CASIS~VANCOUVER~ACERS

SAPERE AUDE

POLICING IN THE 21ST CENTURY

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, Dwayne McDonald, Assistant Commissioner for the RCMP, presented *Policing in the 21st Century* at the 2020 CASIS Vancouver West Coast Security Conference. The presentation was followed by a group panel for a question and answer period. Main discussion topics included technology and policing, big data, and the challenges that social media poses for law enforcement.

NATURE OF DISCUSSION

Presentation

Assistant Commissioner McDonald focused on the challenges associated with technological advancements, but also the new investigative avenues for law enforcement to consider because of the prevalence of online activity.

Question and Answer Period

During the question and answer period, the impact of COVID-19 in policing was discussed, as well an increase in cybercrime.

BACKGROUND

Presentation

The RCMP is Canada’s federal police force, therefore their responses, strategies, and tactics to combat crime are of importance to all Canadians. Today, especially in the era of COVID-19 criminals have shown their ability to adapt; crime is not stagnant, but likely more dynamic as it can be committed in a variety of ways. Complete privacy is difficult to retain because it is likely that everyone is online in some capacity.

Assistant Commissioner McDonald mentions the current challenges that police face in regard to the changing environment of technology. The challenges range from wearing body cameras to accessing the dark web. For example, decryption can be challenging for law enforcement because encryption of data is much more prevalent. Several individuals have the ability to encrypt messages, data, etc. Encryption can be easily learned, is free, and may be impossible to decrypt. In addition, when trying to decrypt data, it is important that public trust is not breached and privacy policies are followed, especially within law enforcement. Conversely, countries may be reluctant to share their own country's data because of privacy concerns regarding their country and citizens. However, there are policies in place that concern the collection of data, how data can be used, and the retention period of data.

Public relations is of the utmost importance for law enforcement entities as they serve communities and look to keep citizens safe. All police investigations are expected to follow the policies and evidence laid out because at the end of the investigation all of the evidence and discovery must be proven in court on a legal basis. Therefore, there must be a balance between decryption and the privacy of citizens.

The online environment brings challenges, but also new avenues and platforms to collect evidence for law enforcement. The range of online platforms and use of social media has had a significant impact in the collection of open-source intelligence (OSINT). Additionally, technological advancements such as facial recognition technologies are likely to become significant sources to consider in police investigations. Yet, facial recognition and its algorithms must be studied further to ensure biases do not exist because that is a concern among online algorithms used for identification purposes. Artificial intelligence (AI) technology is important to understand for beneficial purposes, but also to combat against when used by criminals. Thus, from a law enforcement perspective, the wide range of availability in tools is beneficial, however, they are just tools. The significance is derived from the use of the tools and accountability when utilizing the tools.

Question Period

The COVID-19 pandemic has impacted policing operations, and law enforcement, similar to other parts of society, has had to adapt. Data has illustrated a possible increase in intimate violence, which may be due to people spending more time at home with their families and partners than prior to the pandemic. Additionally, an increase in cyber crime has also been measured as criminals adapt and use different avenues to commit crime.

KEY POINTS OF DISCUSSION

Presentation

- Complete privacy may no longer exist with the prevalence of online activity.
- Data encryption is a challenge for law enforcement because it is becoming more commonly used.
- Law enforcement must follow policies in order to decrypt data to ensure privacy laws are not breached.
- Social media and online platforms have made investigations more complex, but also offer OSINT for investigations.

Question Period

- The COVID-19 pandemic has brought many challenges for law enforcement, and they have had to adapt just as other parts of society have done so.

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

Available from: https://jicw.org/