ANTICIPATORY APPROACHES TO DISINFORMATION: THE ROLE OF TRADECRAFT IN STRENGTHENING RESILIENCE

Date: November 21, 2024

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 21, 2024, Dr. Ruben Arcos presented *Anticipatory Approaches to Disinformation: The Role of Tradecraft in Strengthening Resilience* for this year's West Coast Security Conference. The presentation was followed by a simulation/scenario-based discussion in which the participants worked in groups and used proactive analysis to better understand anticipatory approaches to disinformation. Dr. Arcos designed the fictional scenario and introduced injects based on real cases to move the discussion forward. The simulation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were the evolving information landscape, the impact of disinformation and hybrid threats on democracies, and existing frameworks and responses including anticipatory approaches to countering Foreign Information Manipulation and Interference (FIMI).

NATURE OF DISCUSSION

The need for early management of information manipulation is growing increasingly clear for democracies as hostile actors attempt to shape public discourse and sow discord around significant issues like climate change and public health. Manufactured confusion around international developments, political events, or hostile activities can undermine a society's willingness and ability to respond to pressing challenges. Strategic disinformation and FIMI countermeasures include situational monitoring, incident analysis, and tools such as the DISARM framework for identifying malicious influence operations. An

anticipatory approach emphasizes proactive vulnerability assessments, early intervention, and education to mitigate the impact of hostile actors.

BACKGROUND

Presentation

Hybrid threats, as defined by the European Union, involve a coordinated mix of coercive and subversive activities that fall below the threshold of formally declared war. These tactics often target vulnerabilities through massive disinformation campaigns and efforts to radicalize or manipulate public discourse via the information space. Disinformation campaigns manipulate public opinion and exploit contentious issues around cultural identity, immigration, politics, and the authority of scientific evidence as a means of weakening the capabilities of democratic societies. Revisionist powers challenge the authority of scientific facts and territorial boundaries, amplifying societal divides and sowing confusion amongst the public. Much of this discord plays out on various social media platforms.

NATO and the European Union have developed comprehensive frameworks to combat disinformation. NATO's strategy of *Prepare, Deter, and Defend* emphasizes the gathering and assessment of information to detect and attribute any ongoing hybrid activity. Preparedness for hybrid threats is done through the continuous assessment of national vulnerabilities as well as training, exercises, and education. Deterrence involves the development of political and military capabilities that allow for prompt action. NATO bodies such as StratCom are also essential in signalling to adversaries the readiness and preparedness of NATO forces. Defense against hybrid threats entails the utilization and execution of prepared strategies.

The Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) have developed a conceptual framework for addressing hybrid threats, structured around four key pillars: actors, domains, tools, and phases. This framework is structured around thirteen domains, referred to as "instruments of national power," which include information, cyber, social, cultural, political, diplomacy, infrastructure, legal, military, space, administration, economy, and intelligence. Hostile actors use a combination of tools across these domains to achieve their objectives through activities such as interference, influence operations, and warfare.

Building on this framework, the Comprehensive Resilience Ecosystem (CORE) model represents a systems approach to counter hybrid threats by viewing democratic societies holistically. The CORE model treats the thirteen domains as "entry points or shields" to either exploit vulnerabilities or defend against hybrid tactics. Through detailed analysis, the model seeks to counter threats that undermine democracy and disrupt decision-making processes.

Complementing the CORE model, Alonso-Villota and Arcos have proposed the Coercion-Manipulation-Persuasion Framework (CMPf), which analyses the activities of Systems of Non-State Actors (SNSAs). This approach considers a range of non-state actors (e.g. terrorist groups, political organizations, businesses, and NGOs) unified by shared ideologies and political objectives. While some of these activities fall within legal bounds, they can collectively contribute to FIMI.

Strategic analysis plays a crucial role in identifying and assessing the capabilities, activities, and intentions of states and non-state entities, allowing for deepened understanding of the strategic environment and warning of future developments on issues of interest. The European External Action Service (EEAS) employs a structured analytical framework, including a FIMI threat analysis cycle and the DISARM framework. This threat analysis cycle involves mapping and monitoring the ecosystem of assets used by threat actors for manipulation and interference, collecting evidence through open sources, pooling knowledge amongst stakeholders, and providing situational analysis to guide policy and strategic decisions.

The DISARM Framework is an open-source tool designed to combat disinformation by enabling data sharing, analysis, and coordinated action across disciplines and sectors. DISARM provides a structured approach to understanding and addressing disinformation incidents. It comprises two main components: DISARM Red, which analyses the behaviour of disinformation creators, and DISARM Blue, which outlines potential defensive and mitigation strategies.

An anticipatory approach to disinformation and information-led hostile influence is critical for democracies, argued Dr. Arcos. Policymakers and practitioners can mitigate threats by assessing the likelihood of societal vulnerabilities being exploited by hostile actors, considering factors such as their capabilities, intentions, and activities. These vulnerabilities may arise from socio-political or historical conflicts, as well as events like pandemics or economic crises. Early

management of such issues can prevent damage to public opinion and improve societal resilience.

Question and Answer

What kind of metrics are used to measure the polarization in a country, what kind of metrics are used to measure the potential influence various actors might have, and what metrics are being used to analyze the malicious intent different actors might use?

A society will be severely polarized in political and cultural life, when news outlets are very editorialized and unbalanced and when discourse is overall extremely partisan. We need to develop stronger frequent surveys and polls before and after incidents to better gauge whether something has had an impact [on public opinion]. The use of social science is key. Likes and retweets aren't everything. We need to think of long-term effects such as impacts on democratic institutions. We need to look at specific patterns, sometimes tangential evidence isn't always available but consistent behaviour over time may be evidence of intentions [regarding how to measure malicious intent].

KEY POINTS OF DISCUSSION

- In addition to kinetic activities, hybrid warfare involves non-kinetic hostile acts, aiming to disrupt decision-making processes and exploit existing societal fault lines. These acts, including mass disinformation campaigns, are below the threshold for armed response and seek to destabilize nations and undermine societal resilience.
- Various strategic frameworks are in place to analyze and counter disinformation and influence operations. Models are used to track and analyze the activities of hostile actors, identify vulnerabilities, and develop coordinated responses to mitigate threats.
- Proactive assessment and addressing of societal vulnerabilities to disinformation and hostile actors is necessary to effectively counter hybrid threats. By considering factors such as socio-political conflicts or crises, democracies can mitigate risks and prevent damage to public opinion.

FURTHER READING

Arcos, R. (2021) Securing the Kingdom's cyberspace: cybersecurity and cyber intelligence in Spain. In S. N. Romaniuk & M. Manjikian (Eds.), In

Routledge companion to global cyber-security strategy (pp. 11–25). Routledge Books. https://doi.org/10.4324/9780429399718-3

Arcos, R. (2023, November 1). Strategic, anticipatory, and current analysis of disinformation and information-led hostile influencing. Presentation. Zenodo. https://doi.org/10.5281/zenodo.10064592

Alonso-Villota, M., & Arcos, R. (2024). The Coercion-Manipulation-Persuasion Framework: Analyzing the *Modus Operandi* of Systems of Non-State Actors. *Terrorism and Political Violence*, 1–19. https://doi.org/10.1080/09546553.2024.2357082

Gratton, P. (2023). THREAT RESILIENCE IN THE REALM OF MISINFORMATION, DISINFORMATION, AND TRUST. *The Journal of Intelligence, Conflict, and Warfare*, *5*(3), 96–100. https://doi.org/10.21810/jicw.v5i3.5126

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

SFU LIBRARY DIGITAL PUBLISHING