ASYMMETRIC ATTACK: A QUANTUM OF WARNING

Date: November 23, 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 23, 2021, Alexander Butterfield presented on *Asymmetric Attack: A Quantum of Warning* at the 2021 CASIS West Coast Security Conference. Alexander Butterfield's presentation centered around developing a warning system for incoming threats, with key discussion points being the failures of operational warnings in large-scale terrorist events, the need to compensate for uncertainty, and hypersensitivity to weak signals. Mr. Butterfield's presentation was followed by a question and answer period directed at a group of panelists allowing the audience and CASIS Vancouver executives to directly engage with the content of each speaker's presentation.

NATURE OF DISCUSSION

Presentation

Warnings against asymmetric attacks need to be systemized, as this will compensate for uncertainty and will allow governmental bodies to accept more risk in future decision-making. The journey towards operational readiness will be tough but it is integral in developing a warning system against asymmetric attacks and removing dependency on chasing internet conspiracies.

Question Period

It is integral to balance rights and freedoms with national security needs. Unfortunately, there is a consistent conundrum regarding balance when it comes to security and openness, especially with evidence-based decision-making. With the development of modern day asymmetric threats, it may be useful to dust off some of the foreign intelligence skills, including counterintelligence, used in the past when it comes to identifying baseline activity for extremism and red flags.

BACKGROUND

Presentation

Mr. Butterfield began his presentation by highlighting that the problem of warning brought focus and clarified all dimensions of intelligence collection and analysis like no other problem did. Defence warning systems have been developed by several states. The US Department of Defense, for example, developed an Indications and Warning system (I&W) during the Cold War, which was used primarily for symmetric adversaries that were predictable and observable. With symmetric attacks, military power and strategy did not differ significantly between opponents, which has since changed with the elevation of warfare.

Mr. Butterfield noted that the regional and functional centres of the Central Intelligence Agency (CIA) have undoubtedly developed analytical tools for political and economic warning, which might better serve their hyper secret culture. The defence warning system has evolved over the years to include economic, diplomatic, and political components. Currently, states with growing power struggle to align their expectations of state interests with judgments of the tactical, operational, and strategic means utilized to achieve their goals; this has led to the pervasiveness of asymmetrical warfare. As such, there is a heightened need for adequate warnings against asymmetric attacks in response to this change.

As an illustration, 9/11 was not just a failure of strategic warning but a failure of operational warning, which forced the governmental bodies to abandon systemic warning systems and resort to taking wild guesses. However, every single adversary undergoes a process prior to execution in order to become ready for attack: planning, budget, training, logistics, mobility, etc. which leaves no room for speculations and theorizing.

As it currently stands, there are differences in signature between asymmetric and symmetric threats, with the former’s signature being more discreet, barely observable, and extremely uncertain. With this in mind, the precariousness of asymmetric adversaries desperately requires a systematized warning system in order to increase the state’s hypersensitivity to weak signals and acceptance of more risk in decision-making.

Although there is no comprehensive, whole-of-government effort to develop a warning system against asymmetric attacks, an unacceptable alternative would be to chase internet conspiracies, which simply create further problems of false claims, public cynicism, and the erosion of public trust in state institutions. The systematisation of asymmetric warning is not easy but a slow, patient process that allows better understanding of the complete signature profile of an asymmetric adversary.

Question Period

In democracy, there is always conflict between security and openness, and foreign actors are keen in using this to create internal division at their own advantage. Security systems are often expected to uncover individuals who may commit violence, but it is difficult to engage the public in these issues and simultaneously support practices of the security sector.

While the warning intelligence sphere is changing, using past foreign intelligence skills, such as counterintelligence, may still be beneficial when it comes to identifying baselines for violence, and governments can use this to portray their services to the country in a positive way. Ultimately, small improvements are big improvements when it affects lives, especially with concepts such as asymmetric attacks and operational warning systems.

KEY POINTS OF DISCUSSION

Presentation

- Signatures are the key observable difference between asymmetric and symmetric attacks. Asymmetric signature is discreet and uncertain, while symmetric signature is more predictable.
- For both symmetric and asymmetric attacks, adversaries undergo a process before execution which deals with planning, budget, training, logistics, and more.
- By systematizing warnings against asymmetric threats and adversaries, we will be able to offset deficiencies and better deal with the tactics of unconventional warfare by becoming hypersensitive to weak signals and adapting to precarity.
- It is hard to understand asymmetric profiles while they are at rest, so while the journey towards operational readiness may be tedious and long, it is integral in strengthening the state’s responsiveness to incoming attacks.

- The alternative to developing a warning system against asymmetric attacks would be to chase internet conspiracies, but it would increase skepticism and uncertainty.

Question Period

- It is easier to discuss failures in security, as successes are hard to discuss because of the nature of warnings which deal with prevention; it is difficult to discuss what went right without revealing sensitive information.
- The security sector needs to improve in engaging the public with national issues and why certain actions are being taken to respond to these problems.
- Relying on foreign intelligence skills and tactics can allow the government to better identify baselines for violent extremisms and define red flags.

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

Available from: https://jicw.org/