CROSS BORDER INSTITUTE UNIVERSITY OF WINDSOR

Cybersecurity, Cross-Border Trade and the Digital Economy: Enabling Smart, Secure Systems

Brampton, Ontario, November 19, 2019

Data is the life blood of the 21st century economy. This is true not only in the realm of information technology, but in more traditionally established sectors including automotive, agriculture, public services and virtually every other part of the economy. Changes in technology and culture such as growing roles of ecommerce and social media imply that more commercial and interpersonal exchanges are made via electronic formats that preserve interactions as digital data. Innovations converge to create new ways of doing old things, such as where artificial intelligence, wireless communications, microelectromechanical systems (MEMS) and others converge and combine to make autonomous vehicles possible. All such innovations are driven by and produce huge volumes of data.

The explosion in the volume and flow of data creates endless opportunities, but also exposes new vulnerabilities that are exploited by actors ranging from small time criminals to international terrorist networks and even the governments of adversarial nations. Cybersecurity presents a set of complex challenges that must be met to promote and preserve economic prosperity, individual rights, international cooperation, national security and global peace. Because cyberthreats are adaptive and rapidly changing, the magnitude of these challenges is complicated by the need to address them quickly.

Canada and the United States are arguably more economically and socially interconnected than any other two countries. Over the years similarities in political and economic systems, shared resources and a common set of values have made it possible to integrate defence and intelligence systems, professional networks, supply chains, media and interpersonal relationships resulting in massive daily movements of people, goods, information and funds across the Canada-US border. All of these movements are supported by data transfers. In some cases, such as the transfer of funds and trade in digital goods, they consist entirely of data transfers. In this sense, the Canada-US relationship is especially vulnerable to cyber attacks so coordinated, or at least complementary, approaches to cybersecurity are critical to the future of our mutually beneficial relationship.

> ***Cybersecurity presents a set of complex challenges that must be met to promote and preserve economic prosperity, individual rights, international cooperation, national security and global peace.***

To address this issue the Consulate General of the United States (Toronto), The Rogers Cybersecure Catalyst of Ryerson University and the City of Brampton co-hosted the one-day conference *Cybersecurity, Cross-Border Trade and the Digital Economy: Enabling Smart, Secure Systems* at the Lionhead Golf and Conference Centre in Brampton Ontario on November 19, 2019. The day comprised a series of keynote and panel sessions with people from business, government, academia and not-for-profits with expertise and direct responsibility for cybersecurity. This included representatives of companies ranging in size from tech giants to start-ups. The cross-border logistics sector was especially well represented and there were speakers

from software, border infrastructure operators, law enforcement, security agencies, and municipalities as well as the US Consul General in Toronto, the Consul General of Canada in Detroit and the Charge d'Affaires at the US Embassy in Ottawa.

PERVASIVE CYBERSECURITY

The scope of discussions over the course of the day demonstrates the pervasive nature of the cybersecurity challenge and the important role played by everyone who accesses data networks. Presenters laid out the new environment in which all private and pubic players must operate. Individuals must learn to practice good "cyber hygiene" both in their own affairs and in their roles at work and within organization. Changing passwords, updating software, adopting two source authentication and learning to recognize "social engineering" ploys to gain entry to networks must become second nature. Because employees often interact with corporate or agency systems using their personal devices and home data services, these must be secured, or remote access must be restricted.

> ***Individuals must learn to practice good "cyber hygiene" both in their own affairs and in their roles at work and within organization.***

Businesses must train their employees in best practices and constantly upgrade skills as new threats emerge. They should take advantage of support from organizations such as CyberNB, the Canadian Cyber Threat Exchange and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Available training and certification programs include Cyber Essentials, a UK based program that has been adopted by governments in both Canada and the US and a more technically accelerated cybersecurity program offered by The Rogers Cybersecure Catalyst of Ryerson University.

Cybersecurity must be a priority in choosing hardware and software. Cloud services do not absolve businesses and institutions from taking responsibility for their data – cybersecurity requires cloud service providers and their clients to work together and take joint responsibility. All businesses – especially those who maintain sensitive customer data – must have contingency plans in the event of a breach. In order to maintain end-to-end cybersecurity in supply chains, standards and certifications must be built into procurement processes. If the cross-border supply chains that have been cardinal elements of Canada-US trade are to endure and expand, common standards and certifications for Canadian and American companies will be essential.

As new instruments and methods of cyber crime are introduced, the range of highly vulnerable targets is rapidly expanding. For example, ransomware attacks may target institutions like hospitals, universities, municipalities and others who maintain large volumes of sensitive data. Even if these data have little or no commercial value outside the institutions, the value of holding data for ransom depends on how valuable the data is to its owners. This means that public sector focus must shift to protecting assets that were not considered especially vulnerable in the past. In this sense it's very hard to narrow down a set of valuable and vulnerable assets on which to focus protection. Examples of a large UK hospital and a Canadian municipality illustrated the costs and disruptions caused by ransomware attacks.

As new instruments and methods of cyber crime are introduced, the range of highly vulnerable targets is rapidly expanding.

Public and private owners of critical infrastructure such as wireless communications networks, major transportation facilities, power grids, and water and sewage systems, must be especially vigilant. While most businesses and institutions are principally threatened by cyber criminals seeking financial reward, critical infrastructure systems may also be attacked by actors whose goal is not to gain a quick payoff but rather to cause maximum social and economic destruction or even deaths and injuries. These include terrorists and adversarial nations in time of conflict. Wireless networks are especially attractive targets not only because their interruption can bring down the economy but also because they are the densest hubs for data in motion and therefore the ideal targets for intelligence gathering.

The challenges for law enforcement agencies are especially daunting. They face a major human resources challenge because detecting cyber attacks requires the services of experts in IT and cryptography who can earn greater salaries in the private sector. The resources of agencies are stretched to cover a variety of very different threats, with emphasis sometimes shifting between cybercrime and cyber terrorism. As noted above, the growth of ransomware attacks has expanded the range of targets for cyber criminals, so law enforcement must address an ever-broadening range of vulnerabilities. Perhaps the greatest challenge is that cyber criminals adapt to successful law enforcement operations with amazing speed, while law enforcement functions in a domain of rules that often slows down its ability to respond. This may create tensions in policy making, for example between the need to protect privacy and need to provide greater flexibility to law enforcement.

…cyber criminals adapt to successful law enforcement operations with amazing speed, while law enforcement functions in a domain of rules that often slows down its ability to respond

TECHNOLOGIES

Emerging technologies provide powerful new tools for cybersecurity. But in many cases new technology creates new vulnerability as well as new opportunity. Artificial intelligence (AI) is a powerful tool for anticipating, detecting and thwarting cyber attacks. But as AI becomes available more broadly and in more different forms it also allows more sophisticated cyber attacks and more rapid adaptations to law enforcement efforts. Two areas of rapid technological development and diffusion figured prominently in the presentations and discussions at the conference: 5G wireless communications technology and Distributed Ledger Technology.

… the protection of 5G wireless networks against cyber attacks will be a paramount element of national security for both the US and Canada

5G refers to a constellation of interconnected technologies that combine to deliver wireless data communication with greater bandwidth and lower latency than the 4G service that is currently available. 5G will provide much better service in familiar applications, such as downloading videos to mobile devices. It will also enable rapid development in machine-to-machine (M2M) communications in support of the technology paradigm known as internet of things (IoT) where devices are connected online to create integrated systems within which huge volumes of data are transferred. IoT is a broad concept with an almost unlimited number of use cases that will eventually involve billions of online devices. The extremely low latency of 5G communication will also make it instrumental in the control of automated vehicles, allowing information about the position of one moving vehicle to be transferred to another with enough speed to prevent accidents. 5G technology is widely expected to have a pervasive role in all aspects of our lives – economic, civic, health care, military – putting an unprecedented volume of data in motion. It therefore presents a key target to cyber attacks of all kinds.

5G presents some new cybersecurity challenges. Because it generally operates at higher frequencies its antennae are effective over shorter distances. It therefore takes more of them to achieve coverage than with the current 4G systems. As we already noted, there will be far more nodes on the network as the number of connected devices increases by multiples. More antennae and more connected devices provide more opportunities for attack. Furthermore, the connection of many cheap, simple devices that may not be designed with as much attention to cybersecurity as the average smart phone also implies the presence of vulnerable weak links. Finally, the expected ubiquitous role of 5G wireless implies that the level of disruption that can be achieved via sabotage will be enormous. Thus, the protection of 5G wireless networks against cyber attacks will be a paramount element of national security for both the US and Canada.

The general class of Distributed Ledger Technologies (DLT), of which Blockchain is a specific case, holds the promise to enhance not only economic efficiency, especially in cross-border finance and logistics, but also data security. Every DLT implementation provides a continuously updated ledger that is stored simultaneously on the servers of numerous network members, This makes it possible for all parties to any transaction that can be entered into a ledger to have exactly the same information, eliminating the need for time consuming reconciliations and allowing a common visibility of the movement of funds, documents, goods, etc. as they are passed from one network member to another.

The use of cryptographic functions that make it impossible to go back and change the value of any entry after it has been accepted by consensus on the network creates trust among all members by ensuring an undisputed record of the current state and all previous states of the ledger. This is a valuable property from a cybersecurity perspective because even if an attacker were able to hack into the database, any attempt to tamper with values or make fraudulent transactions would be immediately evident to all network members.

The utility of DLT for cross-border supply chains was evident in two conference presentations of systems that have been developed to record and track all movements of goods as they are transported by various means, providing complete end-to-end transparency and supporting payments and compliance with border and other regulations. Such applications, as well as others for things like cross-border interbank transfers, traceability in support of food safety regulations, provenance for compliance with customs regulations, personal identification and accreditation for immigration purposes and others should support greater Canada-US economic integration over the coming years. While it is certainly a mistake to regard DLT as a panacea for cyber threats[1], the high level of trust, visibility and traceability it provides supports unparalleled data integrity. Discussion at the conference noted that while there have been high profile cyber attacks related to Bitcoin, they were not against the core blockchain, which has been resistant to cyber attacks for a decade.

Despite all these advantages, the widespread adoption of DLT is currently held back by a failure to create a set of common standards. ISO standards are in the works, but progress is slow, with only a set of common definitions expected by 2021. It is often challenging to reconcile existing regulations with the peculiar characteristics of DLT. For example, no information that is preserved on the ledger can ever be deleted. This comes into conflict with European Union's "right to be forgotten" if personal identification information is to be entered on the ledger. The lack of common standards means that while narrow networks can define their own standards or adopt one of a set of competing commercial platforms, there is no universal standard. This means, for example, that it is not always possible to build mutually beneficial connections between ledgers.

REPEATED THEMES

Over the course of the presentations and discussions at the conference, four themes repeated:

The first is the challenge of acting proactively and quickly. As already noted, this is reflected in the task for law enforcement and national security agencies to respond to rapidly evolving threats while operating within a framework of laws and regulations. More generally it is reflected in repeated calls to "get out in front" of cybersecurity problems. For example, fixing vulnerabilities in software after it has been attacked is an almost hopeless problem if cybersecurity was neglected in its design. When it comes to cybersecurity, prevention is always cheaper and better than cure. Legacy systems create inertia in IT systems and networks, as outdated and insecure methods of data transfer remain in use, along with old versions of software that do not include cybersecurity upgrades but remain in use because newer versions will not run on old machines. A network is often only as secure as its weakest node or link, so extraordinary efforts to bring laggards up to date are justified.

..fixing vulnerabilities in software after it has been attacked is an almost hopeless problem if cybersecurity was neglected in its design

[1] DLT/Blockchain systems must address technical challenges of implementing security in distributed systems and TCP/IP networks. See https://www.enisa.europa.eu/publications/blockchain-security for a review of cybersecurity in DLT systems.

It is especially important to get out in front of the potential cyber threats to 5G wireless communications networks before they are deployed. If current predictions are correct, 5G will greatly expand the role of wireless networks in the economy and in national security. They will therefore represent an unprecedented vulnerability for those who wish to steal valuable data, hold data owners to ransom, undermine national security or even weaken our defences during a time of armed conflict. In a sense, the long build-up to the launch of stand-alone 5G networks has provided an opportunity to take the necessary steps in advance. The question now is whether there is enough political will to take the necessary steps, even if they may delay or increase the cost of 5G deployment.

An equally prominent theme in the discussions is that systems of laws and regulations must be developed carefully and cooperatively. The seeming contradiction of this second theme with the first theme, which calls for rapid action, only serves to reinforce the reality that nothing about cybersecurity is easy. The two themes together imply that addressing cybersecurity needs to be pushed up the priority list for all levels of government and international organizations.

For example, the idea that data localization is necessary and constructive in the face of threats to privacy and valuable data was criticized on several occasions by presenters and participants in the conference. Political boundaries mean nothing to cyber criminals and attempts to shelter behind them may increase rather than reduce vulnerability. An implication is that if governments cannot focus on their own territory they must naturally cooperate. This is a huge challenge given differences in interests and perspectives. The chapter on digital trade in the recent USMCA/CUSMA agreement, which rules out data localization requirements, has this general orientation. However, the inconsistency between the North American agreement and the EU's General Data Protection Regulation (GDPR), which supports data localization with cause, illustrates the challenge of reaching international consensus quickly. In the near term it may be possible to develop common behaviours, certifications and standards while leaving room for some differences in interest and perspective.

A third theme that pervaded the conference was the reality that certain national governments could act through their domestically based companies to extract information from or interfere with critical data systems. This threat ranges from intellectual property theft to sabotage during times of conflict. This is not just a question of whether there is evidence of malfeasance in the past, but also of what national laws may compel companies to do in the future. Here the focus was clearly on China, whose National Intelligence Law of 2017 requires Chinese citizens and organizations to "support, assist and cooperate with the state intelligence work." Despite denials from its executive, there is expert opinion[2] that this

.. it may be possible to develop common behaviours, certifications and standards while leaving room for some differences in interest and perspective

[2] For example, the Financial Times interviewed lawyers and technology analysts on this question in March of 2019 https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

law would apply to Huawei, a company that has achieved a level of world-leading expertise and production capacity in equipment that is critical to the build-out of 5G networks. The question is then whether the participation of Huawei in 5G networks poses an unacceptable risk to data security – and by extension to national security – for the US, Canada and their allies. One argument is that Huawei equipment may safely be excluded from the "core" of the wireless network where computational functions take place and limited to the "edge" where wireless antennae communicate with mobile devices. This argument is undermined by the 5G strategy of moving intelligence to the edge.[3]

The impending deployment of 5G and the central role of a Chinese company in the supporting equipment industry brings us back to the theme of acting proactively and quickly. While there may still be room for debate on this topic, there is very limited time for it. Excluding individual firms from what promises to be one of the most important global markets for electronic equipment and software may conflict with principles of open markets. But in the short run it may be the only prudent course available. Here, inconsistent policies in the US and Canada could result in limited cross-border connectivity and inhibit the long-established binational cooperation in defense and intelligence.

Finally, a fourth pervasive theme was the need to educate the highly-skilled people who will take up the challenge of fighting cyber crime, cyber espionage, cyber terrorism and cyber warfare. A 21st century workforce must have knowledge of best practices in cybersecurity that extends to everyone who comes in contact with data resources – which essentially means all employees. In addition to the general knowledge of best practices, organizations must employ or contract people with current expertise in the constantly evolving range of cyber threats. Such people require expertise in advanced technical topics such as cryptography, networks, hardware and software design, wireless communications and criminology. Their attention must be focused not only on defending existing systems from cyber attack but also on building cybersecurity into new hardware and software systems and every device that connects to the internet.

While there may still be room for debate on this topic, there is very limited time for it.

Fortunately, the United States and Canada have great capability to educate highly skilled people in the information sciences. The problem is that there is competition among organizations and even among activities within organizations that does not favor allocation of human resources to cybersecurity. As one speaker commented, most developers in web-based software work on the front end (client facing) to the detriment of back end development – a situation he described as "a hacker's dream." Many aspects of cyber security relate to public sector domains such as law enforcement and national security that struggle to compete with the private sector where salaries are higher. Extreme cyber attacks that are likely to occur in the future may drive a shift in human resources to cybersecurity, but it would be preferable to

[3] The strategy is clearly expressed by Intel: https://newsroom.intel.com/editorials/transforming-5g-network-edge-more-power-performance-intelligence/

make the necessary adjustments without first suffering such dire consequences.

NEXT STEPS

Presentations and discussions at the conference identified several unresolved issues regarding cybersecurity as it relates to the preservation and enhancement of the Canada-US relationship. These issues suggest some next steps that include, but are not necessarily limited, to the following:

- DLT, 5G and general standards and practices for cybersecurity are likely to transform the operation and regulations of supply chains in the coming years. Since integrated cross-border supply chains are essential to mutually beneficial Canada-US trade, intense binational cooperation on research and policy formulation is needed to ensure that new standards and practices facilitate, rather than retard, cross-border supply chain integration.

- These same technologies have great potential to increase the efficiency and security of border processing operations – including customs, immigration and border security – both at and away from ports of entry at the major Canada-US crossings. (For example, 5G wireless may make it easier to transfer compliance data and digital tracking data from a vehicle to the port of entry prior to its arrival.) A cooperative effort by US Customs and Border Protection and the Canada Border Services Agency to adopt common standards, data formats and certifications will help realize the full potential of these technologies for both border security and trade facilitation.

- 5G wireless communication promises to play a broader role in economic activity than the current wireless technology. For this reason, inconsistency and poor connectivity between 5G systems built out in the US and Canada could have serious consequences for Canada-US economic integration. (For example, significant differences between domestic and cross-border data transfer speeds could create a significant non-tariff barrier to digital trade.) It is in the interest of governments and wireless service providers in both countries to coordinate build-out activities and choices. This applies to, but is not limited to, the eligibility of equipment suppliers.

- Highly qualified people are both the most important and the most limiting resource in the fight against cyber crime, cyber espionage, and cyber terrorism. Canada and the United States can benefit from pooling human resources in this area. This can be achieved both through cross-border movement of people with expertise and through cross-border trade in technical services. Immigration and trade provisions should be reviewed to identify opportunities to more efficiently marshal human resources for cybersecurity.

CROSS-BORDER INSTITUTE