**REVISTING DISRUPTIVE TECHNOLOGY AND THE INNOVATOR'S DILEMMA IN THE AGE OF CYBERSECURITY**

**Date:** November 23, 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 23, 2020, Dr. Michael A. Hennessy presented on the topic of *Revisiting Disruptive Technology and the Innovator's Dilemma in the Age of Cybersecurity* at the 2020 CASIS West Coast Security Conference. The presentation was followed by a moderated question and answer period. Key points of discussion included: the difficulties of embracing major technological change in modern military bureaucracies; how organisational culture is an impediment to change; and how leadership and management in military organisations is out of step with the pace of change.

## NATURE OF DISCUSSION

### Presentation

Dr. Michael A. Hennessy discussed his experiences of trying to educate those in military bureaucracies about cybersecurity issues in an effort to implement change.

### Question Period

During the question period, the discussion focused primarily on the factors that prevent bureaucratic agencies from increasing the effectiveness of their data to establish defensive strategies.

## BACKGROUND

### Presentation

Historically, organisations such as Netflix and Uber have been successful in destabilising their respective industries through introducing revolutionary technology, or *disruptive technology*. By focusing their efforts on developing

innovative technologies in the cybersecurity industry, the Canadian Air Force and other military organisations have the potential to "transform the fight" against their opposition. Unfortunately, serious organisational, institutional, and cross-institutional barriers need to be overcome before such changes can be implemented in military bureaucracies.

One of the first barriers to educating and implementing change in a large military bureaucracy is on the individual level. Some people may have competing agendas, or there may be a struggle for resources among departments that can interfere in the acceptance of new ideas and innovations. The egos of organisation leaders may impede technological advancement or they may discourage free-thinking and risk-taking among members.

Although many military-technical bureaucracies may employ small "think-tanks" or cells in charge of innovative technologies, many continue to face barriers to advancement at the organisational level. Organisational culture may create an atmosphere where innovation is neither encouraged nor accepted. Moreover, military procedures and practices are behind the times and face challenges from archaic financial control systems to greater challenges such as the division of roles and responsibilities among government departments.

The lack of cooperation across departments and institutions often creates obstacles to developing innovative programs, despite their clear advantages to the organisation. For example, it would make sense that cybersecurity in Canada would be the responsibility of the Department for National Defence; however, this is not the case. Cybersecurity falls under the jurisdiction of the solicitor general who may face structural or legal impediments to sharing or receiving information from other departments that may possess more expertise in that domain.

As can be seen by Britain's recent initiative, the National Cyber Force (NCF), integrating departments to facilitate sharing of information related to cybersecurity is possible; however, it took upwards of 8 years for this initiative to come to fruition. In the age of light-speed change, taking years to reshape our organisations is problematic. Armed forces that do not stay on the cusp of modern technology are doomed to be outclassed in a modern fight.

**Question Period**

Within the context of bureaucratic military agencies using data to establish defensive strategies, an emphasis was placed on discerning the entity that is seeking information and the source of the data that is being sought.

The government in a parliamentary democracy receives data from various sources which makes it difficult to determine the best way to improve effectiveness of the data. Moreover, each agency or individual within that agency, has varying motives and different opinions on how best to use that data.

## KEY POINTS OF DISCUSSION

### Presentation

- The use of *disruptive technologies* can be advantageous in destabilising the industry especially in the domain of cybersecurity; however, it requires adaptability and a willingness to innovate.
- In order to become a leading organisation in the cybersecurity field, cooperation among departments and institutions is required in order to facilitate the sharing of information and resources.
- Modern military bureaucracies are resistant to change and face barriers at the individual, institutional, and organisational level.
- The organisational, institutional, and attitudinal barriers can be overcome only through constant attention and adaptability to change.

### Question Period

- Within a parliamentary democracy, it is difficult for government agencies and military bureaucracies to improve the effectiveness of their use of data for developing defensive strategies due to the structure of the organisations and the multitude of data sources.
- Such organisations have multiple departments and individuals who have differing opinions on what is important and what information is required.
- Data is obtained from a variety of sources, which creates information confusion and makes it difficult to discern which data may be most useful or effective for a given task.



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