



LEADERSHIP, TECHNOLOGY AND NATIONAL SECURITY

November 26, 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 26, 2021, Mr. Phil Gratton, former DG in the Directorate of Technology for the Canadian Security Intelligence Service (CSIS) and current Associate Faculty at the Canada School of Public Service, presented on *Leadership, Technology and National Security* 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 point discussed was how leadership must adapt to best support its mission and technology workforce in the face of ever-evolving technological advancements in the realm of national security.

NATURE OF DISCUSSION

Presentation

Mr. Gratton's presentation highlighted how leadership must adapt to changing challenges in the modern workplace. Additionally, he discussed emerging technological advancements and how contemporary leaders should transform their management skills in respect to the digital world, which yields threats that come from a different standpoint compared to decades ago.

Question Period/Breakout Room Discussion

The question-and-answer period highlighted topics on leadership attitudes and what qualities and skill sets individuals should be focusing on in order to lead others.

BACKGROUND

Presentation

Mr. Gratton began his presentation by noting that nowadays many managers are finding themselves trying to keep up with the fast-changing digital landscape. Mr. Gratton noted that even for someone who is comfortable with technology, they might not be well-equipped to meet the needs of a highly technical workforce. In addition, he explained how the intelligence community and CSIS is still coming to terms with the notion that understanding and leveraging technology has become increasingly significant. As society has become more digital, so are the threat vectors. Thus, methodologies have been adapted to investigate these threats. Not long ago, some technologies were in the exclusive domain of government; however, now, individuals and groups (including spies and terrorists) are making use of commercially available technologies that are as good as those developed by government. The intelligence community is now concerned about what the private sector might be producing that would end up in the hands of adversaries. According to Mr. Gratton, the pervasiveness of technology offers new opportunities, but also new challenges related to the workforce, which need to be addressed.

Mr. Gratton also discussed the importance of current technologists and the significance of upskilling employees and managers to understand complex forms of technology to face the new threats. Making space for technologists, ensuring they are supported, integrated, and appropriately compensated has been particularly challenging for CSIS and its leadership. However, Mr. Gratton advised that this is changing as he noted that this is a challenge that CSIS is ready to meet.

Mr. Gratton stated that leadership is an attitude and a set of behaviours expected not only from managers but also from employees. Managers and employees must integrate into the realm of the technological world to combat new digital threats. For non-technical managers it can be difficult to lead technologists; however, investing in technologists, who are at the forefront of new technological innovations, can help the transition into the technological world. Mr. Gratton explained that it is important for managers to be in tune with technology and understand the way it operates as it has its unique requirements. If this is not prioritized, these managers may not be in the position to lead.

Leadership in technology is a human role and requires creativity and passion. Technology is not only pervasive but also ever increasing in complexity,

diversity, and novelty, making it difficult for many managers to grasp. To ensure that leaders can deal with the complexity of new digital threats, they must be able to trust in the technology workforce, who can be highly specialized in their respective fields and understand the technical and legal frameworks they need to work within. Trusting technologists means creating a space for them to experiment and learn from collective failures. Mr. Gratton noted that acquiring leadership qualities is often more challenging than acquiring technical skills. Non-technical managers need to cultivate their humility, which is often difficult, and understand that it is acceptable not to understand the technological aspects of something as long as they are willing to learn. Mr. Gratton also noted that all managers must have a basic understanding of the technology that underpins our connected world and its relation to the business they are responsible for. They also need to appreciate that technical specialists understand their roles and the consequences of their mistakes.

All employees must contend with emerging technologies and expand their digital awareness, literacy, and hands-on experience. Considering the increasing development of digital threats, taking these precautions are crucial to ensure preparedness for future situations.

Innovation is not a destination but rather a constant state of being. Although change can be uncomfortable, we cannot afford complacency when dealing with threats to national security. Embracing this change starts with clear and consistent communication from leaders to demonstrate how all employees will be confronted by emerging technologies and how they can have a positive impact to meet the mission and the mandate of the organization. Although taking on the new emerging digital age comes with growing pains, it is something that needs to be implemented to best serve Canadians in this increasingly technical and digital world.

Question Period

During the question-and-answer period Mr. Gratton noted that leadership is a skill that can be developed amongst all individuals and not a characteristic that is genetically coded. Although some people naturally acquire leadership skills, others leverage their personal experience to develop their skills and transform them into the leaders they are.

Regarding whether technology is disrupting the way that leaders are developing today, Mr. Gratton stated that there is a challenge to organizations such as CSIS to be able to adapt to the interchanging and multiple layers that technology

presents. During a time where individuals are given devices to work from home, which is a security risk as they can be compromised, individuals must have extensive awareness of their work environment. Since working from home has become a routine, it now behooves the leadership of these different organizations such as CSIS to be able to lead their employees and give them guidance.

In addition, Mr. Gratton emphasized that leaders are also human and are expected to make mistakes and have weaknesses. As he reflected on his own experience, he indicated that it is ultimately up to the individual, as a leader of an organization, to continue modeling leadership behaviors in an effort to help others and guide them effectively.

Breakout Room Discussion

During the breakout room discussion CASIS Executives and audience members asked questions regarding leadership skillsets, effective leadership, and how leaders can address some challenges that the current workforce might be facing. Mr. Gratton mentioned that those who have not been associated with technology often struggle to adapt to the new reality. With this in mind, he further argued that bringing a new technological workforce to work along those who are not comfortable with technology helps them transform and keeps them relevant in the organization.

Mr. Gratton also noted that there are many different leadership styles, which have been successful for a range of individuals. When thinking about behaviours a leader should avoid when leading people, following the organization's code of conduct is a must. Additionally, most leaders have established lines they will not cross, but it would also depend on the individual's style. However, a good leader is someone who is able to lead people to great things and allow them to flourish.

KEY POINTS OF DISCUSSION

Presentation

- As society has become more digital, so have the threats. This means we must adapt and introduce new methodologies to investigate these threats.
- Nowadays, individuals and groups (including spies and terrorists) are making use of commercially available technologies that are as good as those developed by government.
- The workforce must upskill or develop new technical skills to overcome the new digital threat challenges.

- To ensure that leaders can deal with the complexity of new digital threats, they must be able to trust in the technology workforce by creating a space for them to experiment and learn from collective failures.
- Leadership is an attitude and a set of behaviors that is expected from managers and employees.

Question Period

- Although many people naturally become good leaders, leadership is a skill that can be developed amongst all individuals.
- The objective of leadership is to be able to elevate and guide people and let them flourish.

Breakout Room Discussion

- Pairing new technological workforce with those who might not be comfortable working with technology can help them adapt and transform and keep them relevant in the organization.
- A good leader is someone who moves people to great things, elevates them, and allows them to flourish as employees.



This work is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International License.

© (PHIL GRATTON, 2022)

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

Available from: <https://jicw.org/>