COVID-19: CHINA'S FOREIGN POLICY IN THE SOUTH CHINA SEA

Date: July 16th, 2020

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

KEY EVENTS

On June 2nd, 2020, the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its second digital roundtable event of the year titled, "Privacy and Security: Working Hand in Hand to Protect You Online." This presentation featured Dr. Patrick Neal who has been involved in the public safety field since 1982. Dr. Neal's presentation focused on the cohesiveness of privacy and security in the near future, privacy constructs, myths and harms of privacy, and privacy enhancing technologies. The subsequent roundtable discussion centered around Dr. Neal's lecture in a question and answer period.

NATURE OF DISCUSSION

Presentation

The digital roundtable discussion focused on areas of privacy and security in which its constructs, benefit and harms, myths, and privacy enhancing technologies were laid out to examine. Additionally, current debates highlighted the importance of balance between cyber defense and civilian security. With the increasing innovations of privacy enhancing technologies, questions may arise surrounding the enforcement of privacy regulations.

BACKGROUND

Presentation

Privacy problems that we are now dealing with not only have an impact on police officers but have hindered them from doing their job as well. When Anonymous, an international collective who target government institutions and corporations, dumped personal data online of various police forces across the northern United States, it illustrated that the people who we thought were untouchable in such a direct way, such as the people of state or people of government, were now having to deal with their own concerns and dynamics. However, on the other side, we have an example of a police officer making use of open sources to find a woman who set a police cruiser on fire through a tattoo that was on her arm in a picture that was taken moments before the incident.

'Privacy is dead, I have nothing to hide' is in fact a myth. There are things that we ourselves want to keep private for the purposes of our mental health. Being mindful of the things we post publicly is how we are going to protect our privacy which is tremendously important for our professional development and professional status.

Many privacy enhancing technologies are being developed to counter some of the ongoing issues. Currently, encryption keys are used to attack privacy problems. However, in the next couple years, we will be able to use homomorphic encryptions which will be able to break off, leaving the attacker stuck within. In theory, once it is broken off, there is no way to crack it. Another privacy enhancing technology that is being researched is smaller AIs. However, the development of smaller datasets within our cellphones that can do the same things that a big data engine can do, may cause more problems for security teams in the near future.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Presentation

- It is everyone's responsibility to know the common principles that privacy is grounded in and how they are applied.
- When developing national security and public safety strategies, the balance of the pros and cons of privacy need to be prominent.

- Gen Zs will be coming into the workforce looking to balance their privacy with their workplace transparency. Privacy enhancing technologies will assist them best in accomplishing this.
- There is no sure way of deleting your personal data once it has been uploaded onto the internet or in a database.
- We need to shape public policy to influence forensic analysis, identity management, and privacy in the new era of anonymity, so we are prepared for the acceleration in privacy enhancing technologies that we will be seeing in the next 5-10 years.

Question Period

Other suggestions for citizen protection against privacy breaches were discussed:

- Most breaches take approximately 180 days to discover and up to two years before one can finally get an idea of what they are up against.
- Once a breach has been identified, a citizen calls the privacy commissioner's office for the companies that possess these and/or the government with authority.

Other challenges to brain manipulation and human weaponizations were discussed:

- Once one has agreed to their brain being present, then they have agreed to receive feedback from an object.
- Current research shows that brain performance can be modified. There is risk of hijack when we are able to plug in soldiers and through their brainwave patterns, monitor and control ammunition, firearms, and drones.

Other solutions to enforcing privacy regulations were discussed:

- Citizens have to be held accountable for the content they post online and the sites they utilize.
- Corporations incentivize privacy and security as a profit center. Once money is tied to this, people will start to see its worth and begin building up these instruments. The government has to step in here and provide the incentivization model.

Other suggestions for the maintenance of cyber defense and civilian privacy were discussed:

- Like community/blockwatch policing, if you agree to be a part of a cyber community, you agree to participate in defending yourself and others if there is an attack.
- In order for active cyber defence to work, we must get around the revenge, retaliation, and retribution problem.

Other suggestions for the kinds of power that law enforcement should possess were discussed:

- The ability to compel the privacy legislation to actively participate in debates around national security.
- The Law Enforcement and National Security Parliamentarian Committee needs to push the mandate that the breach of someone's privacy is a law enforcement problem, not a civil problem.

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

Available from: https://jicw.org/