(3) To support cybercrime investigations with specialized skills, tools and training.

The RCMP is a large organization with multiple mandates and a dual policing role within Canada as the federal police service and as a police service contracted out to provinces. One of its mandates is what Flynn referred to as the "Federal Policing Cybercrime Investigative Mandate," which tasks the RCMP with addressing any cybercrime that attacks Canadian infrastructure and key business assets—that is, anything that will have a significant impact on Canadians. In addition, the mandate also tasks the RCMP with any cybercrime that involves the use of cyber systems to facilitate or support terrorist activity, while also providing technological investigative capabilities in national security investigations and in major computer-facilitated crimes. The operational focus of the RCMP is on targeting malware developers and distributers, cybercrime infrastructure developers and operators that facilitate cybercrime (e.g. botnets), as well as financial network operators that facilitate money laundering and monetization of proceeds from cybercrime. By attacking these enabling services, the RCMP hinders the ability of these actors to facilitate cybercrime.

Moreover, the cybercrime investigative mandate tasks the RCMP with investigating traditional crimes under the federal mandate—for example, crimes such as fraud where perpetrators may use cyber systems to easily target larger numbers of people. On the topic of victimization, Flynn highlighted that victims of cybercrime often must contend with the stigma associated with their ordeal as the public is quick to vilify victims by implying attacks were the victim's fault. This is problematic and is a key facet of cybercrime that should always be considered: The shame victims experience often results in individuals not reporting the crime, leaving the crime unaddressed by the police.

The RCMP recognizes it is not able to prevent cybercrime on its own. Cyber security is an area where there is a strong desire among differing departments to collaborate rather than compete. Analysts, criminal investigators, field operators, and others have discussed strategy collaboratively, which has been a beneficial practice to break down departmental barriers within and outside the RCMP. Furthermore, the RCMP has recognized the need to move forward in adopting technologies to improve the speed and efficiency of analyzing data from cybercrime. As a result, a relationship between policing and the private sector has developed that did not previously exist: The RCMP has started to welcome working with partners to overcome any technological knowledge gaps it may have in achieving its cybercrime mandates. As cyber criminals become more sophisticated, it is imperative to find an effective means of analyzing information so that the cyber hacker can be promptly identified. ■

BUILDING A WORLD-CLASS SECURITY OPERATIONS CENTRE

by Casey Babb

Paul Dwyer, Partner IBM Security

As a Partner and Global Competency Leader for IBM's Security Intelligence and Operations Management Consulting practice, Paul Dwyer delivered a presentation that spoke not only to his expertise in this regard, but to his vision of what a security operations centre (SOC) should look like.

According to Dwyer, the primary responsibility and function of a SOC is to detect, prevent, and respond to malicious threats that matter to an organization. Like many of the other expert speakers at this event, Dwyer emphasized the need to tailor specific response mechanisms and capabilities within a SOC that address the specific needs of the business or organization—in a sense, it is about knowing what threats matter, why they matter, and how to defend against them in a timely fashion. That said, given the volume of cyber-attacks or intrusions, companies and businesses need to focus on developing an effective and efficient triage system, rather than developing a net with the intent to stop or respond to all attacks.

Dwyer provided a detailed analysis of some of the most invasive and damaging cyber security threats through 2016 and 2017, while highlighting key characteristics of the attacks, patterns, and emerging trends that we are now seeing across the broader cyber threat environment. From malicious applications that emulate the "look" and/or "feel" of financial applications, to ransomware that revolve around cyber extortion, to the dark-web now being much more accessible to average users, to credit card fraud, insider threats, and biometric fraud, Dwyer painted a clear picture of how problematic the cyber world has become. Ultimately, he emphasized how the landscape of cyber threats has evolved into a much more diverse, accessible and criminally-oriented network.

Using the 2013-2015 Carbanak cyber-attack as a case in point, Dwyer discussed how, what he refers to as sophisticated "hack-a-preneurs", are now outsourcing criminal cyber know-how and technical capabilities to carry out multi-layered and extremely complex attacks that often deliver a tremendous return on investment. In the same sense that various contractors might be employed to build a single home, criminal cyber organizations are now using various actors to carry out specific elements of the overall attack. Not only does this make pinpointing the actual source of the intrusion that much more difficult, it often blurs the lines of criminal persecution given that individual actors are often located in different states that have their own specific cyber laws. In the case of Carbanak, the initial investment of $5 million dollars to pay these individuals and/or organizations generated a gain of nearly $1 billion dollars. Evidently, the business of cyber hacking has transitioned from being generally focused on disruption, to a major multi-billion dollar element of organized crime aimed at financial gain.

In terms of how to create effective SOCs, Dwyer focused on the need to leverage the National Information Exchange Model (NIEM). According to Dwyer, the NIEM was created to provide a simple, flexible, scalable data model that facilitates information sharing across disparate systems using various data formats. In other words, the NIEM is an effective information sharing technique that relies on data analysis and exchange. To Dwyer, given the current cyber threat environment, the frequency of threats, and the crosscutting issues various sectors and governments are experiencing, there ought to be an increased use of resources such as NIEM, in addition to enhancing more traditional forms of information sharing.

Dwyer made a point of discussing the need for increased collaboration among all implicated stakeholders across both the public and private sectors. At present, organizations and businesses are too standardized, too generic, and too isolated from broader collaborative networks that would aid in the hardening of their systems and their abilities to develop enhanced pattern analytics. According to Dwyer, although a group's SOC needs to be innovative, specialized and tailored to the threat environment, it also needs to operate like a factory, wherein organizational efficiency and standardized threat reporting is prioritized.

Dwyer went on to say that while the current number of known threats exceeds the number of unknown threats, that will not be the case for much longer: Within a year, we will likely find ourselves in a situation where there are more unknown than known cyber threats, and as such, the need to develop rigid reporting systems and organizational structure is more pressing than ever. ■

ADVANCED CYBER THREAT DETECTION

by Christopher Cowan

Image courtesy of Flickr user Sherpzz47

Dr. Oded Margalit, Chief Technological Officer, Security Intelligence Strategy

Dr. Oded Margalit, Chief Technology Officer (CTO) of IBM's Cyber Security Center of Excellence in Beer-Sheeva, Israel spoke about how he recruits the next generation of cyber security talent. In his presentation, he addressed the global cyber skills shortage, before sharing some of his inventive ways of recruiting and mentoring new talent.

The need to find and develop new cyber security talent has never been greater. There is currently around 1.8 million vacant cyber security positions worldwide, a 20% increase from 2015. Unfortunately, that skills shortage comes at a time when the costs of cybercrime are nearing an all-time high. It is estimated that cybercrime will cost businesses around the world approximately $8 trillion over the next five years. Without enough talent to help organizations protect themselves, it seems likely that those costs will only increase as the current environment is a "dog's breakfast" for cyber criminals.

Two alternatives, automation and outsourcing, are commonly cited as potential means to alleviate the issues created by vacant cyber security positions, but neither are realistic long-term solutions. Automation can only do so much to fill in the skills shortage, as humans still do the "hard work" in the end. Current artificial intelligence cannot replace a human cyber security specialist, but it can make a human operator more efficient by compiling and analyzing data at speeds and quantities unmatched by humans.

According to Dr. Margalit, outsourcing tends to be less effective than many organizations realize. Contracting network security tasks to a managed security service provider is one option, but some organizations are unwilling or unable to give up control of their security systems. Poaching cyber security experts from other organizations, another common tactic, also does little to relieve the industry-wide skills shortages as it perpetuates a cycle of organizations continuously poaching from one another.

In the end, recruiting top cyber security talent is by and large the most effective way for an organization to protect itself in a world where threats are growing and becoming more sophisticated by the day. Recruiting and developing the best people possible is not easy, but IBM has developed several different means of doing so.

For instance, IBM has created numerous Research Labs around the world with the goal of bringing together the best talent in the world to find solutions to key cyber problems. In 2014, IBM created a Cyber Center of Excellence (CCoE) at Ben-Gurion University in Beer-Sheeva, Israel that focuses solely on finding innovative solutions to pressing cyber security problems. IBM has been growing its presence in Israel recently and as Beer-Sheeva is a high-technology hub that attracts highly-qualified cyber security specialists from around the world, the city is a natural fit for the CCoE.

But getting the right talent together is only half the battle. Developing it is another matter and one that IBM is also addressing. According to Dr. Margalit, recruiting and developing new talent is about incentives and teaching the right skills. Instead of having companies fight for a "piece of the cyber security talent cake", it is better to "make the cake bigger" by teaching more people. Teaching dual-use skills and how to solve problems are effective ways of giving young professionals the ability to deal with new security issues and problems that will arise in the future.

The shortage of cyber security professionals is a problem that cannot be solved overnight as it requires companies to make a concrete effort to fill in the gaps in their security. IBM is currently an industry leader in recruiting and developing world-class cyber security talent thanks to its investments in world-class research facilities and finding the right talent. In a time where the costs of cybercrime are rising, failing to invest in the human side of cyber security is a poor business decision. ■

CYBER THREAT HUNTING

by Christopher Cowan

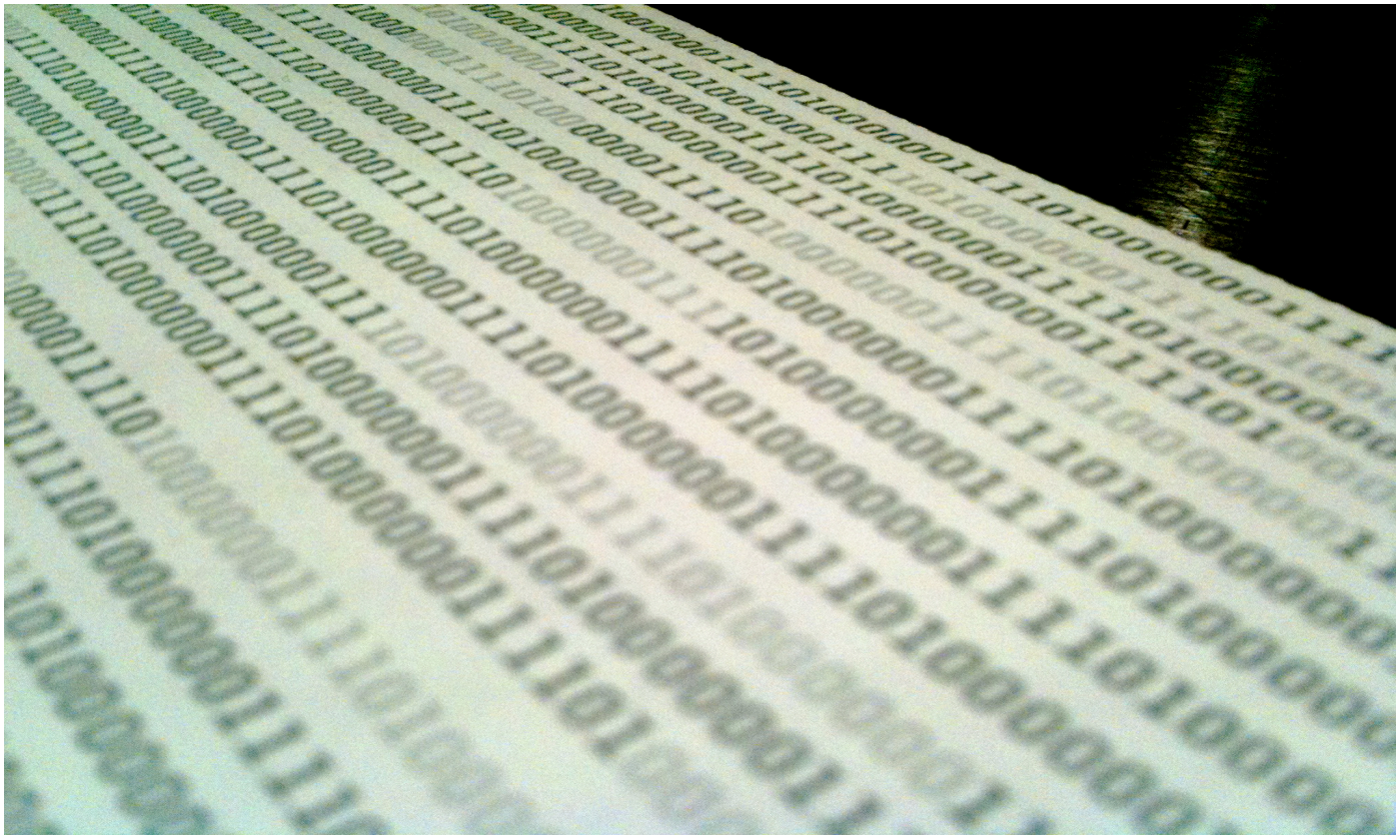

Image courtesy of Flickr user washingtonydc

Jeremy Rodgers, Technical Sales Manager & Cyber Subject Matter Expert, Safer Planet

Jeremy Rodgers spoke about how organizations can conduct effective cyber threat hunting to proactively protect their networks. In his presentation, he addressed the concept of cyber threat hunting, the importance of accurate and timely intelligence analysis, and how IBM's i2 Intelligence Analysis products help analysts pre-empt threats to their networks.

In a world where cyber threats are becoming more numerous and sophisticated, simply passively protecting a network is no longer enough. Detecting and defeating both insider and outsider threats requires organizations to invest in technology that enables the pre-emption of those threats—called cyber threat hunting. IBM's i2 Intelligence Analysis products are world-leading in this regard, giving organizations the ability to collect and analyze data, and produce actionable intelligence that can then be used to pre-empt cyber threats.

There are some big upsides to cyber threat hunting. Instead of relying on passive defences, actively searching can help organizations discover latent threats in their networks, as well as eliminate active threats in their networks as soon as possible. As the old military adage goes, sometimes the best defence is a good offence.

But, Rodgers emphasized, cyber threat hunting is not easy, nor can it be successful without accurate and timely intelligence to inform it. Successful pre-emption requires that the hunter know the source of the threat, as well as the motive behind a potential attack. Discerning both source and motive requires that the hunter receive timely and accurate intelligence to inform decision-making. Producing that intelligence requires analysts who can collect and analyze large volumes of data from numerous sources, domains, and silos.

IBM's i2 Intelligence Analysis products help fill that need, as they are some of the world's most popular intelligence analysis tools. They are used by the majority of Western militaries and national security agencies. They take traditional intelligence tradecraft into the cyber world by giving organizations the tools necessary to

conduct successful cyber threat hunting. They provide analysts with new tools to search through reams of data from a variety of sources, both cyber and non-cyber. They also allow analysts to see data in new ways, recognize patterns that they may not have been able to previously see, and track campaigns against specific threats.

Successful cyber threat hunting requires a holistic view of intelligence collection and analysis. Analysts need to look beyond traditional sources to gather data that provides them with a more complete picture of the threat, where it comes from, and what motivates it. IBM's i2 Intelligence Analysis products help the analyst do just that by finding links and patterns that might have been missed before. Pre-empting cyber threats is not easy, but with the right tools in place, it can improve an organization's network security immensely. ■

Image courtesy of Flickr user[Blue Coat Photos]

THE COGNITIVE ERA OF CYBER SECURITY

by Uri Marantz

Chris Meenan, Global Director, Security Intelligence Strategy

Chris Meenan spoke about "Bringing the Power of Cognitive Security to the Security Analyst." He gave a thought-provoking presentation on how IBM's running experiment with artificial intelligence (AI), Watson, can facilitate the work of security analysts in any sector and for any organization.

The motivation for IBM's innovation with AI emerges from the reality of cyber threats today. The number of threats and alerts are increasing daily, but the availability of analysts with the necessary skills, as well as the available that they have to respond, are decreasing simultaneously. As it stands, 93% of security managers fail to triage potential threats successfully, 42% of security professionals ignore a "significant number of alerts" due to time constraints, and 31% of organizations are forced to ignore more than half of their security alerts for lack of resources.

The cognitive study of security has revealed the limitations faced by human analysts. Intelligence, accuracy, and speed all decline precipitously with human performance, but machine-powered cyber security analysis can overcome many of these limitations. Given the increasing sophistication of cyber threats and attacks, and the increasing volume, variety, and complexity of data streams, the need for enhanced cyber threat response has never been greater. This is where IBM's threat detection analytics and solutions can make an impact.

IBM security introduces a revolutionary shift in security operations with a new approach to cognitive security, QRadar Watson Advisor. IBM's cognitive security program assists the human security analyst with gaining local context leading to a cyber incident or anomaly, gathering threat research and developing expertise, and applying that intelligence to anomaly investigation. Like a detective cracking a criminal case, QRadar Watson Advisor creates knowledge graphs that links activities and entities in patterns that security analysts would otherwise not be able to detect or recreate themselves.

QRadar Watson Advisor enables key comprehensive investigative insights by unlocking the vast security knowledge and potential that is simply inaccessible to human analysts. Botnets and malware pioneered and networked by malicious users can be detected, identified, and counteracted. Incidents can be investigated, threats confronted, and attacks thwarted in record time. Whereas manual threat analysis took days or weeks, with QRadar Watson Analysis it can be done in a matter of minutes or hours. Tedious tasks are automated and complex procedures simplified so security analysis conclusions can be presented clearly and simply.

IBM security intelligence and incident response offers significant improvements in cyber threat and risk detection, security investigation and qualification, and organizational governance and incident response. Accelerated alert triage, enhanced threat analysis, optimized incident response, and increased threat awareness all bring the power of cognitive security to the security analyst. Overall, IBM security is making investments in cognitive technologies that have the potential to revolutionize the way security analysts work today. ■

CONCLUDING REMARKS BY BOB KALKA

by Uri Marantz

Bob Kalka discussed IBM's improvement in the realm of security and the current direction of the company. He explained that cyber security is about risk management and stressed the importance of differentiating between compliance and risk-based management. He described the "consumability challenge", a term used to capture the increasing challenges cyber security faces as compliance goals broaden to include risk management controls.[1] The broadening scope of security goals has led to shortcomings in risk management, as IT security functions have not been able to effectively "consume" this wider mandate. From this perspective, cyber security activities should focus on how to maximize security within a company's existing systems. Kalka discussed two methods to "get more" out of existing systems to address this consumability challenge.

The first method is to increase wisdom. Cyber security activities should avoid short-term fixes in response to current risks that may eventually lead to undesirable consequences in a few years' time. For IBM, ensuring decisions are made in consideration of future implications is a reason why 3300 out of IBM's 8000 employees are consultants gathering information to make better informed decisions.

Following an increase in wisdom, the next method is to enhance horsepower. A company's cyber security is not going to improve with more people even if the company could afford them; however, improving the efficiency and effectiveness of existing resources by increasing their horsepower through innovation does provide a means of improving cyber security. Kalka proposes three ways to increase horsepower:

(1) use cognitive machine learning;
(2) leverage the cloud; and
(3) acquire technology that works together intelligently.

Making use of cognitive machine learning technology, such as IBM's artificial intelligence Watson, is imperative for improving horsepower. Given the sheer volume of available data, humans simply do not possess the capacity to consume and interpret all threat intelligence every day. For example, the most common practice has been to manually search through only 20% of the 6000 pages of data being produced daily. To address this challenge, IBM has started to teach Watson to ingest and dissect cyber threat information. Watson has now reached a point where it is able to draw on three million different sources of intelligence. Rather than manually searching through the data, a company can simply ask Watson if there is a cyber security threat of concern and act accordingly. With Watson's assistance, threat investigations are now 60% faster. The horsepower of an organization is vastly improved through machine learning, as machines can solve problems that are physically impossible for humans.

Furthermore, leveraging cloud services will also increase the horsepower of a company. The switch to cloud services by companies is inevitable—within the next five years, likely half of the security market will be delivered by the cloud. Accordingly, IBM intends to invest heavily in cloud services, especially since cloud services significantly improve the speed of setting up security services for a company. In addition, the idea of cloud identity services—services that address identity and access management needs—is growing and contributing to the increasing relevance of cloud services overall.

On the last point, acquiring technology that works together to identify cyber threats is important because when systems do not work together, gaps are left open that cyber hackers may exploit to gain access to a system. As such, technologies need to act as an immune system and collaborate to orchestrate a response that is not simply an analysis of an attack, but that can protect a system from attack. New technologies are making this orchestration possible. ■

Notes

1. For additional information on the Consumability Challenge, see note 1 in *Welcoming Remarks by Bob Kalka*.

IN-DEPTH ENGAGEMENT OPPORTUNITY: INTERVIEW WITH BOB KALKA AND CHRIS MEENAN, CYBER SECURITY SUBJECT MATTER EXPERTS

by Mike Belyea

Every problem requires cooperation. CSIS' *2018 Security Outlook* describes the contemporary world as one in which individuals have the power to work against states. States such as Canada have impressive cyber security capabilities, but defending Canadian society against cyber threats requires cooperation with other experts.

Collaboration between the Canadian government and the private sector is likely the most viable way to protect Canada against cyber-attacks, such as data breaches, ransomware, and attacks on Canada's critical infrastructure. The Canadian government needs the expertise and experience of the private sector to help defend against such attacks. In turn, the private sector requires government policy to assist with its own needs. The modern world is a place where Canada can be a shining example of a mutually beneficial public-private partnership in cyber security.

To begin, collaboration is necessary as Canada's enemies are increasingly anonymous. Sun Tzu's adage—"If you know your enemy and know yourself, you need not fear the result of a hundred battles"—will not apply to Canadian defence policy for much longer. The enemy is growing and has no face, nor a common goal. Cyber-attacks are played out for political power, blackmail, money, leverage, and occasionally amusement.

Canadian businesses and governments are at constant risk of a cyber-attack. One method to decrease the likelihood of damage is through risk management. Cyber security professionals can often see when their systems are under attack and subsequently formulate an appropriate response method based on the importance of the data breached. As with any other organization, the Canadian government can be exploited. The risk management and response capabilities provided by the private sector would be an irreplaceable asset to the Canadian government.

A prime example of the Canadian government trusting the private sector is through the government's cloud adoption strategy. Cloud services offer a means for Canada to provide public services with private-sector efficiency by storing some of its data on servers owned by private companies. Instead of the government housing its own servers and maintaining them, it is more cost effective and secure to store its information with a private company. With the private sector's collaboration, the government can place its focus and resources elsewhere.

A stronger relationship with the cyber security private sector will help strengthen Canada's defences. The 2017 WannaCry cyber-attack did not affect Canadian institutions, but Canada was unprepared. A cloud service provider would decrease the risk of such an attack affecting government systems.

Critical infrastructure is also a target for cyber-attacks. Governments are largely ill-equipped and unprepared for the aftermath of an attack on a city's power grid, for example. Infrastructure Canada's "Smart Cities Challenge", an initiative to encourage the use of "internet of things" devices on a city-wide level, will only increase the vulnerability of municipalities. The government must work closely with technological security firms when designing and building critical infrastructure. It is too difficult for a company to secure a piece of critical infrastructure after it has been built. The best way to ensure truly secure infrastructure is to collaborate in the design process.

Governments already work with the private sector to solve problems in cyberspace. IBM is an important contributor and one of the biggest players in cyber security. It is host to one of the largest research institutes in the cyber industry based on its record number of patents. IBM promotes the importance of collaboration between companies and with governments. It is currently undertaking projects with universities and colleges around the globe to foster skills in cyber security. Some of its innovative policies include a focus on skills-based hiring. The movement IBM is creating under its Twitter banner, #NewCollarJobs, is teaching people important skills in cyber without requiring them to have degrees.

This is not just beneficial for IBM, either. Governments benefit enormously from innovations such as this. Universities and colleges are heavily subsidized, but neither have developed many cyber programs yet. On this front, IBM is helping to take the burden off governments by training future leaders of the cyber community. Also, colleges and universities need to compete with the private sector for faculty—it is

difficult for governments to attract talent in cyber security because the opportunities and salaries are often better in the private sector. Governments should embrace this massive strength that the business sector has and work with them rather than trying to compete.

The private sector is experimenting with cyber ranges, which will be invaluable to the Canadian government. A cyber range is used for cyber warfare training and to develop cyber technologies. The IBM X-Force Command Centers offer IBM's clients the opportunity to simulate real-world cyber-attack scenarios. This way, people will be prepared for the next attack and will have a better idea of how to respond. It can be difficult for the Canadian government to openly utilize such a tool as a cyber range, especially since the public may not view cyber security as a priority. However, a company like IBM does prioritize cyber security, allowing them to fine-tune their cyber strategies and provide those services to the Canadian government.

There are plenty of positive aspects of a public-private partnership to strengthen Canada's cyber security. The Canadian government needs to strengthen its cyber security capabilities and work with its partners in the private sector, such as with IBM. Together, with security as a shared goal, the private sector and the Canadian government can help Canada become a world leader in this field.

Furthermore, with security as a shared goal, peace may be an inevitable outcome. For instance, it may be logical to consider cyber operations in an offensive capability. However, the entire world essentially runs on the same machines. Exploiting vulnerabilities in an enemy's system would essentially exploit everyone's system, including the attacker's. In a sense, it is mutually-assured destruction and neither side would likely be the first to act.

Without the expertise of the private sector, the Canadian government might act in an arena of ignorance. Without the government enacting policies to help develop the private sector's cyber capabilities, cutting-edge research may be hindered. The best solution to help make Canada a strong player in cyber defence is to partner with companies like IBM and dominate the field. ■


CDA
Institute
L'Institut
de la CAD
~ 1987 ~