HYBRID APPROACHES TO INCREASE THE EFFECTIVENESS OF DEFENSES IN THE FACE OF INFORMATIONAL WARFARE

Felix STAICU
CEO Cyber Dacians
felix.staicu@cyberdacians.com

Abstract: An overarching crisis looming over global stability is underway with no end in sight. Informational warfare is not an accessory to conventional warfare, but a strong enhancer, with the (dis) advantage that it can be used in peacetime as well. Informational warfare is now the most dangerous and important aspect of modern warfare. While propaganda and influence operations have existed since antiquity, the propagation of social media and technology have made it viral, cost-effective, and reaching potential billions of users in a short time, with the strong potential to influence and direct the new global order. Resiliency must be the key strategy to defend against it, enhancing operational capabilities in the informational sphere, government proficiency in cybersecurity innovation, and education at all levels. Modern states and alliances must acknowledge the seriousness of the threat and constantly build capabilities, develop strategies and be prepared to use them wisely to defend against informational threats that are dominating the digital world.
Keywords: Informational warfare, Cybersecurity, Disinformation, Hybrid, Ukraine, Russia.

INTRODUCTION

Current events in Ukraine demonstrate once again that history repeats itself in parallel with the unprecedented growth of the means of warfare. A great number of war dynamics have changed remarkably in the last few years making an abrupt transition to the so-called 5th-generation warfare (5GW). A global order turning multipolar, the incredible acceleration of technology, and a new global mindset have afflicted rather classic operational procedures, confusing diplomats and military leaders alike who are confronted with an invisible, face-less, and border-less enemy that disrupts the foundations of reality.

5GW implies that war is transitioning to a war on information and perception that is using mis/disinformation, cyber-attacks, artificial intelligence, social engineering, Open Source Intelligence (OSINT), electronic warfare, and social media, to target cognitive biases of individuals and organizations, disrupt/manipulate the functioning of key IT systems, in a way that is close to impossible to attribute it and *currently* defend against properly (Radio Research Group, 2022). 5GW includes Influence Operations, which are coordinated efforts to manipulate or corrupt public debate for a strategic goal. Influence Operations are done through paid humans that are being used to shape narratives and through coordinated inauthentic behavior on social media, realized through armies of bots and trolls.

In Russian strategy, informational warfare is a holistic concept conceptualized within a broader framework that addresses cybersecurity, disinformation, and cognitive operations altogether in a cohesive informational warfare strategy that guides its foreign policy (Connel, Vogler,

2017). Soviets understand the value of information and its capacity to influence mentalities and actions, thus they are using the strategy masterly both at home and abroad to influence and advance their interests. The Russian use of *maskirovka,* translated into military deception, is being witnessed firsthand in the Ukrainian war. Moscow has established a new level of ambition – strategic Maskirovka – by which disinformation is applied against all levels of NATO's command chain and wider public opinion to keep the West politically and militarily off-balance (French, 2015).

NATO countries think of cybersecurity strategy separately from other informational elements, leaving some key elements uncovered, which in turn result in vulnerabilities. NATO countries also have separate strategies for each element of the informational warfare, thus resulting in an insufficiency of cohesiveness between the cognitive, informational, and cyber-space which is detrimental to an effective defense against informational warfare. In this paper, informational warfare is defined as the combination of cybersecurity, information, and cognitive warfare.

RUSSIA'S INFORMATIONAL WAR IN UKRAINE

Even though the harsh reality in Ukraine is still highly kinetic, Ukrainians are fighting a 21st-century war, which is half on the internet. It was witnessed a surge of moves from the informational sphere, from all parties involved. In pre-war times, psychological operations were conducted to demotivate the Ukrainians and instill fear, and cyber-attacks were conducted to demonstrate force, gather intelligence and confuse leaders. At home, Kremlin conducted a disinformation campaign to gather support for the invasion, suggesting that Ukraine needs to be saved from the nazis.

During the war, the informational spectrum of warfare has become increasingly active, with a plethora of cyber attacks being conducted from both actors involved in the warfare, and non-state actors supporting each side, such as Network Batallion 65 (NB65), supporting Ukraine, or Conti Ransomware group supporting Russia. Non-state actors have been progressively active during the war, two months into the war, NB65 hacktivists have leaked more than 6 million Russian documents (Lee, 2022), and Russian hacker groups are launching thousands of Distributed Denial of Service (DDoS) attacks on countries that support Ukraine, using Dark Web forums to gather supporters.

Since the start of the war in Ukraine, the Russian influence operations had not been as effective as in previous conflicts in Georgia and Crimea, having limited effects being met with a determined Ukraine that responded wisely, taking the lead in the informational arena. The low intensity of the Russian informational warfare, should not be interpreted as a lack of capabilities or willingness to use them. Doing so would be a dangerous bet that can have serious consequences.

On social media and international press, Ukrainian rhetoric became preponderant, quickly attracting the support of the public, using it in the informational offensive against Russia. Shortly after, Russia decided to ban Facebook, Instagram, and Twitter (The Guardian 2022), limiting the amount of information its citizens could interact with. Intending to enhance intelligence leaks within Russia, the CIA has shared information on Instagram, instructing

Russian users on how to securely submit data over the Dark Web, without being traced (Loh, 2022). Ukrainian strategists took advantage of the support shown online and gathered the ranks of a cyber army, in which hackers could join after a vetting process and attack Russia.

HOW INFORMATIONAL WAR IS FOUGHT

Social media became a treacherous weapon at everyone's disposal, where influence operations are conducted with the help of groups of trolls and networks of bots that spread narratives, artificial intelligence that interprets and predicts the behavior of millions (or even billions) of accounts, coupled with attentive manipulation experts that are creating cognitive campaigns able to influence masses and even elections. At large, social media is and will be the main arena for 5th generation warfare, with plenty of new techniques in the pipeline, for example, deep fakes videos, that impersonate realistically the appearance and voice of any person, using Artificial Intelligence.

Informational warfare offensive is highly effective when done right, and most operations are cost-efficient. Defending against it on the other side is highly difficult, requiring both proactive and reactive approaches, investment in continuous education, operations, and cybersecurity defenses, and a well-established strategy of response when such attacks happen. The lack of international regulations against cyber attacks and disinformation is another factor worth noting, deterrence in this regard is almost inexistent, although efforts have been made both in Europe and the US to build a regulatory structure. Former NATO officials mention that NATO must re-learn deterrence (Hodges, Koster, 2022), and this is especially true in the informational spectrum, where NATO states have long been the subject of attacks with no consequences for the *alleged* perpetrators. Efforts have been made at the Nato Strategic Communication Center of Excellence based in Riga to work with social media companies on developing a robust platform of analysis and tracking Influence Operations and recommendations on how to improve effective policies against them. However, the lack of proper reaction and a structure of response against informational warfare is concerning and should come at the top of the priority list for diplomats and statesmen alike to build resiliency and deterrence.

During the Cold War, deterrence between the US and Russia was achieved by the fear of Mutually Assured Destruction (MAD). During current times, when classic deterrence seems to have expired, there are proponents of a Cyber Mutual Assured Destruction Doctrine (CyberMAD) that will rebuild deterrence in the cyber world, based on the fear of consequences. Proponents argue that for CyberMAD to work, there must be a capability to be worthy of the fear, and there must exist a threshold and a trigger for it. Attacks from non-state actors or unattributed attacks might constitute an issue for the CyberMAD Doctrine, which in theory would work to deter a state actor, but might be excessive and impossible to apply for a non-state actor.

No country controls the cyber-space and all countries are now reliant on cyberspace, which makes it a hefty target. CyberMAD does not imply exclusively a cyber attack on a target, it can also imply a kinetic attack on a cyber node, a space attack on satellites, or an electromagnetic pulse that will blackout instantly the internet (Gale, 2009). This is already happening,

malicious Russian submarine activity was frequently identified close to the undersea internet cables that connect the global internet (Warsaw Institute, 2022) and Russia was behind the Viasat satellite cyber attack, which produced outages in Eastern Europe hours before the Russian invasion (Page, 2022).

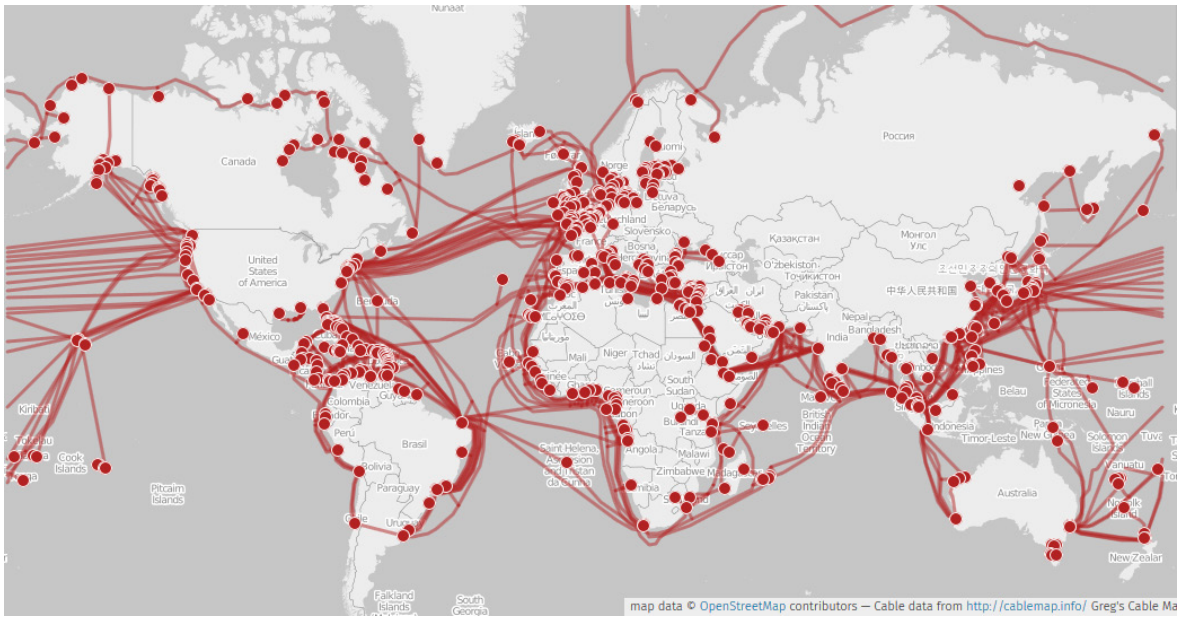

Figure. 1 *Undersea Internet Cable Map,*
Source: Wikipedia, retrieved from https://en.wikipedia.org/wiki/Submarine_communications_cable#/media/File:Submarine_cable_map_umap.png/

An increasing number of countries are taking serious measures to increase their cyber readiness. The US, UK, Israel, China, Russia, and Iran are global leaders in this regard, possessing advanced capabilities, especially in the offensive spectrum.

Recently, informational warfare as a whole started to receive more attention, and states started to launch anti-disinformation agencies that began to counter the effects of informational warfare. In Sweden, the recently created Psychological Defence Agency (Psychological Defense Agency, 2022) has the mission to coordinate and develop the psychological defense of the country, strengthening the resilience of the population. It is a government agency created under the Ministry of Justice that was created to create and develop a modern psychological defense that has a real capability in peacetime, at heightened preparedness, and ultimately in war. Similarly, France, Slovakia, and recently the US have created anti-disinformation agencies that will be responsible for dealing with disinformation increasing the resilience of their states. The trend is clear, sooner or later, all countries that value the power of information must protect it, and agencies such as these will become the norm. Critics might name them the Ministry of Truth and might argue that it is not the government's job to say what is true and what is not. The alternative, however, is more dangerous, full exposure to the informational offensive without a reaction paves the way to strategic defeat and social decomposition. It is the responsibility of statesmen to find the right balance that'll preserve security and democracy.

CONCLUSION

5th-generation warfare is on the verge of becoming a permanent state between countries fighting for supremacy in the new global order. To counter the informational warfare effectively, NATO must employ a better strategy than Russia, encompassing cybersecurity, influence operations, disinformation, psychology, and other key factors in a body that will be consistently evolving to keep pace with the growing threat landscape.

For the strategy to be successful, the key requirement is the cohesiveness of the NATO member states in their internal and external affairs. Once that is achieved, the next step for NATO is to jointly develop capabilities to efficiently emanate deterrence in the virtual space. The strategy as a whole should follow a top-down approach, emanating from NATO, having a central Informational Operations Command and Control Center (IOC2) that will gather specialists from all states to defend the interest of the alliance. Capabilities should include influence operations, offensive cybersecurity, cognitive operations, intelligence sharing, OSINT, and threat intelligence, among others. Cyber offensive capabilities are especially important for member states to increase the consequences of an attack on their infrastructure and avoid fighting a cyber-war only defending, which is doomed to fail eventually. These capabilities will help to start tilting the balance of power in the cyber realm and help the Member States which have been consistently subjected to cyber attacks to regain the deterrence in the cyber-space.

The purpose of the IOC2 should be multi-dimensional, being both proactive and reactive, defending against all types of informational threats, building knowledge about the threat environment, developing tools and strategies that will be ready to use in the case of a threat, and most importantly, creating capabilities that can help NATO as a whole to win the informational warfare in the long run and create deterrence against its strategic competitors.

At a minimum, Member States should implement a national Anti-Disinformation agency, that will protect its citizens against disinformation reactively, will build critical thinking amongst its most vulnerable targets, and will act as the responsible central body to respond to these threats. The center should be fully integrated into the central IOC2, contributing and extracting knowledge, and being included in a closed network of similar agencies that are sharing intelligence to ensure swift and proper response against informational warfare. Ideally, the agencies should come under the Defense Ministries as they will be dealing with the collective defense against informational warfare, which should be recognized by the Member States as a threat to national security. Agencies must be independent of political and military influence and should have a strong code of ethics that will be enforced by a transparency board. This is necessary to avoid manipulations of decisions and to progressively construct the trust of citizens in these kinds of institutions. Agencies should also be fully integrated with the national CERTs, being trained to act together when situations that include both cyber attacks and influence operations occur in conjunction.

Regional dynamics that are in danger of escalation suggest that a *timely* approach to developing strategies and capabilities should be employed, addressing holistically the key

points of information warfare in line with the conventional strategies. Nevertheless, 5th generation warfare is something that leaders, military people, and diplomats recently started to experience and which requires the development of 5th generation diplomacy to solve crises peacefully. Diplomacy is generally the first line of defense against any type of threat, and it must adapt to the informational warfare spectrum to create convincing strategies for dealing with these issues. At a minimum, Cyber Ambassadors should become common for every country that wants to be on top of cyber threats, and the role should evolve to encompass all aspects of informational warfare as previously demonstrated. Through strong diplomacy, cohesiveness, strategy, and operational capabilities, informational warfare can be defended against, avoided, fought, and won, safeguarding the values of democracy and free thought in the face of aggression and interference.

REFERENCE LIST

Connell, M. & Vogler, S. (2017). *Russia's Approach to Cyber Warfare. CNA Analysis and Solutions*, retrieved from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

French, L.F. (2015). *NATO: Countering Strategic Maskirovka,* ISIJ 50: DIGILIENCE 2021: AI-driven Cybersecurity Solutions, Cyber Ranges, and Military ICT Applications, retrieved from https://www.cgai.ca/nato_countering_strategic_maskirovka

Gale, D.A. (2009). *CYBERMAD: Should the United States adopt a Mutually Assured Destruction policy for Cyberspace?*, Air Command and Staff College Air University, retrieved from https://apps.dtic.mil/sti/citations/ADA539622

Hodges. B., Koster, T. (2022). *NATO must re-learn deterrence*, retrieved from https://cepa.org/nato-must-re-learn-deterrence/

Lee, M. (2022). *Russia is losing a war against hackers stealing huge amounts of data,* retrieved from https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/

Loh, M. (2022). *The CIA is using Instagram to teach Russians how to share state secrets with it,* retrieved from https://www.businessinsider.com/cia-using-instagram-teach-Russians-share-state-secrets-ukraine-war-2022-5

Page, C. (2022). *US, UK, and EU blame Russia for 'unacceptable' Viasat cyberattack*, retrieved from https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/

Psychological Defense Agency. (2022). *Mission*, retrieved from https://www.mpf.se/en/mission/

The Guardian. (2022). Russia bans Facebook and Instagram under extremism law, retrieved from https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law

Warsaw Institute. (2022). *Russia Cripples NATO's Undersea Communications,* retrieved from https://warsawinstitute.org/russia-cripples-natos-undersea-communications/

Felix STAICU
Is a professional with an overarching experience across the digital threat landscape, with experience ranging from cybersecurity, diplomacy, and information warfare. He holds a Master's in International Security and Law, from the University of Southern Denmark, specializing in new types of conflicts. Currently, he is leading Cyber Dacians' commercial activities while also coordinating field projects and implementations in the cybersecurity field.

In parallel, he's leading the Threat Intelligence department of Intel4Patriam, an organization focused on combatting online disinformation, influence operations, and the new generation of information warfare. By leading a cross-functional team he is interested in the source and propagation of influence campaigns directed by state and non-state actors.

Following his vision to unite the Romanian cybersecurity industry, he is a founding member of CYSCOE - Cyber Security Cluster of Excellence, a cluster made of companies, universities, and research institutes focused on cybersecurity and the application of new technologies.