ONLINE NEIGHBOURHOOD PATROL: HOW TO BEST UNDERSTAND THE CHANGING ONLINE SOCIAL CONTRACT

Date**:** November 25, 2021

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 25, 2021, Kathy Macdonald (M.O.M.), former Calgary Police officer, presented on *How to Best Understand the Changing Online Social Contract* at the 2021 CASIS West Coast Security Conference. The presentation was followed by a question and answer period and a breakout room session with questions from the audience and CASIS Vancouver executives. The key points discussed included the knowledge, skills, and abilities required for police work in dealing with forensic cyber investigations and processing digital evidence, as well as building community relationships.

NATURE OF DISCUSSION

Presentation

Ms. Macdonald's presentation centered around the challenges that advances in technology has brought for police services, as well as the integration of community policing with online communities as the advent of social media has led to the formation of more online networks. Some of the pros and cons of the Internet of Things and how some individuals are misusing it were also discussed.

Question Period

During the question and answer period, Ms. Macdonald provided some of the key aspects to keep in mind when forming a community blockwatch. The importance of building trusted relationships with experts in the cyber space and what the next step on cybercrime and fraud prevention could be were also discussed.

BACKGROUND

Presentation

Ms. Macdonald began her presentation by reflecting on her own experience while working on crime prevention for the Calgary Police Service and noted that back in the early 2000s, the main subjects of discussion were identity theft, viruses, trojans, and worms. However, after Facebook emerged, other problems such as cyber bullying and luring started to arise, but investigators working on high tech crime were focused on forensics on cell phones and computers. In addition, there was not a lot of communication or interaction between investigations and community policing departments although they had a common purpose. Ms. Macdonald noted that police efforts as of late, have strengthened as they begin to recognize the value of awareness, education, and training in cyber security.

Often, cyber criminals' intent is financially focused, but it could also be for political gain or recognition, and they can range from simple opportunists to very sophisticated organized crime groups and state-sponsored foreign actors. Most importantly, they do not discriminate between age, gender, or occupation; they prey on individuals, business, schools, and hospitals. Cyber criminals now have better access to tools, techniques, and procedures for social engineering and to remain anonymous. They can do reconnaissance, open-source intelligence gathering on social media, event staging based on news cycles, and share information on the dark web. These new criminal trends add challenges and complexity to police services because cyber criminals know more about their victims and the investigative techniques used by the police.

Ms. Macdonald noted that the pool of victims of cybercrime has grown, as well as the age gap. Some members of the community may not be aware that they are being victimized, or they do not know what to do once they learn they have been victimized. This unawareness becomes a problem in and of itself because some victims, who have ransomware in their computers, might just end up going to a computer-related service instead of reporting it to the police.

Lack of training constitutes another layer of the challenge, Ms. Macdonald noted. Not every police officer is an expert forensic investigator, nor do they want to be, but increasingly, police agencies are starting to deliver cybercrime training in recruit training classes. There are huge demands on forensics. For example, high-tech crimes units have to deal with large quantities of seized mobile and computing devices and process different platforms used for different kinds of crimes. This takes a great deal of time, expertise, and tools.

Some additional challenges for police officers in the context of cybercrime when responding to calls from the community, is not having a standardized response to complaints from the public for investigation or the prevention advice shared with victims of fraud or revenge porn, for instance. This scenario has created a situation whereby some police services in Canada now possess expertise in investigation and great capability when handling complaints involving a variety of cybercrime. However, the velocity of changes on the Internet of Things introduces an unknown factor and poses a great challenge to police services because they are often the last ones to get involved.

In terms of the online social contract, Ms. Macdonald highlighted that communities expect the police to respond, understand the technologies they are using, and investigate and protect them not only now but also in the future. However, Ms. Macdonald noted that when it comes to cybercrime, it is very difficult for police forces to do that but informing the community and ensuring that they understand that anything that. She reiterated that it is imperative that the public understand that if it is against the law in the real world, it is against the law in the virtual world, and it should be reported to police. However, online sexual exploitation and coercion, revenge porn, cyber bullying, and financial crimes have increased exponentially during the pandemic, and it has become difficult for police services to keep up. Some of the reasons this has become a problem is the lack of standardized reporting, responding, and investigating. Additionally, the police might not get the full forensic narrative since they are often the last ones getting involved.

Ms. Macdonald concluded her presentation by pointing out that the Internet of Things has created fantastic and innovative devices, such as doorbell surveillance cameras, which can sometimes contain images of thefts or other incidents, so police are increasingly having to handle digital evidence from devices owned by the public to monitor their property. Sometimes these devices are scooping up too much information and are surveilling the public or other houses, which can become an issue of spying, voyeurism, or casing a place for break and enters. Similarly, indoor security cameras are sometimes hacked and personal activities are streamed online for the world to watch because the owner is not aware of the risks to privacy. The Internet of Things is a very dynamic area, and it is a new frontier for police services and one that Ms. Macdonald believes will become a greater challenge for police in the future.

A current concern is that since the community knows the police cannot always respond to and investigate everything, they are starting to take matters into their

own hands. They create a group on a private messaging platform and then communicate ongoing incidents they might witness, which can be read by other people in the area considering intervening. It is crucial for the police to work with the community, look at future technology, get everyone up to speed on cybercrime, and look at the value of prevention and proactivity. Teaching children and seniors about cyber security is a great way for the police and the community to start working together.

Question Period

When asked for advice on starting a blockwatch, Ms. Macdonald stated that it is important that police have a role in these virtual spaces and be available to offer advice when required, help to keep people engaged, direct the organizer in the right way and be involved in criminal matters. The police should try to be aware of what is happening in the community and build trust. Finding a common ground can allow them to work together despite how different their backgrounds might be. When it comes to finding solutions to a problem, it is easier when there is common ground.

When asked whether she thought that the complexity of the cyber situation could result in subcontracting smaller private companies for a better chance to address the issue, Ms. Macdonald pointed out that within the Calgary Police Service, they work diligently on building relationships with trusted groups and individuals. Input from subject matter experts is very important, but the field is very broad and not one single individual is an expert on everything. Building those trusted relationships takes time, and it is important for police leaders to understand that it is essential for police officers to build those relationships, and be given support to attend conferences and improve their education in such an evolving field.

Additionally, Ms. Macdonald stated that cyber criminals have taken great advantage of the pandemic by working on people's emotions and fears, which is why there has been an exponential increase in fraud and many other problems related to social engineering. Ms. Macdonald noted that the best way to counteract this is by encouraging leaders at all levels to take opportunities to get out in front to reassure and calm people down because cyber criminals have been attacking emotions, including urgency and fear that cause people to do things they would not normally do against their better judgment.

When asked what the next step on cybercrime and fraud prevention was, Ms. Macdonald noted that there needs to be an opportunity for the police to get involved from the beginning in some way. Private companies need to take more

responsibility and provide better explanations instead of just releasing devices without letting people know the precautions they need to take. The private industry has unfortunately profited from people who do not take the time to read the privacy policies, making billions of dollars from people's personal information and without regard for others. She believes a portion of these profits could be put towards supporting community policing and the community itself by ensuring proactive awareness and reiterated that she does not agree with initiatives that try to defund the police. It is also important for police officers to receive standardized prevention training and know where to direct people for good information.

KEY POINTS OF DISCUSSION

Presentation

- Police efforts have strengthened as they begin to recognize the value of awareness, education, and training in cyber security.
- Anonymity and access to better tools, techniques, and procedures for social engineering add challenges and complexity to police services because cyber criminals research their victims and learn the investigative techniques used by the police.
- Community's lack of awareness of what cybercrime looks like or how to deal with it is a huge problem for police services causing many cases to go unreported.
- Lack of standardized knowledge or ignoring what the best advice might be regarding cybercrime prevention are also some challenges that police officers face when responding to calls from the community.
- The velocity of changes on the Internet of Things has introduced unknown factors that pose a great challenge for police services and potential liability when dealing with cybercrime because they are often the last ones to get involved.

Question Period

- When forming a community blockwatch, it is important not only to keep members engaged but also to include the police when there is a criminal matter.
- Although it takes time, it is crucial for police services to build trusted relationships with subject matter experts when dealing with cybercrime; the field is very broad and not one single individual is an expert on everything.

- Cybercriminals have taken advantage of the urgency and fear that the pandemic has induced in people, often making them act against their better judgment.

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

Available from: https://jicw.org/