CYBER INVESTIGATION: A NEW FRONTIER FOR POLICE

Date: November 26th, 2020

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 26, 2020, Kathy Macdonald, M.O.M, presented on Cyber Investigation: A New Frontier for Police at the 2020 CASIS West Coast Security Conference. The main points discussed were centered on the evolving nature of cybercrime, the resulting challenges, and steps forward to address the security issues it presents. Following the presentation, there was a question and answer period to allow for attendees of the conference to engage with Kathy Macdonald's presentation and the topic of cybercrime.

NATURE OF DISCUSSION

Presentation

The speaker highlighted the challenges faced by police and law enforcement in the area of cybercrime, the role COVID-19 has played in exacerbating security issues in this space, and provided potential pathways forward.

Question Period

During the question period, discussion centered on how the misunderstanding of cybercrime and barriers to transnational cooperation complicate investigations for police and law enforcement.

BACKGROUND

Presentation

Cybercrime in the 21st century is transnational, multi-jurisdictional, and continuously evolving. The complexity of cybercrime networks and the ability of cyber criminals to constantly change and develop is a security issue by way of posing a challenge to police investigations.

There has been an exponential growth in cybercrime in the past year. Some illustrations of this growth are increased instances of youth sexual exploitation in Canada; a rise in revenge porn in Australia, India, the UK, and the US; and higher cases of cyberbullying in Australia.

Police investigations are inundated with data regarding such crimes and are often overwhelmed with how to effectively and efficiently investigate in the cybercrime space. Given the enormous amount of cybercrime, police have to do ‘triage’ in order to focus on what they can realistically investigate and tackle. Along with an overwhelming amount of data, further hindrances to their efforts include a lack of training for police investigators and frontline officers, and budget issues that decrease the capacity and availability of special units. How can police stay on top of every reported case if one investigation of reported revenge porn could potentially take up to two years? A lack of information sharing channels among practitioners and experts, as well as these types of crimes going under-reported provide further challenges to cybercrime investigations.

Although adapting technology and tactics has allowed cybercrime to grow and evolve even in isolation from COVID-19, the changes in the online space brought by the pandemic has been harnessed by cyber criminals to cause more damage.

The adaptive nature of cybercriminals takes advantage of the uncertain times and the vast increase in usage of technology. COVID-19 has resulted in feelings of loneliness, isolation, and fear which has individuals turning to virtual spaces for everyday tasks, as well as guidance. This landscape has provided the ‘perfect storm’ for social engineering and cybercrime to easily manipulate users. Social engineering takes advantage of uncertainty and fear to provide click bait on things like a curiosity to follow COVID-19 news stories or to buy PPE (personal protective equipment) where supplies are dwindling. Additionally, there has been an increase in identity theft and financial fraud in Canada during COVID-19. It is from this context that one can clearly see the complexity of security issues and challenges that police investigators face in attempting to command in the cybercrime landscape.

Police forces would be well-served by working proactively to educate the public on cybercrime before they are taken advantage of. Being proactive will arguably reduce fear by addressing the issue and delivering the message directly from the police, rather than after the fact in sensationalized media stories. Continued education about cybercrime, rather than a one-time concentration of information would benefit the public by creating awareness around how emotions are utilized in social engineering and which tactics to watch out for. Further, information about cybercrime needs to be easy for every-day users to understand and digestible by all ages of individuals who are online. More open and available resources are needed in order to empower the public to save evidence, set up alerts, and monitor their own PII (personally identifiable information) to address the information void.

Lastly, it is the responsibility of everyone in the online space to be informed about cybercrime and to take action. It is important that users know how to report what is experienced to preserve security in online spaces and avoid the suffering of those involved.

Question Period

During the question and answer period, points were raised about how legislation and legal issues may be contributing to the challenges law enforcement in Canada experience in attempting to address cybercrime. There needs to be more clarity in legal codes and legislation pertaining to cybercrime and cyber bullying. In Canada, there may be misunderstanding about what is actually considered to be cyber bullying. It is not merely a threat experienced by youth or teenagers. It can affect someone of any age and has the potential to have devastating effects on its victims.

Of another legal nature, the sometimes transnational nature of cybercrime results in barriers regarding information sharing and communication between law enforcement agencies across borders. A formal process and multilateral treaty agreement to ask for assistance from police in other countries can take up to eight months, all the while money and information continue to move and adapt during this time span.

KEY POINTS OF DISCUSSION

- Cybercrime is continuously evolving and has adapted to take advantage of the current COVID-19 landscape.
- Law enforcement are overwhelmed with cybercrime investigations and need to be proactive in order to prevent crimes from happening in the first place.
- There needs to be more clarity in legal codes and legislation pertaining to cybercrime and cyber bullying to keep up with the reality of this developing landscape.
- More training, infrastructure, resources, and funding is needed to support investigations in the dark web.

- Continuous and digestible information is required for online users to educate themselves or those close to them on cybercrime.

- It is everyone's responsibility to report cybercrime.

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