DATA ANALYTICS AND SECURITY POLICY: THE NEW PARADIGM?

Date: January 16, 2020

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

KEY EVENTS

On January 16th, 2020, the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its first roundtable event of the year, titled "Data Analytics and Security Policy: The New Paradigm?" This presentation featured Mr. Mark Masongsong, CEO of Urban Logiq, a Vancouver based data analytics company. Mr. Masongsong's presentation focused on the development of data analytics technology, its utility in addressing recent security cases, and the projected future of the data analytics industry. The subsequent roundtable discussion centred around a case study on deep fakes and their prevalence throughout social media. Thereafter, audience members discussed the security implications of deep fake technology and ways to address the problem within online spaces.

NATURE OF DISCUSSION

Presentation

The emergence of data analytics technology is resulting in new tools, policies, and opportunities for security practitioners. The 21st century has brought a revolution in the way humans communicate and broadcast information. The rapid spread of information requires security professionals to be vigilant when analyzing data. Moreover, the sheer amount of data created has changed the way we must look at security. Consequently, Mr. Masongsong states, it has also created a need for adaptive policies that reflect the 21st-century security climate.

Roundtable

The roundtable discussion focused on areas of security in which data analytics are being employed, such as criminal investigations, intelligence analysis, and human security. Moreover, current debates highlighted the establishment of policies for these technologies emerging in such fields listed above. With the increasing use of data analytics in intelligence and law enforcement, questions surrounding their ethical use may be asked.

BACKGROUND

Presentation

Data analytics technology, like other computer-based technologies, has been growing at an exponential rate since its inception. As this growth follows Moore's Law, the number of transistors that fit on a microchip doubles every two years, thereby decreasing the price and increasing the speed and performance of computer technology accordingly. Although it is impossible to say for certain how this trend will continue in the future, we can be confident that data analytics technology will become more powerful and accurate in assisting with jobs.

At present, more data is created every year than in the past 5000 years of humanity; providing security practitioners with a powerful tool to conduct their work is arguably ever more crucial. Today's algorithms can understand humans and our behaviour better than we understand ourselves. Data analytics functions as a predictive tool where data is analyzed and predictions are made against every possible outcome; the correct predictions are weighted more heavily in future analysis and accuracy is improved. Therefore, the more data is collected and analyzed, the more powerful becomes the predictive ability.

The range of uses for data analytics technology is expanding and many operations are quite simple. Examples expressed in the presentation included the following: how Netflix uses big data to drive success; how Target diagnosed a teen girl's pregnancy before her father, simply based on purchasing patterns; how data analytics can predict future unemployment rates, food safety violations, or when and where disease outbreaks will occur. Data analytics have been used to help girls in Africa stay in school, predict shortages in income following poor harvests, and to assist the CIA in predicting social unrest several days before it begins.

Grey areas emerge when examining this type of technology, which will require new policy decisions moving forward. One example was how data analytics can be used to address human trafficking, but the same approach may potentially violate personal privacy as a civilian's behaviour and private life are examined. Additionally, large tech companies like Google use many algorithms and their obligations to reveal information or refrain from collecting data are uncertain. As Mr. Masongsong states, algorithms are not flawless, and it is important to be mindful of biases that may develop from the input data, potentially leading to inaccurate conclusions.

Roundtable

- Government agencies can collect large amounts of online data. Some agencies are collecting this data en masse and storing it so that in the future they will have the computing power and algorithms to translate the data on people from 10 years ago.
- Governments are not always securing their data. Agencies have left some of their most powerful data unencrypted in their database, thereby allowing opportunity for hackers to attack them.
- One potential use of data analytics is in court sentencing, but it is not clear how biases in the system can be prevented to avoid unjust sentencing of individuals, despite the accuracy of the algorithm.
- The issue of human nature and error remains. An oversight by an individual is always possible and that is all it takes for errors and vulnerabilities to occur.

Case Study Presentation

The case study discussion focused on the increasing use of deepfakes— online entities who are not really in the outside world— to manipulate audio, video, and images, as well as the security implications produced by this technology. The technology to create deepfakes continues to improve to the extent where real or fake profiles are becoming increasingly difficult to differentiate, moving beyond what can be discerned by the casual observer.

Case Study Roundtable

The following perspectives were put forth on addressing the use of deepfakes:

- Officials can choose to hold individuals responsible for the creation of deepfakes, rather than addressing the technology alone as individuals will continue to find new methods.
- Governments can take responsibility in discerning whether or not a document is a deepfake.
- Companies who are complicit in the creation of deepfakes can be held liable.
- The international community can be engaged to address deepfake technology, attaching economic penalties for creation and incentives for reporting.
- Pamphlets and other educational materials can be created to inform the population about deepfakes.
- Deepfakes can be treated in the same way as other cyber warfare/hacking software.

The case study highlighted how the governments of Estonia and Sweden are taking measures to address deepfake technology, and how this technology is a national issue with no single solution. Society usually adjusts to new technology and then legislation follows. Arguably, the priority should be education, as many individuals do not know what deepfakes are.

How do we effectively put in place government regulations?

Placing government regulations on this technology is not a simple procedure. There is a fundamental debate that arises between freedom of speech and expression on one hand and the censoring of information for public safety on the other.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Presentation

- Data analytics technology is developing rapidly with new applications continuously emerging for use in security fields.
- The projected benefits to law enforcement and intelligence analysis operations are numerous.
- Massive amounts of data are being created, collected and stored for use in the future as new technologies develop.
- Some aspects of data analytics technology have the potential to violate individual privacy rights.

Roundtable

- As deepfake technology increases in quality and ease of use, there may be an increase in their use to discredit and mislead individuals within the online sphere.
- Deepfakes may be increasingly seen in political spheres to influence elections, create misinformation and divide communities.
- Countermeasures exist to filter content, but the responsibility to implement and monitor them will have to be taken up by governments or businesses.

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

Available from: https://jicw.org/