# COUNTER-CYBER REFLECTIONS FOR NATO

Author-Casey Riggs, HQ U-A/A5X, SOS 21A, 15 December 2020

## Background

Since the mid 1990's, Russia has steadily recovered its ailing economy from post-Soviet collapse and resurfaced onto the world stage. It is Vladimir Putin's objective to re-establish the Russian Federation (RF) in the international arena as a global security broker and secure Russia's sphere of influence in a polycentric world rife with instability[1]. The Russian strategic vision is clearly illustrated by both publically available documentation as well as overt action on Russia's periphery in places like Ukraine, Moldova, and the Baltic states. Much like the Allied dealings with the USSR during the Cold War, some have claimed that recent events are reminiscent of the clandestine and indirect interaction between the Soviets and West[2], an idea expressly acknowledged by the second highest ranking Russian official, Prime Minister Dmitry Medvedev. This notion is also supported by the relative continuation of proxy conflicts between Allied nations and the RF in Syria, Libya, and Nagorno-Karabakh.

Both the Russian National Security Strategy and Military Doctrine serve to frame the Russian worldview and set an important backdrop for RF political and military actions around the world. The RF views the world as an increasingly chaotic environment, and specifically mentions the political and military actions of the U.S. and NATO Alliance as direct threats to Russian welfare[3]. From this viewpoint, the RF sees itself as involved in an ongoing conflict with the West, unlike the Western perception of peacetime competition. The defensive lens that the RF views the world helps to provide context for the seemingly aggressive actions Russia is taking, notably in their near-abroad – the very same area of influence the Soviet Union held at its height.

### *Russian Doctrine and Organization*

Since the Russian-backed cyber attacks of the Second Chechen War, both the West and the RF have seen an increasing growth in capability and complexity of cyberspace activities in the military sector. Although the RF has shrouded their organizational structure in secrecy, especially those forces assigned to conduct operations in cyberspace, most of these capabilities remain embedded in various intelligence agencies. Russia has also demonstrated use of proxy forces, hired on as "mercenaries" to conduct non-attributable cyber operations.

RF doctrine nests cyber operations within the structure of information warfare alongside electronic warfare, psychological operations, and information operations (IO)[4]. In this fashion, cyber operations (or "computer network operations") are easily paired with, and historically used as an enabler for these other activities in an offensive capacity – notably IO. In fact, Russian

---

[1] "Russian National Security Strategy." 31 December 2015. <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf>.
[2] Shuya, Mason. "Russian Cyber Aggression and the New Cold War." Vol. 11. 1. 2018. 1-18. <https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1646&context=jss>.
[3] "The Military Doctrine of the Russian Federation." 25 December 2014. <https://rusemb.org.uk/press/2029>.
[4] Connell, Michael and Sarah Vogler. "Russia's Approach to Cyber Warfare." 2016. <https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf>.

Doctrine consistently acknowledges the potential threats of IO against the RF, and their actions support those realizations via conduct of their own IO against other nations.

Recently, the Main Directorate of the General Staff (GRU) has been taking a more prominent role in the conduct of cyber related actions including attacks against electrical networks, banking sectors, government institutions, and the 2018 Olympics[5][6]. This development marks a shift in focus from intelligence collection by state agencies such as the FSB and SVR to more brazen military cyber activities by the GRU.

*Allied Doctrine*

Allied Doctrine frames cyber operations within a defensive lens, however subsequently acknowledge requirements for coordinating offensive effects through a structure called Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)[7]. Although NATO nations are developing these cyber capabilities, they struggle to organize under a cohesive operational goal and within a military framework, in which the budding NATO Cyber Operations Center (CYOC) may well address[8].

Although defensive cyber operations appear to fall within the purview of military responsibility, NATO has repeatedly emphasized a strong cooperation with academia and industry to bolster passive defense (i.e. cybersecurity) via outreach to entities such as the EU, UN, and OSCE. NATO also shares information and training through the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), various schools throughout Europe, the NATO Industry Cyber Partnership (NICP), as well as various NAC boards and committees.

The member states of the NATO Alliance have also increasingly integrated cyber focused capabilities within their respective military hierarchies. Of the NATO Alliance, the U.S. CYBERCOMMAND structure arguably represents the most mature entity for the conduct of cyber operations in a respective NATO nation since its inception in 2010[9]. NATO has embraced its role in the collective defense of cyberspace by adding cyber defense to its core tasks in 2014[10].

*Fundamental Cyber Issues*

The basic military responsibility is often defined within the construct of security and safeguarding the homeland against outside threat, and in some cases, ensuring stability of internal affairs. With regard to the cyber domain, the notion of sovereign cyberspace, positive attribution, and appropriate response, and applicable legalities are ill-defined and complicated in a number of ways. These fundamental issues shape the current approach to cyberspace

[5] "Russian Military Intelligence: Background and Issues for Congress." 2020. <https://crsreports.congress.gov/product/pdf/R/R46616>.
[6] "BEARING WITNESS: Uncovering the Logic Behind Russian Military Cyber Operations." Booz Allen Hamilton, 2020. <https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html>.
[7] "AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS Edition A Version 1." NATO STANDARDIZATION OFFICE, 2020.
[8] Lewis, Don. What is NATO really doing in cyberspace? 4 February 2019. <https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/>.
[9] Smeets, Max. "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis." 11th International Conference on Cyber Conflict: Silent Battle (2019): 163-177.
[10] Cyber Defence. 25 September 2020. <https://www.nato.int/cps/en/natohq/topics_78170.htm>.

operations by both Russian and Allied governments and largely account for the clandestine nature of modern cyber operations.

Firstly, the geographic borders of states provide a clear delineation of territorial sovereignty in the areas of land, sea, and air. Akin to the first layer of cyberspace, physical infrastructure can mostly be accounted for via relationships between autonomous systems. However, ownership and authority become more complex with undersea infrastructure or satellites in orbit, as there are no internationally recognized borders above the Kármán line (100 km). Even in the first layer of cyberspace, legal frameworks begin to degrade as common infrastructure is spread across physical space.

Second, the logical structure of the internet, used to route information, rests on a highly interconnected network topology and shared trust between connected devices. Central organization of allocation of IP addresses is provided by IANA, however there is are no "owners" of the disparate logical topology and IP addresses themselves are only loosely connected to information systems owned by governed businesses. Traffic between logical entities is easily modifiable for nefarious use. Herein presents a core problem of attribution, an important factor in the conduct of cyber operations. An actor can communicate or attack from one logical entity to another, while easily obfuscating any information which might reveal their identity. This issue, combined with a lack of central authority and agreed upon governing rules, presents a veritable "Wild West" in which the most cunning actors are able to operate with near impunity. Both the RF and Allied forces utilize the attribution problem to conduct clandestine cyber operations, protecting both themselves and the grey space networks they operate from with plausible deniability.

Third, it does not suffice to omit the problems of cyber-personas. While cyber-personas can be used as a tool to partially address the attribution problem, they only represent one-half of the progressing legal enforcement mechanisms; the other half is characterized by application of appropriate response. Exercising an effective and appropriate response to a hostile cyber action is not well-defined and response in-kind may not be possible or effective. For example, the EU has attempted to address this problem with the Cyber Diplomacy Toolbox that provides recommended response options[11]. The RF, on the other hand, consistently exercise a policy of "threats" and "punishment", while holding adversary infrastructure at risk.

Fourth, obscure legalities create an opportune environment with which to conduct clandestine operations, especially those which fall below the threshold of armed conflict and therefore do not invoke International Humanitarian Law. Proponents of cyberspace law advocate the need for tenets in-line with laws of armed conflict such as proportionality and necessity[12]. The development of the Tallinn Manual 2.0 represents perhaps to most mature legal approach to

[11] Moret, Erica and Patryk Pawlak. "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" European Union Institute for Security Studies (EUISS), July 2017. <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf>.
[12] Roguski, Przemysław. "Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?" 12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade (2020): 25-42.

application of existing legal frameworks, yet highlights the lack of international agreements in this area[13].

## Counter-Cyber

### *Offensive vs. Defensive Dilemma*

Offensive and defensive actions have long been the contention of political rhetoric and cyberspace is no different. The applicability of the terms “offensive” and “defensive” are usually based around sovereign ownership, which as aforementioned, is ill-defined. By examining the environment, we can see that any effective cyber operation must capable of extending effect through grey networks and affecting red networks, whether to defend one’s own network or to attack another’s.

For example, passive cyber defense (i.e. patching and best practice) is largely insufficient against a determined cyber actor, especially those belonging to well-funded national institutions such as militaries or intelligence entities like those in the RF. Russia has effectively demonstrated the ability to covertly prepare a cyber environment for follow on action, as well as conduct more ad-hoc DDoS style attacks against various types of systems for political purposes or even in coordination with military movements. There is no conceivable way to ensure the security of networked systems by passive measures alone.

NATO, as a military entity, is currently focused on defending its military Command and Control networks. This priority is mirrored in U.S. Joint Doctrine[14], however CYBERCOM has taken a more aggressive stance in its “Defend Forward” concept[15], realizing the strategic importance of extending cyberspace effects, in a defensive capacity. Notionally, this concept seeks to mitigate vulnerability by active defense, however this version of active defense can closely resemble that of pre-emptive offensive action.

### *Critical Infrastructure*

Civilian critical infrastructure has been a longstanding topic of concern and most recently, the attacks on the Ukrainian power grid have shown just how vulnerable this sector can be. It is clear that military cyber activities unconstrained to military target networks can have devastating effects on the civilian populous, that very same populous that military institutions are charged to defend. As a practical example, effects based operations and center-of-gravity analysis often identify non-military targets which can have extremely effective results, a lesson learned around the world during the U.S. led Operation Desert Storm.

Although Allied cyber defenses, by necessity of limited capacity, are concentrated on military communications networks and major weapon systems, civilian cybersecurity remains ill-equipped to confront determined military cyber actors. It is therefore necessary to include the active defense of critical infrastructure within the realm of military affairs. This does not

[13] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.
[14] Staff, Joint Chiefs of. JP 3-12, Cyberspace Operations. 8 June 2018.
<https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150>.
[15] Cyberspace Solarium Commission Report. March 2020. <https://www.solarium.gov/report>.

preclude civilian cybersecurity practice, but rather enhances it with offensively oriented military capabilities when necessary, and preferably proactively.

*Legal Frameworks*

The development of legal frameworks with respect to cyberspace will have major consequences for the conduct of both active cyber defense and offensive operations. The sanctity of national boundaries in cyberspace and an increased focus on national responsibilities to protect non-combatants from the effects of cyberspace action will make operating in grey networks more legally restricting and further entrench the clandestine conduct of cyber operations[16]. The ability to project effects through this grey space in active defense will likewise become more difficult.

Conversely, garnering support through civilian sectors, formerly classified as grey space, to operate complex cyber operations will drastically affect non-attribution, and would mark a major shift for executing cyber action covertly. Operating overt cyber operations is prohibitive and counter to the current asymmetric advantage non-attribution provides, at least currently[17]. The progression of legal frameworks needs coincide with the development of national agreements regarding the ability to project effects through grey space for both offensive and defensive operations, while still balancing a legal regard for civilian networks.

## Conclusions

The rapid progression of Russian military cyber capability, increasing complexity and frequency of malicious cyber action, and the threat to civilian populous through asymmetric effects on both military and civilian architectures garners increased attention by the NATO Alliance. The scope and responsibility of the NATO Alliance with regard to cyber operations must continue to develop and expand in order to better posture against Russian threats. It is advantageous for NATO to adopt a more active defensive posture, as well as maintain a focus on information sharing and cybersecurity practice in a civilian industry ill-prepared to defend itself from advanced national actors. It is vital that NATO include a focus on critical infrastructure within the purview of its cyber operations as a matter of responsibility to the collective defense of the civilian populous. Lastly, it is extremely important that NATO and the EU cooperate in the international arena to smartly develop legal frameworks that balance both the sovereignty of national cyberspace borders and the necessity to conduct active cyberspace operations in grey space, until the benefits of overt cyber action outweigh non-attribution of clandestine operations.

[16] Park, Tina and Michael Switzer. "R2P & Cyberspace: Sovereignty as a Responsibility." 12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade (2020): 113-127.
[17] Baram, Gil and Udi Sommer. "Covert or not Covert: National Strategies During Cyber Conflict." 11th International Conference on Cyber Conflict: Silent Battle (2019): 197-212.