ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON
THE
INFORMATION DOMAIN
Issue 11/22 (November)

The Hybrid War: Strengthening Defences Against Information Warfare

INTRODUCTION

1. In this contemporary VUCA[1] era we live in, the emergence of non-traditional warfare and tactics have transformed the nature of conflict. Warfare is no longer confined to conventional weapons and physical spaces, but includes new domains such as the cyber and information realms.

2. Information warfare has emerged as a fast-growing and widespread phenomenon and strategy. It falls within the ambit of hybrid warfare[2] and involves the use of different techniques and tactics to spread misinformation, propaganda and smear campaigns to engender fear and ill-will create hatred against the adversary. These methods can manifest across the entire spectrum of issues from politics to economy, and even public health.

3. Information warfare is 'borderless' as such activities are not bounded by geographical limitations and attackers can reach just about any target in the information space, particularly online. These activities are considered unconventional[3] operations that seek to manipulate one's information space, while attempting to control or destroy the adversary's information systems and flow.

[1] The VUCA era is marked by Volatility, Uncertainty, Complexity and Ambiguity.
[2] Hybrid warfare is an orchestrated campaign to fracture the solidarity of the target nation through undermining its defences in civil, economic, social, psychological and military spheres.
[3] Unconventional activities include sabotage and subversion methods to manipulate public's perception on certain issues. On the other hand, conventional means include state actors and resources that include chemical, biological, and nuclear dimensions. Most of the activities under this category include open/overt warfare.

Examples of Information Warfare

4. The North Atlantic Treaty Organisation (NATO) has reported that the internet has enhanced and expanded the possibilities of data acquisition, information defence and information disruption, making it easy to reach both the citizens of a given country and the international community. Social networking sites have also become valuable platforms utilised by malicious actors to accelerate the speed and spread of certain (dis)information.

5. One of the prominent examples include an attempt by Russian mercenaries in Apr 2022 to stoke anti-French sentiment in Mali. According to *France 24*, videos showing a blurred image of bodies buried in the sand near the military base near Gossi, Mali, with a caption accusing the French Army of torturing Mali citizens and leaving behind the mass grave was circulated on Twitter on 21 Apr 2022. This was the same week that the French Army withdrew from a military base in northern Mali. However, the French forces debunked the tweets by releasing drone footage of Russian mercenaries, stated to be members of the Wagner Group[4], planting the bodies in the sand.

Figure 1: French Forces Debunked the Accusation With Snapshots of Russian Military Planting the Bodies

6. Another example is the growing barrage of disinformation targeting United Nations (UN) peacekeeping operations such as the missions in the Democratic Republic of the Congo (MONUSCO). False claims were made that MONUSCO is exploiting the country's natural resources, selling weapons to armed groups, and supporting foreign troops. Some UN officials suggested that the sophistication of the disinformation targeting MONUSCO indicated that it was coordinated and coming from outside the country. By tapping into local anger against foreign intervention, the disinformation has endangered UN peacekeepers and made it harder for them to implement their mandate.

[4] The Wagner Group, also known as PMC Wagner, ChVK Wagner, or CHVK Vagner, is a Russian paramiltary organisation. It is variously described as a private military company, a network of mercenaries, or a de facto private army of Russian President Vladimir Putin.

Strengthening Defences Against Information Warfare

7. The use of such information strategies – be it in the forms of covert intelligence or overt domestic propaganda – to achieve strategic objectives is now an integral part of military warfare, and it has the potential to destabilise a nation and threaten national security. As such, many nations have announced tougher measures against the spread of disinformation and fake news.

8. Militaries around the world – such as Australia, India, Singapore and the US – have also recognised the importance of equipping the army with knowledge on combatting disinformation. According to *Military Times*, the training for military personnel could include: (a) providing a broad overview of the domestic and regional media ecosystem; (b) analysing the different types of disinformation campaigns and how they play on individuals' emotions; and (c) using different tactics, techniques and procedures (TTPs) such as employing reverse photo lookups or determining changes in the direction of shadows in online videos, so as to assess the authenticity of the material posted online.

9. Inoculation by raising awareness to commonly-employed information warfare tactics would also be a useful form of training. For instance, Project Convergence, conducted by the British Army at Fort Irwin, sought to strengthen soldiers' resilience and hone their responses to disinformation campaigns through a series of simulated and role-playing exercises. According to *The Sun*, the staff role-playing as civilians were given false social media networks to whip up a mob by reporting stories of abuses by US troop, and the soldiers were tasked to respond to and 'pacify' the fake civilians. According to *Modern War Institute*, militaries could also adopt the practice of inoculating against mis-and-disinformation through the launch of public awareness campaigns.

10. The *Information Professionals Association (IPA)* reported that other ways for militaries to combat disinformation could include: (a) monitoring the information space; (b) keeping track of any disinformation trends; (c) posting information ahead of time about upcoming exercises and other events to prevent any confusion about what the troops are doing on the continent; and (d) responding to disinformation warfare, such as by disseminating materials to illustrate the actual narratives.

ASSESSMENT

11. Social media and other online content generation platforms are often used by malicious actors to manipulate the opinions or perspectives of the masses. As evident by the ongoing conflict between Russia and Ukraine, social media platforms have served as a digital battleground for both sides to spread and accelerate competing narratives about the war so as to portray the conflict in their own terms. To deal with such challenges, it remains imperative for militaries from various countries to enhance the readiness of their soldiers through relevant training and exercises.

CONTACT DETAILS

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

REFERENCES

News Articles

1 Hybrid Warfare: Are Indian Armed Forces Ready to Face New Challenges?
[Link: https://www.indiandefencereview.com/news/hybrid-warfare-are-indian-armed-forces-ready-to-face-new-challenges]

2 Media – (Dis)information – Security: Information Warfare
[Link: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf]

3 Truth or Fake – Social Media Users Falsely Claim That French Soldiers Are Arming Terrorists in Mali
[Link: https://amp.france24.com/en/tv-shows/truth-or-fake/20221025-users-falsely-claim-that-french-soldiers-are-arming-militants-in-mali]

4 France Says Mercenaries From Russia's Wagner Group Staged "French Atrocity" in Mali
[Link: https://amp.france24.com/en/africa/20220422-france-says-mercenaries-from-russia-s-wagner-group-staged-french-atrocity-in-mali]

5 Information Warfare and India's Level of Preparedness
[Link: https://www.claws.in/information-warfare-and-indias-level-of-preparedness/]

6 Truth or False? The Fight Against Disinformation
[Link: https://www.mwi.usma.edu/true-or-false-the-fight-against-disinformation/]

7 Disinformation against UN Peacekeeping Operations
[Link: https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf]

8 Fake News is Wrecking Havoc on the Battlefield. Here's what the Military's Doing About it
[Link: https://www.information-professionals.org/what-the-u-s-military-is-doing-to-combat-disinformation/]

9 Military, Veterans Learn To Fight Disinformation Campaigns
[Link: https://www.militarytimes.com/veterans/2022/09/04/military-veterans-learn-to-fight-disinformation-campaigns/]

10 How British Army's Elite New Ranger Regiment is Preparing for Russian Invasion with Desert Drills in High-Tech Warfare
[Link: https://www.the-sun.com/news/6654715/british-army-rangers-preparing-russian-invasion-war-drills/]

11 Rajnath Singh Calls For Joint Global Efforts To Counter Cyber Attacks
[Link: https://www.livemint.com/news/india/rajnath-singh-calls-for-joint-global-efforts-to-counter-cyber-attacks-11668068108007.html]