THE CHALLENGES OF DATA ACQUISITION AND THE USE OF ARTIFICIAL INTELLIGENCE/MACHINE LEARNING

Date: November 24, 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 24, 2020, Paul Jenkins presented *The Challenges of Data Acquisition and the Use of Artificial Intelligence/Machine Learning* at the 2020 CASIS West Coast Security Conference. The presentation was followed by a question & answer session. Main discussion topics included the importance of data when tackling organized crime; the challenges that the exponential growth of data presents; and the importance of having ethical and regulatory frameworks when dealing with data.

NATURE OF DISCUSSION

Presentation

Mr. Jenkins discussed the benefits and challenges of criminals' technological dependency; the acquisition and exploitation of data; and the importance of data sharing for better decision making.

Question Period

During the question and answer session, the speaker discussed different topics such as general concerns when dealing with organized crime, unethical retention of data, information security when sharing intelligence with other countries, and unregulated cyberspace.

BACKGROUND

Presentation

In the UK, crimes such as sexual exploitation, human trafficking/slavery, cybercrime, money laundering, and fraud take operational priority that requires all systems response and sometimes extension to international partners. The

Threat and Risk Assessment, Capability Exploration and Research team, which is led by the National Crime Agency, examines technological developments used in organized crime. They research and develop propositions to exploit opportunities and mitigate threats. They also maintain an up-to-date threat assessment that may inform investment decisions to develop capabilities that would help tackle serious organized crime.

Data underpins all investigations as almost all crimes are either technologically enabled or technology-dependent. However, as criminals are adapting, crime is increasing and becoming more complex. Globalization and evolving communication have facilitated criminals to exploit victims around the world and to move commodities while easily avoiding detection and persecution. The amount of data associated with crime is vast. Although there are challenges in obtaining and extracting value from it, criminals' dependency on technology also provides the opportunity to understand, detect, and disrupt criminal activities. Police responses to the volume and nature of digital information have changed but making informed decisions to reduce crime and identify victims and offenders has remained a priority.

Technical and human abilities are crucial to derive, transform, and combine the insight acquired from data to a more concrete way of identifying trends, gaps, actors, and opportunities to support decision making. The exploitation of data can be considered as the ability to connect to stored data, combine different datasets, and provide visualized information and reports to inform actions and decisions. However, it is not just about the acquisition and exploitation of data, but about being able to share the information with investigators and operational and policy decision-makers and partners so that they can act on the intelligence. It is important to note that more data is not necessarily better; the more data organizations have, the more challenging it becomes to store, exploit, and manage it. In the next few years, this will become even more complex; however, the interconnected data generated by devices will also offer immense opportunities to develop more effective and efficient data capabilities.

Due to the exponential increase of data, computing power will soon require a public cloud infrastructure for all data processing and analytics tasks. This, however, does not mean that artificial intelligence will replace humans, but rather that it will be used to augment human decision-making. The fragmented nature of data sources and lack of clear identifiers results in the need for data science techniques to associate it to trends and common patterns. Analysts need to draw conclusions not only based on the data but also the accuracy and origin of the

source. Furthermore, the demand for high-level data analysis will require whole organizations to be data literate, not only data scientists.

Investment resources for business decisions need to take into account the requirements of data management to meet legal, ethical, regulatory, and organizational standards to protect them against biases and discrimination in human decision making. The development of ethical and regulatory frameworks, decision intelligence, and transparent algorithm design will help mitigate the risks of biases. Decision-makers need to know how much they can rely on analytical insights derived from augmented processes and understand their limitations. New models of security and developments in data governance need to allow more flexibility in collaboration and sharing.

Question Period

- General concerns that have emerged in terms of organized crime throughout the years were discussed:
  - Technology has changed, and opportunities to penetrate or intercept criminal organizations have increased. Right now, the focus on threat actors and groups is on a global scale. However, the speed at which criminals can work presents a significant challenge for law enforcement. There are also challenges regarding jurisdiction and coordination with multiple agencies around the world. For example, criminals could potentially retreat to a country with weak law enforcement personnel.
- The complexity between various forms of collaboration when bound by treaties was discussed:
  - All of the Five Eyes countries invest in networks and officers around the world to overcome these issues. Human relations are a crucial factor in the sharing mechanism. It is also important to trust the appropriate actor without disclosing to an adversary; those relations are formed over a long period.
- Public engagement and how agencies have managed the pandemic was discussed:
  - Like the rest of the world, law enforcement has relied on technological platforms. There are more secure ways, but those secure ways can be limiting in accessing everyone. A halt on in-person meetings makes making new relationships very challenging. Video conferencing is more comfortable than before, but the value of real in-person engagement is still lost. Other benefits include reducing the carbon footprint of law enforcement.

- The disposal systems with particular interest of the unethical retention of data were discussed:
  - In the UK, some are linked to the Criminal Justice System. Some things are flagged for review and are disposed of after a certain amount of time.
  - Although law enforcement tries to be as compliant as they can, there are challenges with unconnected datasets, which were created for a specific purpose. Other challenges such as data protection rules developed years ago no longer apply to the present. The real risk arises when data is used and law enforcement believes it is holding it legitimately without knowing that the data led to intelligence that may cause issues such as worsening the public's perception of government data handling. When failure occurs, it is highly likely that it is unintentional.
- Military work with other organizations in managing information security was discussed:
  - In the UK, law enforcement deals with serious organized crime, but they also work closely with the militaries of other countries. For example, the navy can be deployed in the Caribbean for disaster relief but depending on intelligence, they may also perform a narcotics operation. These organizations have to be confident that they can handle the intelligence provided. Military outlets may use law enforcement officials and military personnel together, but they would play different roles while working hand in hand tactically. For example, in Africa, they may assist in facilitating migration, but they may also become military targets.
- Future technological/cyber restrictions as a result of ungoverned cyber black markets were discussed:
  - There are no regulations in place for the governance of places like the dark web, and law enforcement has not seriously considered putting regulations in place. It's already unlawful. Regulations would result in disruptive technological capabilities that would push criminals further into obscurity. Also, not all the communication within the dark web is related to crime, so law enforcement is just trying to mitigate the criminal activity.

KEY POINTS OF DISCUSSION

Presentation

- Almost all crimes are either technologically-enabled or technology-dependent, and it is this technological dependency that allows law enforcement to understand, detect, and disrupt criminal activities.

- Artificial intelligence will not replace humans but rather augment human decision-making; both technical and human abilities are crucial when dealing with and acting on data.
- The development of ethical and regulatory frameworks for data management can help mitigate risks of bias and discrimination in human decision making.

Question Period

- Technological advancements have provided numerous opportunities for law enforcement to intercept criminal organizations; however, there are also challenges such as jurisdiction and the speed at which criminals work.
- All of the Five Eyes countries invest in networks and officers around the world to build trust and overcome issues of collaboration when bound by treaties.
- Attempting to put regulations in place for ungoverned places such as the dark web would only result in disruptive technological capabilities that would push criminals further into obscurity.

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

Available from: https://jicw.org/