RUSSIAN INFORMATION WAR

Date: November 14, 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 November 14, 2023, Dr. Maria Miron presented the *Russian Information War* for this year's West Coast Security Conference. 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 origin of the Russian information war, Russia's objectives, and the actors involved in Russia's information war.

NATURE OF DISCUSSION

Dr. Miron discussed Russia's path in updating and reformulating the Soviet Union's active measures to meet their objectives. Russian information war does not limit itself to peacetime and encompasses both psychological operations and the military domain. The concepts of cyber-psychological and cyber-technical operations were then discussed, which included an overview of the Russian information war, Russia's objectives, and key actors involved in Russia's information war using examples from the invasion of Ukraine.

BACKGROUND

Presentation

Dr. Miron shared the core ideas of Russian information war, namely that the strategic target is the general population and not simply the military or the military psyche of the adversary. She emphasized that information war from this perspective is an all-encompassing psychological operation, with this idea emerging from references to Evgeny E. Messener's *War of Consciousness*, which he viewed as the third world war. Dr. Miron explained that Messener was an

imperial Russian soldier and military theorist who fought against communist powers, later fleeing to Belgrade where he taught at the Military Academy and eventually Argentina in 1947 where his work was conceived.

Dr. Miron stated that Russia is following a 'sticky path', meaning that they have updated and reformulated the Soviet Union's active measures, or *aktivnye meropriyatiya*, a concept known as political warfare that includes a plethora of activities; namely, espionage, propaganda, formation of front organizations abroad, and religious organizations. She explained that in 2000, Igor Panarin, a former KGB agent pushed for Russia's information doctrine which set out threats that Russia was facing in the information spectrum such as the "Color revolution". He argued that Russia needs to deny its information space to its adversaries in order to gain the ability to influence the information space independently and without attracting the attention of other actors in the international system.

Dr. Miron explained that Russia wants to engage in what it regards as 'quid pro quo', meaning the ability to undermine adversaries and prevent a victory by diverting their attention. She explained that Russia saw the West—specifically NATO enlargement—as a threat to Russia, and subsequently needed other levels of influence in order to earn a degree of plausible deniability. This case was observed with the annexation of Crimea in 2014 in which NATO was in a strategic paralysis, and delivered a great victory for Russia. The concept of creating ambiguity, fomenting chaos, and disorienting adversaries was laid out in the Russian doctrine of "Strategic Containment" in the National Security Strategy of 2009 and 2015.

Dr. Miron explained that the idea of information warfare does not limit itself to peacetime and aims to encompass the military domain, emphasizing that Russia seeks to exert control and create controlled chaos to sow division in Western societies. She stated that this is achieved through cyber-technical operations such as gathering intelligence on adversaries, probing for vulnerabilities in IT infrastructures, and causing deliberate damage using malicious code and cyberpsychological operations, such as disinformation and deepfakes. Dr. Miron identified various relevant actors such as intelligence agencies, the Internet Research Agency, troll farms, mass media, private military companies, patriotic hackers, and social media celebrities.

Dr. Miron provided the 2014 Sandworm operation in Ukraine as an example of Russia's information war, explaining that Russia practices multi-domain coordination, using cyber-attacks as precursors to kinetic actions. While its

psychological operations have faced limitations in the West due to channel bans, she stated that they have found more success in Latin America, sub-Saharan Africa, and Asia. Furthermore, Dr. Miron noted that in the military domain, Russia developed anti-satellite weapons like the laser Peresvet to blind Western satellites and extensively employs electromagnetic warfare systems causing disruptions in Ukraine by jamming drones, disabling radars, intercepting communication, and locating Ukrainian units through radio signals.

Dr. Miron asserted that Russia employs asymmetric and inexpensive means in order to exert influence, operating in channels that are difficult to trace back to Russia. She stated that while the concept of information war is not new, the methods have evolved and understanding the broad spectrum of tools and actors involved are crucial for effective countermeasures. Lastly, she mentioned that the focus on the information-psychological realm is just one aspect of Russia's strategy, emphasizing the need for a more integrated approach across all domains.

Question and Answer

Can the West overcome the narrative of Russia as an anti-imperial vanguard in emerging democracies, particularly in African nations with histories of colonial exploitation?

Dr. Miron expressed that addressing misinformation and disinformation requires increased investment, particularly in education, to help people distinguish between factual and false information. Russia's operations in Africa use a targeted narrative of psychological victimization that can manipulate a person's consciousness, underscoring the importance of countering such a narrative. There is a need for an interdisciplinary approach and multifaceted strategies to create countermeasures.

Do we have non-kinetic population defense forces or the ability to build this in democracy?

The Baltic countries and Sweden actively combat disinformation by educating their citizens and integrating Russian populations to prevent exploitation. Protection is needed not only in the physical but also in the cognitive domain, with states such as Iran, Russia, and China creating a network of disinformation to undermine democracies, and there is a need to address how these operations exploit existing societal schisms and problems.

KEY POINTS OF DISCUSSION

- The Russian information war has a strategic focus on the civilian population rather than solely the military. The psychological nature is drawn from Evgeny E. Messener's perspective as an imperial soldier and military theorist.
- Russia wants to engage in a 'quid pro quo' which means to undermine adversaries and prevent a victory by diverting their attention.
- Russia seeks to exert controlled chaos to sow division in Western societies. This is achieved through cyber-technical operations that include malicious code and cyber-psychological operations that include the spread of disinformation and deepfakes.
- Various actors involved in Russia's multi-domain coordination include the intelligence agencies, the Internet Research Agency, troll farms, mass media, private military companies, patriotic hackers, and social media celebrities.
- Education and an interdisciplinary approach are necessary for countermeasures of false narratives.

FURTHER READING

Miron, M., Whetham, D., Auzanneau, M., & Hill, A. (2023). Public Drone Perception. *Technology in Society*, *73*, 102246.

Thornton, R., & Miron, M. (2020). Towards the 'third revolution in military affairs' the Russian military's use of AI-enabled cyber warfare. *The RUSI Journal*, *165*(3), 12-21.

Thornton, R., & Miron, M. (2022). Winning Future Wars: Russian Offensive Cyber and Its Vital Importance. *The Cyber Defense Review*, *7*(3), 117-135.

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