APPLIED (ACTIVE MEASURES) COUNTERINTELLIGENCE

Date: November 24th, 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 24th, 2020, John Ardis presented *Applied (Active Measures) Counterintelligence* at the 2020 CASIS West Coast Security Conference. The presentation was followed by a question and answer period.

NATURE OF DISCUSSION

Presentation

Dr. John Ardis' presentation focused on the reasons why active measures counterintelligence (ACI) should be developed, the operational requirements for ACI, and the overall benefits of ACI.

Question and Answer Period

The question and answer period focused on how new technology developments affect counterintelligence operations and the approach taken by modern counterintelligence. A second question and answer period took place in a breakout room, which focused on the differences between ACI in the public and private sector, the issues with manipulation, the human aspect of intelligence, and issues with counterintelligence in corporations.

BACKGROUND

Presentation

ACI can be used to exploit the increase in connectivity and demand for rapid data by selectively manipulating the information that is gathered by opposing intelligence agencies or terrorist groups. The operating environment of modern warfare is increasingly complex and filled with deception, bias, competitive narratives, and ambiguity, and basic military deception is not sufficient for such

a complex environment. It is essential to exploit the complexity and uncertainty in this operating space to gain an information advantage over our opponents. It's often cheaper, easier, and quicker to degrade an adversary's capabilities than it is to improve one's own capabilities, making ACI a valuable strategy in this domain.

There are certain requirements that are necessary to develop or enhance current ACI strategies. Innovation is key and is usually achieved by developing a variety of operational concepts, along with a concentrated analysis so that we can understand which operations to consider, how to adapt them, and when we should deploy certain operations. Synchronization with other operations and the activities of our partners is important in the development of ACI, as well as consolidation across channels and across time. This allows for the development of a series of operations that reinforce the exploitation of the operating environment, which can provide options and latitude for commanders down-stream.

Resilience is another requirement for the development of ACI. Single outcome strategies are not ideal in complex or uncertain environments because they only account for one way of succeeding. The focus of ACI is to design activities and operations that have several methods of succeeding, while minimizing potential failures. One such method is the implementation of several decoy operations or "sacrificial shells", designed to be uncovered by adversaries while protecting primary operations.

The final requirements of ACI are effective auditing and record keeping, as well as ethical practice. Maintaining a proper and comprehensive record of events, actions, and outcomes helps to design and adjust future operations. Operations must also satisfy legal and ethical criteria to ensure there are no unacceptable third-party risks and to ensure reputation is not jeopardized.

There are a number of benefits of implementing ACI alongside typical military defense counterintelligence operations. ACI increases agility by offering multiple options, which provides practitioners more choice and makes them less predictable to adversaries. Enhancing ACI operations also assists in the development of long-term strategies that contain and suppress risks, which reduces the need to deploy reactive short term defensive measures. Moreover, ACI allows for the development of new capabilities without interrupting current operations and can be used to justify current or planned intelligence collection. ACI capabilities are also adaptable to different operating environments and may even help to identify chronic problems. Finally, ACI allows for comprehensive

record management which guards against knowledge evaporation from members who retire, move, or become promoted.

Question and Answer Period

New technological developments have changed counterintelligence efforts dramatically. With the large influx of data available, it is essential to balance the human and technical skills in a dynamic way. There is a limit to our capabilities in terms of quantum computing, artificial intelligence, and machine learning, making the human component necessary.

In terms of the counterintelligence approach taken in the cyber domain, there are multiple streams of investigation occurring simultaneously, some of which are defensive and some are offensive. The longer-term trend is towards protection and risk reduction; however, there are advantages to taking a more offensive approach. For example, it takes a lot of effort to improve one's own operational capabilities; however, it takes much less effort to degrade an opponents' operational functions.

There are significant differences between the public and private sectors when it comes to ACI. The private sector provides more lucrative opportunities than government agencies; however, the ethical boundaries are much different. Furthermore, certain methods should only be retained within government operations, because they cannot be used again once they are publicized.

With regard to our Five Eye partners, manipulation is not endorsed as it is detrimental to relationships; however, deception can be used in certain circumstances if it is carefully planned. For example, using undercover officers must be planned and approved before proceeding along with their would-be handlers and agents overseeing and aiding the operation.

In the future, the human aspect of intelligence will still be important in recognizing the cultural nuances with technology and addressing the generational gap. Intelligence will need to be tailored to help make decisions in difficult circumstances. Social media and open source intelligence remain problematic, so the human aspect is essential to weed out the useful information in the vast mess of data that is available online.

With regard to large corporations, information security is a critical concept. People are capable of misleading big technology companies by interrupting algorithms through looking at irrelevant information. Planting this misleading information dilutes the intelligence to the point the information is no longer viable.

KEY POINTS OF DISCUSSION

Presentation

- The operating environment of modern warfare is increasingly complex and filled with deception, bias, competitive narratives, and uncertainty, which requires a more nuanced approach than just basic military deception.
- Active measures counterintelligence (ACI) can contribute to information advantage by manipulating information gathered by opposing intelligence agencies or terrorist groups.
- There are several operational requirements for ACI including: innovation and variety, synchronization, consolidation, resilience, cost and risk economy, records, and ethics.
- The benefits of using ACI include increasing agility, assisting with the development of long-term strategies that contain risk, increasing overall capabilities without interrupting current operations, enabling options management, adaptability to different operating environments, guarding against knowledge evaporation, identifying chronic problems, justifying current and planned intelligence collection, and facilitating access to experts.

Question and Answer Period

- New technological developments have significantly changed counterintelligence efforts. Limitations remain with quantum computing, artificial intelligence, and machine learning, which makes it essential to retain the human component of counterintelligence alongside technological advances.
- Modern counterintelligence utilizes both offensive and defensive approaches with regard to espionage in the cyber domain.
- There are several differences between public and private counterintelligence agencies including the salary, ethical boundaries, and methods used.
- Manipulation is detrimental to relationships and often becomes a problem. Deception can be used so long as it is carefully planned and approved.
- The human aspect of counterintelligence remains important to recognize cultural nuances, address the generational gap, and pick out the relevant information in the vast amounts of data available online.

- Information security is a critical concern with large corporations. Seeding misleading information dilutes the intelligence to the point information is no longer critical.

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