CYBER SECURITY IN AN INFORMATION WARFARE AGE

Date: October 18, 2018

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

KEY EVENTS

On October 19th, 2018, the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its ninth roundtable meeting which covered "Cybersecurity in an Information Warfare Age." The following presentation was hosted by Dr. Steven Pearce, a lecturer in the School of Computing Sciences at Simon Fraser University and an astrophysicist by trade. Dr. Pearce has over 30 years of experience in mathematics and technology, focusing on the theory of technology and socio-technology. In his presentation, Dr. Pearce used these themes to highlight how technological advancements accelerated the destructive capabilities of humans, while simultaneously warning of conflating cyberwarfare with information warfare as it detracts from their unique underpinnings and objectives. The subsequent roundtable discussion centered around a case study where Chinese microchips that create backdoor access to systems were found embedded in server motherboards that Amazon purchased. After discovery, they were allegedly shown to have been distributed to banks, companies and US defence agencies. Thereafter, audience members discussed the security implications of hardware hacks and what the Canadian government and citizens could change to safeguard against both software and hardware hacks.

NATURE OF DISCUSSION

Presentation

The presentation first defined cyberwarfare and information warfare. Then, cybersecurity was examined through the lenses of five maxims: aggression is a key factor of the human condition, offense is easy – defence is difficult, privacy

is dead, technology evolves much faster than the law, and security has become big business.

Roundtable

The roundtable discussion focused on both the security and economic implications of technological hardware being outsourced to other countries. The case study presented how the Chinese government has the advantage of being able to attempt a hardware hack early on in the supply chain. Moreover, the patient and resource heavy nature of the attack suggests a long-term goal of accessing intellectual property and defence systems rather than the personal information of citizens.

BACKGROUND

Presentation

Under Maxim one, Dr. Pearce describes warfare from a scientific perspective: as an extension of animal behaviour that is naturally aggressive. He suggests technological advancement has accelerated the implications of human aggression. Additionally, warfare has transcended the traditional model to include non-state actors.

Information is observed data combined with systems required to give the data meaning. Therefore, the security challenges are opponents who directly act upon the information rather than indirectly influence information, as was done in the past. Information warfare is the weaponization of information, an example being the Russian activity in the 2016 U.S. election. Information warfare has arguably been conducted well before the invention of the internet and the connectivity of social media, human advancement merely changes the realm, reach, and speed in which this is done. Dr. Pearce shows how sending toothbrushes to troops instead of bullets is an example of meddling within information systems.

In contrast, cyberwarfare is the attacking of systems. Encryption and decryption are considered to be munitions and could be viewed as weapons of war. The word cyberwarfare is often misused by the media in order to mobilize people, which contributes to the definition being unclear.

Under Maxim 2 Dr. Pearce emphasized that offense was much easier than defence, and the fundamental assumption that there is no fully secure system.

Several audience members expressed agreement that a Cyber Pearl Harbour was possible in the future given Canada's arguably current lack of vigilance in protecting information and information systems.

Dr. Pearce presented a cyber threat taxonomy which identified the motives, targets of opportunity, methodologies, and capabilities of nation-states, pranksters and organized crime syndicates. It is suggested that in peacetime, nation-states have the same targets, methodologies, and economic, military and political motives as they do in times of war.

There are three target landscapes of cybersecurity: national security (intelligence and counter-intelligence), personal security (personal databases in a free society), and corporate security. It was argued that these three realms are naturally in conflict when in a surveillance society.

Another issue brought forward was the competitive nature of quantum technology research. A 2016 Veracode study revealed that cryptographic (coding) issues were the number two vulnerability found in apps in 2016, second to information leakage. There has been an ongoing quantum computing rush by nation-states to spend money on quantum technology research due to the fact that should one state vastly exceed the other in capability, protection mechanisms of the state security systems can quickly become obsolete.

An economic aspect of cybersecurity is that a constant threat is beneficial to businesses that sell system protection. The cyber landscape shows signs of these attacks significantly accelerating, and it is suggested Canadians should be increasingly critical in disentangling what is real from what is an exaggeration.

In Maxim 3, Dr. Pearce claims that privacy is dead, arguably, due to the complacency of citizens. It was shown that the Canadian government has greatly surpassed the Stasi in its surveillance of Canadians, and a potential cause is the apathy of citizens. He suggests that protecting the homeland is a necessity, but, comes at a cost.

It is also noted that a private company, Google, has arguably more advanced cyber capability than the Canadian government, leading to Maxim 4: technology evolves much faster than the law. Given that the law is based on legal precedent, technology can evolve at a significantly faster rate, and thus, is not bound by law.

Maxim 5 is that security has become a big business. The surveillance state has arguably changed information technology security, launching momentous increases in defence spending.

Dr. Pearce concluded with the example of U.S. government census data being used to round up Japanese-Americans to place them in internment camps. It was codified law that information provided in the census would in no case be used to the detriment of respondents, yet in 1942 it was.

Roundtable

When asked whether system penetration rates will rise in societies with quickly evolving technology, Dr. Pearce answered that it would depend on how well coders understand the physical model of what they are trying to test. For example, when verifying the safety of a vehicle researchers study the physics of a crash, but in the realm of cybersecurity there is no physical model.

Dr. Pearce then presented the Logistic Map, which is a simple non-linear equation. This equation runs in a circular manner, doubling at every step, and diverging to the point of chaos after 35 steps. The Map demonstrates the limitations of knowledge and prediction. Therefore, applying a linear framework in kinetic warfare has functioned in the past, but it cannot be applied to cyberwarfare with the assumption that the outcome will be correct.

When discussing AI, it was argued that the human mind cannot manage the complexity of the type of code we have been developing. Therefore, code should be written by "intelligent code", meaning code should write itself. Humans lack the specification to be able to calculate several outcomes and select the best one immediately, where AI has the potential to do this. Because of this, software engineering could be coming to an end.

In addressing what has changed in the landscape since he began his career, Dr. Pearce said the socialization of the internet, the complacency of people regarding their information and security, the scale of previous security challenges and the omnipotence of computers. AI was once considered a failure, whereas it has currently reached new heights despite humans being unable to create neuro-networks artificially.

It was argued that because cyberwarfare has the potential for kinetic implications, it could be looked at more simply as war in another operational environment. The

Chinese book *Unrestricted Warfare* details methods of war outside of direct confrontation and is currently in use by the Chinese government. Academics in China will openly state they are at war with the United States, yet it is a matter of debate whether a cyberoperation run by the state is considered a declaration of war in a North American context.

In relation to the smart city phenomenon, the audience provided that there are several vulnerabilities in the movement. New technologies are, arguably, often more susceptible to bugs. Therefore, those at the forefront of these advances are the most at-risk for hacking. Data collection in smart city models also creates paranoia among those in the population with an aversion to information sharing.

Case Study Presentation

Four companies located in China were subcontracted to create server motherboards for a company called Supermicro, and investigators concluded that a special arm of the People Liberation Army had tricked, bullied, and/or bribed these subcontractors to insert microchips that created back-door access into the boards by allowing access to the baseboard management control.

The Bloomberg report released on October 4th, 2018, stated that the boards were distributed and assembled into computers over a two-year period that reached almost thirty institutions, including a major bank, government contractors, Amazon, and Apple. Bloomberg claims their report is backed by 17 sources, including U.S. government officials and Apple insiders.

This was not presented as an attempt to access consumer information or steal credit card numbers. Hardware hacks are more difficult to succeed in, promising long-term, stealth access that intelligence agencies are willing to invest millions of dollars and several years in.

It is argued that China has a unique advantage in hardware hacking, as they control the majority of computer and mobile phone part creation, allowing them to attempt the hack early in the supply chain.

Some say that other states cannot do this and must use interdiction, which is a less cost-effective way of hardware hacking. The interdiction method would insert the chip in the middle of the process, meaning the chances of infecting the target systems are less likely. For example, this hack required four companies to contain the chip, whereas later on it in the chain it could require dozens. This is

because the higher up the supply chain, the more companies there are to supply to, meaning more resources are required as well.

Case Study Roundtable

Dr. Pearce argued that this act of aggression by the Chinese was reactive and happens on both sides. The prominently suggested way to defend against hardware hacks is to remain hyper-vigilant. This type of attack is asymmetric, where China can leverage their ability to provide cheap technology against the West. The audience expressed a lack of political will and urgency on Canada's part in invigorating the movement towards additive manufacturing.

When discussing the manipulation of onboard systems by a foreign power, an instance arose of an F-15 Eagle being taken down by a man with a rifle in Texas. This event never came out publicly, as it could show a great vulnerability. Therefore, it was argued that Canadians should recognize the extent to which these instances are occurring out of view.

When discussing using the chips to spread disinformation, it was said that although difficult it has the potential of being likely if the goal is only to spread uncertainty.

Viewing the case study from a business perspective, it is not feasible to change the market as China is skilled in the creation of parts and can manufacture them for much cheaper. If the U.S. were to move towards producing servers within their borders, it would slow the manufacturing time down substantially. It was argued that President Trump is attempting to bring manufacturing into the U.S. again from an industrial perspective and may have missed the security benefits of keeping electronic parts with sensitive data in-house.

This instance is not new and can be applied to the concept of sleeper agents in the past. What has changed is the speed at which we can now experience harm, and because of this, we should change the way we view asymmetric warfare to include more creative ways of assessing threats.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Presentation

- The distinction between information warfare and cyberwarfare should be made in order to formulate effective defences against both: information

warfare is the weaponization of information, cyberwarfare is an attack on information systems.

- For nation-states, cyberwarfare will arguably still have the same motives, methodologies, and targets in times of peace, and attacks could be looked at as a disruption of peace, not as something occurring as an aside because it may fall just short of kinetic in capability. Both are acts of war, the only difference being the operational environment.
- The apathy of the average Canadian citizen towards privacy and security could pose a security risk in itself.
- Applying linear thinking to kinetic warfare has worked in the past but moving forward, Canada could be considering non-linear approaches to cybersecurity, while at the same time remembering the Logistic Map.

Roundtable

- Some have argued that there should be a shift in how the Canadian government views cyberwarfare and information warfare that encourages a proactive approach to defending from these attacks. Being unable to change how we view these attacks could leave Canada vulnerable. Some argued that more creative offensive and defensive approaches to cybersecurity challenges should be considered.
- Canadian citizens on the West Coast are, arguably, far removed from the realities of security issues, which could leave them more susceptible to economically and socially devastating cyberattacks and scams in the cyber realm.
- Audience members argued whether or not the hardware hack report was factual or not is not important, as it was made real by the plausibility of such an attack, demonstrating where Canada could also be exposed.
- Creating policy forbidding foreign hardware could serve to drive out leading technological companies from Canada and disrupt the economy.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/