DATA & INFRASTRUCTURE SECURITY: THE RISK OF AI ENABLED CYBER ATTACKS AND QUANTUM HACKING

Date: November 21, 2022

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 21, 2022, Dr. Ryan Prox, Adjunct Professor in the School of Criminology at Simon Fraser University, presented Data *& Infrastructure Security: The Risk of AI Enabled Cyber Attacks and Quantum Hacking*. A question-and-answer period with the audience and CASIS Vancouver executives followed the presentation. The key topics discussed were the evolution of data and infrastructure security, the increasing interconnectedness of critical infrastructure, and the need to increase resilience in the face of revolutionary technological advancements.

NATURE OF DISCUSSION

Presentation

Dr. Prox discussed the evolution of data storage and security, emphasizing the transition from simple networks to Cloud Services and the impacts on critical infrastructure security. He addressed the evolution of the technology industry and its eventual transition to Quantum Computing. He also examined the need to make critical infrastructure more resilient in order to mitigate potential risks.

Question & Answer Period

Dr. Prox suggested that the profit-driven nature of the private sector has led to gaps in forward-thinking investment regarding critical infrastructure. He recommended that legislation must seek to increase vendor accountability as a means of incentivising investment in security.

BACKGROUND

Presentation

Dr. Prox began by providing an overview of the technological landscape, noting a definitional understanding of key concepts as essential to navigating data and infrastructure security. He highlighted Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Big Data as essential concepts in the field. AI, broadly defined, is any human cognitive function carried out by a machine, whereas ML is a subset of AI consisting of a set of algorithms that interpret structured data to complete a task without explicit programming. DL uses a layered structure of ML algorithms known as Artificial Neural Networks (ANNs) which can learn, train, and restructure their neural pathways to obtain better results. Big Data refers to the analysis of vast amounts of information that cannot be processed manually or through simple computation.

Dr. Prox noted that in the past five years there has been a transition from data stored on simple networks to Cloud Services capable of consuming entire industrial centres containing thousands of processing cores. He explained that the industry focus has changed from the internet as related to people to the Internet of Things (IoT), and has shifted to an emphasis on machine-to-machine efficiency. Dr. Prox pointed to the growth of IoT projects globally, citing the example of increased investment in “Smart Cities” and interest in the “Connected Industry”. Europe leads North America in Smart City projects and investment; however, the Americas represent 55% of global Connected Healthcare projects. Dr. Prox emphasized that there is a transformation occurring in the way industries are moving towards digital automation and interconnectivity, pointing to a drive towards Cloud Computing and data storage for major industries.

Dr. Prox then discussed critical infrastructure, defined as all assets, systems, and networks—whether virtual or physical—that are essential to the proper functioning of society's economy, public health, safety, and security. He pointed out that, in Canada and the US, much of the Critical Infrastructure is owned and operated through the private sector, which potentially creates security issues. He mentioned that surveys have revealed limited incentives for the private sector to invest in advanced infrastructure security measures in some cases, and a willingness to tolerate a certain level of risk for cost-effectiveness in others. Dr. Prox suggested that cost can lead to neglect in investigating errors and mitigating risks for “what if” scenarios. However, even though these events may have low probabilities, their potential high impact necessitates that systems are in place to address vulnerabilities.

Dr. Prox stated that Critical Infrastructure, which was historically operated on closed systems, is now frequently run by Industrial Control Systems (ICS) containing Supervisory Control and Data Acquisition (SCADA) systems, which automate industry processes. Nearly all ICS are now hosted on Cloud Services—which are susceptible to coordinated attacks—and attacks on SCADA systems or other ICS have the potential to compromise vital systems, such as disrupting electrical grids, water supplies, communication, and banking. Dr. Prox noted that only five vendors dominate the hosting of critical infrastructure Cloud computing services, which could result in a cascading effect in case an attack or catastrophic failure. As an example, he cited the Canada-wide system failure of Rogers Communications in July 2022, which had a significant impact on many emergency services, banking, and public transportation systems.

Dr. Prox discussed the threat of Malware attacks as critical infrastructure becomes more advanced and relies more on Cloud Computing and Networked ICS, creating interdependencies that are vulnerable to cyber-attacks. The latest evolution of AI-powered Malware is designed to independently target systems while intelligently evading detection. An example of this is DeepLocker, a program developed by IBM. Dr. Prox explained that the program employs a Deep Neural Network (DNN), an AI model that controls the trigger conditions to execute its objectives. This can potentially be utilised for data theft, critically disabling systems through destructive encryption, or triggering of catastrophic outcomes, such as releasing flood gates on a dam or causing power generation facilities to fail.

Dr. Prox mentioned that, so far, there has been no recorded criminal use of AI-enabled cyber-attacks. However, the possibility of weaponized AI Malware being used by some states' intelligence services is a concern. Tests have shown that conventional cybersecurity methods are easily bypassed during DeepLocker attacks. To counteract AI-enabled malware, Dr. Prox suggested the use of AI-enabled tools to assess and manage cyber risks to critical infrastructure. These tools can prioritise risks based on their likelihood and respond automatically when triggers are identified.

Dr. Prox concluded his discussion with a focus on Quantum Computing, a remarkable development that has spurred intense competition in the technology industry to create a commercially viable product. Despite the fact that this goal has not yet been achieved and is at least a decade away, Dr. Prox argued that the eventual arrival of commercially viable Quantum Computing will have a profound impact on the security landscape. Governments are preparing for the security challenges of the Quantum Age by transitioning to Quantum-Safe Cryptography, modifying current cryptography to make them more resilient.

Question & Answer Period

Dr. Prox emphasized that the private sector is driven by profit and there is little motivation to invest in security if it is not profitable. He used the example of the energy infrastructure in the US, where many States have suffered from lack of investment, leading to more power outages than any other developed country. To address this issue, there must be incentives for the private to prioritize security. In Canada, organizations such as the Communications Security establishment Canada (CSEC) inform private sector industries about security risks.

Dr. Prox also discussed Bill C-27, an omnibus legislation in Canada that contains the Artificial Intelligence and Data Act. This legislation is significant, as it includes provisions for the imposing substantive fines for privacy breaches and the assignment of liability to private sector organisations found in violation. Previously, there were limited options for recourse in the event of a privacy or security breach due to negligence. Under Bill C-27, vendors are directly responsible for any breaches or compromise of their systems, which may encourage greater investment in cybersecurity.

KEY POINTS OF DISCUSSION

Presentation

- The transition from data storage on simple networks to Cloud Services has led to an increased focus on the Internet of Things (IoT) and an emphasis on machine-to-machine efficiency, as evidenced by increased investment in “Smart Cities” and interest in the “Connected Industry”.
- In Canada and the US, much of the critical infrastructure is owned and operated by the private sector, which raises concerns as there may be limited incentive for the private sector to invest in advanced infrastructure security. In some circumstances, there may be a willingness to accept a degree of risk, as it can be more cost-effective.
- Almost all Industrial Control Systems (ICS) are now hosted on Cloud Services, which are susceptible to coordinated attacks. In the event of an attack or catastrophic failure, there can be a cascading effect on the critical infrastructure operated by a very limited number of Cloud Computing service providers.

- To counter AI enabled malware, AI powered tools are needed to evaluate and mitigate the cyber risks to critical infrastructure. These tools can prioritise risks based on the probability and respond to triggers they identify.
- The arrival of commercially viable Quantum Computing will transform the security landscape. Governments are preparing for the security challenges of the Quantum Age by transitioning to Quantum-Safe Cryptography and modifying their current processes to enhance resilience.

Question & Answer Period

- The private sector is motivated by profit and will only invest in security if it is profitable. For instance, the United States has seen an ongoing and protracted lack of investment in the energy infrastructure, leading to a higher rate of power outages than other developed countries.
- In Canada, organisations like the Communications Security Establishment Canada (CSEC), reach out to private sector industries to raise awareness of security risks.
- Bill C-27, including the introduction of the Artificial Intelligence and Data Act, aims to increase investment in security by placing direct accountability on manufacturers.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/