COUNTERINTELLIGENCE AND THE CHANGING THREAT LANDSCAPE

Date: March 16, 2023

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 March 16, 2023, Daniel Stanton—Director, National Security Program, University of Ottawa, Professional Development Institute—presented *Counterintelligence and the Changing Threat Landscape*. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were the definitions and outcomes of offensive and defensive counterintelligence (CI), the principle states engaged in CI, and the shift in CI tactics and operations in recent years.

NATURE OF DISCUSSION

Mr. Stanton outlined purpose and outcomes of CI operations—both historically and at present—while also providing a review of key players in CI globally. He discussed the ways in which CI operations shifted in the post-Cold War environment and have evolved in a liberal society and accelerated technology environment.

BACKGROUND

Presentation

Mr. Stanton began by outlining the differences between defensive and offensive CI, stating that the former consists of activities to thwart or prevent espionage and the latter represents active campaigns aimed at acquiring intelligence. Defensive CI operations can involve physical and workplace security; IT protocols and restrictions; internal investigations; and legislation, and offensive CI operations can consist of forms of espionage, such as state or industrial; the targeting and monitoring of dissidents; and foreign interference or influence campaigns. Mr. Stanton stated that the targeting and monitoring of dissidents and the diaspora communities represents a significant aspect of Chinese, Russian, and

Iranian offensive CI at present. Regarding espionage, Mr. Stanton declared that it is a difficult and high-risk action, generally involving illegal means, yet remains a priority within CI. He noted that cyber-espionage has largely replaced human-espionage in modern CI.

Mr. Stanton discussed the key players in CI internationally, highlighting the Russian Federation, People's Republic of China (PRC), and Iran as states of principal interest to Canada. Within the Russian Federation, he pointed to the SVR (previously KGB first directorate); GRU (military intelligence); and FSB (previously KGB second directorate) as significant actors in CI, noting that the latter is favoured by President Vladimir Putin as it is his former post. Mr. Stanton marked a shift in Russian CI following the collapse of the Soviet Union, stating that there was less state-versus-state espionage and an increase in "seeding" operations, in which foreign actors insert themselves into the targeted society and gain and maintain relationships to be exploited in the future. He highlighted the case of Richard and Cindy Murphy (aka Lidiya Guryeva of SVR) from the FBI's Ghost Stories investigation as a significant example.

In the PRC CI operations, Mr. Stanton noted the Ministry of State Security (MSS); Second Department, People's Liberation Army (2PLA); and United Front Work Department (UFWD) as the principal actors. Mr. Stanton pointed to the aggressive, but sometimes ineffective, nature of CI operations run by PRC. He suggested that the significant Human Intelligence (HUMINT) failures on behalf of the PRC can be attributed to the speed in which the state attempts to bring individuals into the field of operation, often neglecting proper training and operational security. Mr. Stanton stated that, despite these failures, the PRC maintains a technological advantage over the West which is leading to the loss of Western dominance in the CI theatre. He stated that technological advancements such as artificial intelligence (AI) are increasingly important in CI prominence, and there is a push on behalf of all states to gain the advantage in these new technological areas.

Regarding foreign interference in Canada by the PRC, Mr. Stanton discussed the role of the UFWD in gathering intelligence and managing relations and influence among elite individuals and organizations inside and outside China. He stated that these measures are centred on the cultivation of relationships, influence, and desirable outcomes as opposed to the acquisition of state secrets. Mr. Stanton pointed to the 2017 National Intelligence Law of the People's Republic of China—which tasks Chinese organizations and citizens globally in the preservation of state security—and Operation Fox Hunt—targeting identification

and repatriation of Chinese nationals alleged to be corrupt—as examples of new and significant forms of CI employed by the PRC.

Mr. Stanton discussed Iranian CI, highlighting the prevalence of offensive CI by the state. He asserted that Iran is highly aggressive in its targeting of dissidents, often carrying out large purges on behalf of the regime. Mr. Stanton noted a unique aspect of Iranian CI in the monitoring of dissidents: the tendency to contract surveillance to the private sector. He stated that this is often a poor strategy, as private investigators lack ideological or national loyalty to the state and often contact law enforcement when the purpose of their surveillance comes into question. Mr. Stanton asserted that, although this tactic lacks sophistication, it is indicative of a highly aggressive offensive CI operation and an evolving threat landscape.

Mr. Stanton concluded with the assertion that the offensive CI threat from main state actors has shifted from easily identifiable Cold War-era operations to a more difficult to discern landscape, made possible by an open, liberal, and globalized society. He argued that this new threat landscape in CI is potentially more damaging to society at large than more traditional and state-centred CI, in that it sows doubt across and surrounding established institutions.

Question and Answer

Mr. Stanton contended that focus and policy are crucial in mitigating the effects of foreign interference on the general public. He stated that in the current threat landscape, there is a tendency of some actors to exacerbate public fears regarding a wide array of topics—such as AI, climate change, and economic insecurity—and the principal task of the Canadian government should be to pursue a strong national security policy while not overloading the discussion. Mr. Stanton suggested that the threat environment is often overstated by the media and perpetuated through ease of access to information, and that security and intelligence should seek to prioritize disseminating credible information in key areas. He noted, however, that the fomenting of distrust in the general public caused by an exaggerated threat environment is the goal of malign foreign CI operations, and Canadian CI must address this.

Mr. Stanton addressed the recent collision between a Russian aircraft and US drone, stating that it is ambiguous as to whether this can be referred to as foreign interference and that the US is primarily seeking to de-conflict the situation as opposed to escalate. In terms of the Canadian perspective, Mr. Stanton stated that Canada’s position is to maintain its course of support for Ukraine. He noted the

significance of drones in the new CI landscape, however, remarking that they harken back to past counter-procurement efforts.

Mr. Stanton discussed economic espionage and the potential for its growth in coming years, noting that it is an area of great contention. There are concerns regarding state intention when monitoring and collecting economic information and, if it is to occur, it must be made abundantly clear that states are not advantaging one player above another in competition.

Mr. Stanton suggested that, in part, recent CI failures by the PRC can be attributed to changes within the regime. The elevation of the Politburo as well as changes to tradecraft have pushed intelligence services outside of areas of comfort, leading to accelerated operations that recruit from new communities. These changes have resulted in many arrests and increased pressure within the PRC, leading to increased efforts in industrial espionage.

Discussing the failure of FSB in Ukraine, Mr. Stanton asserted that it is well-known that Putin favours the organization and, in order to maintain this position, he is often provided with information that is in line with his views as opposed to factual and effective. Mr. Stanton noted that there was historical precedent for this in Russia, dating back to the Soviet Union and similar behaviour during the Stalin regime. Mr. Stanton offered that Ukraine also utilized effective disinformation campaigns that amplified false narratives to their advantage.

Mr. Stanton noted that there is a tendency to quickly label interference that harms social cohesion in Canada the result of foreign actors, but that there is a significant domestic threat as well. The federal government has recognized mis- and dis-information as a serious threat to social cohesion in Canada, but Mr. Stanton suggested that there is a need to expand the definition of foreign interference. Citing the example of the Freedom Convoy, he pointed to the CSIS report in which there was no findings of foreign interference, though cautioned that the organization only monitors state driven interference, as per its mandate under section two. Mr. Stanton suggested that this definition must be expanded to capture the efforts of private individuals with significant resources and malign intent, as this can have massive impact in a globalized environment.

KEY POINTS OF DISCUSSION

Presentation

- Defensive CI is the thwarting or preventing of espionage and offensive CI is the active pursuit of intelligence. Defensive CI operations can involve physical and workplace security; IT protocols and restrictions;

internal investigations; and legislation, and offensive CI operations can consist of forms of espionage, such as state or industrial; the targeting and monitoring of dissidents; and foreign interference or influence campaigns.

- The Russian Federation, People's Republic of China (PRC), and Iran are the states of principal interest to Canada in CI. Targeting and monitoring dissidents and diaspora communities represents a significant aspect of these states' CI and that cyber-espionage has largely replaced human-espionage in modern CI.
- There has been a paradigm shift in Russian CI following the collapse of the Soviet Union, stating that there was less state-versus-state espionage and an increase in "seeding" operations. PRC and Iranian offensive CI has been characterized by aggressive and accelerated actions as of late, yielding poor results for the states, but indicating an evolving threat landscape in CI.
- The offensive CI threat from main state actors has shifted from easily identifiable Cold War-era operations to a more difficult to discern landscape, made possible by a liberal society that provides more open and globalized access to a variety of actors. This new threat landscape in CI is potentially more damaging to society at large than traditional and state-centred CI, in that it sows doubt across and surrounding established institutions.

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