Offensive Cyberspace Operations for Cyber Security

Gazmend Huskaj[1]
[1]Geneva Centre for Security Policy, Geneva, Switzerland

g.huskaj@gcsp.ch

Abstract: This work-in-progress research product covers Offensive Cyberspace Operations for Cyber Security or "Offensive Defense" for Cyber Security. Offensive cyberspace operations are shrouded in secrecy. From an intelligence perspective, this makes sense because of their development since Operation Desert Storm in 1991. The phenomenon, dubbed "Information Warfare," and to the professionals' surprise, they could remotely turn off an Iraqi power substation. However, the implication of remotely turning off the power substation was not only to cut off the power source to an Iraqi military headquarters, but it also meant cutting off the power to a nearby hospital, risking the lives of injured Iraqi soldiers protected by the Geneva Conventions. Since the 2000s and onwards, and with the US military recognizing cyberspace as a war-fighting domain, establishing United States Cyber Command (USCYBERCOM) may be a milestone. Thus, researchers have put much thought into cyberspace operations (offensive, defensive), such as doctrine, organizations, training, materials, leadership and education, personnel, facilities, and policy. One phenomenon, dubbed "defending forward," was coined in the 2018 US Department of Defense Cyber Strategy. The idea is simple: take the fight to the adversary. Other terms include "hunt-forward operations" and "offensive defense." Therefore, what is "Offensive Defense" for cyber security, and why now?

Keywords: Cyber Security, Information Warfare; Offensive Cyberspace Operations, Offensive Defense.

[1]*The views expressed in this paper are only those of the author, and do not represent the Geneva Centre for Security Policy (GCSP), or any other party.*

1. Introduction - Why Offensive Cyberspace Operations for Cyber Security?

Offensive cyberspace operations for Cyber Security is a relatively new concept. The idea is to strike a threat actor's targets through offensive methods to impose cost (Fischerkeller & Harknett, 2017) on the adversary to alter the threat actor's decision-making. Inferring costs could be by attacking critical infrastructure necessary for the threat actor to conduct their operations. By taking the fight to the adversary, it may be possible to make them switch stance: from an offensive stance to a defensive stance, for example to secure their systems.

Researchers have described the issue with deterrence and argued that the concept applied in the physical domains (air, land, sea, and space) does not work in the same matter in cyberspace. The research question is, therefore: What are offensive cyberspace operations for cyber security, and why now? Offensive cyberspace operations are defined as:

"a sequence of planned actions executed by an organised group of people with a defined purpose in and through hardware and software which are used to create, process, store, retrieve and disseminate information in different types of interconnected networks that build a large, global network, built and used by people. The offensive aspect includes methods to affect an adversary's target system's confidentiality, integrity and/or availability. These targets include 'weapon systems, C2 processes, logistics nodes, high-value targets'"

(Huskaj & Wilson, 2020, p. 513)

This article begins with a review of the scientific literature identifying the concepts of persistent engagement, defending forward, and offensive cyberspace operations for cyber security. The review output is a conceptual framework of elements needed for offensive cyberspace operations for cyber security, depicted in Table 1. The methods section is presented in 3, while the results in 4 and the discussion in 5.

2. Reviewing the Literature

In 2017, Fischerkeller & Harknett wrote an essay arguing that protecting or advancing national interests could not merely rely on deterrence. Second, shaping behavior in cyberspace requires conducting "active cyber operations" (p. 382). Their rationale is that because many cyber attacks have taken place, the deterrence strategy within the assumption that threat actors would restrain from conducting attacks is not working. One of the main reasons behind this rationale is the nature of the cyber domain. The cyber domain is an operational environment with information systems interconnected in networks of networks. Because of this, threat actors use this low-entry high-impact domain to influence, a domain that cuts through all the other domains of national power. Therefore, connected entities are always in contact with each other. Instead of having this deterrence strategy, the idea is to have a forward-leaning approach with persistent engagement. One year later, James A.

Lewis (Lewis, 2018) presented his perspectives in a book chapter about risk, resilience, and retaliation: American perspectives on international cyber security.

Lewis (2018) notes that because information systems are always vulnerable, more than a defensive strategy against persistent threat actors is required. He continues to note that states that are "not constrained by the etiquette and rules of Western law" (p. 252) will exercise cyber power by combining it with "conventional military and intelligence assets" (p. 252). Just like Fischerkiller & Harknett, Lewis (2018) argues that a defensive posture is insufficient, and the notion of "imposition of consequences" must be considered. In other words, it is about imposing costs on a threat actor's behavior and actions in cyberspace. Imposing costs is achieved by "persistent engagement" and "collective deterrence": like-minded states respond to malicious actions in cyberspace that violate UN-developed norms of responsible state behavior. Lewis (2018) continues to discuss potential risks with a "persistent engagement"-strategy, such as the risk of escalation, and that policy for this should be in place. He concludes that U.S. cybersecurity policy is more confrontative with a greater risk of warfare. However, not acting and remaining a victim is not that way forward.

Jason Healey (Healey, 2019) provides the background story of the policy direction of persistent engagement and the possible actions the new strategy might have. he presents the topics of strategic stability, superiority, and forward defense. Regarding strategic stability Healey (2019) states that the Internet is a complex system, and small input can generate unintended effects. The continuation of persistent engagement may create a far more insecure system than today which would impact trust. Furthermore, Healey (2019) notes that forward defense in cyberspace could be one of those problems that do not provide more stability but can make things worse, and the process of understanding this new environment is as with nuclear weapons; it is going to take decades because this is not only persistent it is permanent. He continues to present the importance of rhetorics concerning, for example, the difference between offensive cyberspace operations (OCO) and defensive cyber operations-response actions (DCO-RA), where the main difference between OCO and DCO-RA lies in the fact that DCO-RA missions may include actions that rise to the level of use of force with physical damage or destruction of enemy systems. At the same time, OCO is "intended to project power in and through foreign cyberspace [to] target adversary cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading effect" (Healey, 2019, p.2). Finally, he presents the changes to policy, from Presidential Policy Directive 20 (PPD-20) to National Security Policy Memorandum-13 (NSPM-13), delegated authority to the dual-hat chief of the National Security Agency (NSA) and US CYBERCOM for OCO: a shift from the Obama administration to the Trump administration.

In 2019, Healey & Jenkins presented a policy framework to assess whether the U.S. policy in persistent engagement is "suppressing or encouraging attacks." The idea here is like the concept of "battle damage assessment" but on the policy level.

Kosseff (2019) looks at defending forward (persistent engagement) from an international law perspective. More specifically, what opportunities and limits does international law provide? He concludes that international "provides the United States with significant leeway to position itself to degrade adversaries' cyber operations, collect information about cyber threats, and discourage other states from acting against the United States in cyberspace" (p. 1).

Sebekin (2020) analyses the U.S. policy on persistent engagement. He states that while there is an opportunity to shape acceptable behavior in cyberspace, so are the related risks with possible escalation. He concludes that "the prospects of this strategy are ambiguous" (p. 96), and only through the "accumulation of empirical experience in the application of this strategy" (p. 96) will the advantages and risks become apparent. The author argues that state relationships between Russia and the United States require an understanding of "U.S. approaches to cyber security and key strategic changes to them" (p. 96) to help shape Russian cyber security policy and build a "constructive dialogue with Washington on cyber security issues" (p. 96).

Table 1: Summarizes the concepts from the review discussion.

Concept	Definition	Key references
Deterrence	Through the threat of attack, or the conduct of attack, alter the adversary's calculus by enforcing costs	(Fischerkeller & Harknett , 2017; Lewis, 2018; Healey, 2019)
Persistent engagement	Using offensive methods in the adversary's infrastructure to shift their posture from offensive to defensive	(Fischerkeller & Harknett , 2017; Lewis, 2018; Healey, 2019)
Policy	Necessary policy in place that enables a cyber unit to conduct offensive cyberspace operations for cyber security	(Fischerkeller & Harknett , 2017; Lewis, 2018; Healey, 2019)
Frameworks	Frameworks to measure if policy on persistent engagement is suppressing or encouraging attacks	(Healey & Jenkins, 2019)

Concept	Definition	Key references
International law	What does international law state in relation to offensive cyberspace operations below the threshold of an armed attack	(Kosseff, 2019)
Diplomatic Dialogue	By understanding other states' policies help shape own polities for constructive dialogue	(Sebekin, 2020)

3. Methods and Materials

The research approach to this article was to search the Scopus database, the world's largest academic database of abstracts. Using the keywords {persistent engagement} reveals 74 document results. The results included many other research fields, such as Agriculture, Biology, Medicine, and Neuroscience. A manual review of the results revealed 14 research articles on Persistent Engagement. Manual screening of the 14 research articles presents six articles for review. The next step was to review open sources for empirical evidence on persistent engagement. The purpose was to identify cases for review to answer the research question and, more precisely, the second part: why now?

4. Results

Research articles on persistent engagement, defending forward, and offensive cyberspace operations for cyber security have increased over time. In 2017, one article presented why deterrence in cyberspace does not work as it does in the physical domains. In 2018, only one article provided the risks and opportunities of this new policy strategy. In 2019, researchers published three research articles reviewing historical developments in the field and providing a rationale for why deterrence in cyberspace was not working with different cyber operations concepts and a policy shift from one administration to another. The same year, another researcher wrote about how international law could allow persistent engagement. According to that author, international law provides significant leeway. Finally, in 2020 a Russian researcher provided an article to analyze US policy on persistent engagement and why this kind of research is essential for understanding another nation's cyber security policies and to help shape Dialogue between the two capitals.

Deterrence is a strategy applied in the physical domains. The early thinking was about applying deterrence in cyberspace. However, as the review provides, strategists and researchers considered it not applicable in cyberspace. Because the operational environment, information systems in networks of networks, is unique in many causes compared to the traditional domains. Some examples include proximity, speed, and impact. States, while geographically separated, in cyberspace are only milliseconds away. While combat aircraft can fly at 3.2 Mach, information systems can send instructions at speeds close to light speed, and while a navy ship can fire cruise missiles, the impact can be devastating. In cyberspace, it is possible to alter the instructions of a system to create all the effects as in physical space. However, it is also possible to generate disruptive effects through operations below the threshold of armed attacks.

A policy that dictates the use of offensive cyberspace operations within an overarching national strategy for cyber security is essential. Policy-makers must understand all the technical underpinnings of offensive cyberspace operations and the operational environment. However, they understand the impact and consequences of failed operations. It is ultimately the policy level that takes the political risk. According to open sources, when President Bush was in a hand-over/take-over with President Obama, President Bush asked President Obama to continue with two programs: the "drone program" and a program on offensive cyberspace operations. The Obama administration understood the importance of OCO. However, they likely did not feel comfortable delegating their use to USCYBERCOM. Reviewing the open-source literature indicates that USCYBERCOM became more mature as they conducted OCO. With the shift from the Obama administration to the Trump administration, they delegated decision-making to conduct OCO to the head of the NSA and USCYBEROM. It is likely an indication of an administration willing to take more political risk and that USCYBERCOM was becoming more mature.

International law is necessary and tries to govern the behavior of states. However, international law does not prohibit the work of intelligence agencies. Therefore, cyberspace operations for intelligence, surveillance, and reconnaissance (ISR) are not prohibited. Cyber-ISR operations can occur over time and, like traditional intelligence operations, do not violate international law.

Frameworks can support the planning, preparation, and execution of cyberspace operations. Frameworks can also support battle damage assessment and the measurement of policies for OCO and Cyber-ISR. It is essential to have frameworks to measure success in the mentioned areas. Hence, it is crucial to continuously feed new knowledge into the frameworks through a cybernetic feedback loop and update them accordingly.

Diplomatic Dialogue ensures that communication between states' occurs at all levels, from peace to crisis and un-peace. States have realized they can avoid mentioning war because they can achieve impact through cyberspace and hybrid means without declaring war. Declaring war is problematic as a lot of legal instruments are triggered.

5. Discussion

The answer to the research question, *What are offensive cyberspace operations for cyber security, and why now?* is that more empirical evidence exists on applying OCO for deterrence and cyber security. Cases like Operation Glowing Symphony presents how USCYBERCOM, with US policy support, a base on national and international law that is against terrorist organizations, with frameworks to plan, prepare and execute OCO targeting terrorist cyber-infrastructure, is an example of low-entry/low-risk OCO that generates much experience.

A model of maturity development to conduct offensive cyberspace operations for cyber security requires a combination of a deterrence strategy with a spoken component that states the use of OCO for cyber security; a policy where policy-makers feel comfortable and take the necessary political risk; an interpretation of international law which provides much leeway for OCO and Cyber-ISR; frameworks for planning, preparing and executing OCO and Cyber-ISR, but also frameworks that measure the policies. Diplomatic Dialogue is a back-channel to ensure communication between capitals. When states cross red lines, Diplomatic Dialogue enables Heads of State to discuss and lower tensions, just like in the Colonial Pipeline case.

References

Fischerkeller, M. P., & Harknett, R. J. (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis, 61*(3), 381–393. https://doi.org/10.1016/j.orbis.2017.05.003

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity, 5*(1), 1–15. https://doi.org/10.1093/cybsec/tyz008

Healey, J., & Jenkins, N. (2019). Rough-And-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. *International Conference on Cyber Conflict, CYCON, 2019-May*, 1–20. https://doi.org/10.23919/CYCON.2019.8756890

Huskaj, G. and Wilson, R. L. (2020). An anticipatory ethical analysis of offensive cyberspace operations. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020,* 512–520. https://doi.org/10.34190/ICCWS.20.054.

Kosseff, J. (2019). The Contours of "Defend Forward" under International Law. *International Conference on Cyber Conflict, CYCON, 2019-May*, 1–13. https://doi.org/10.23919/CYCON.2019.8757141

Lewis, J. A. (2018). *RETALIATION American perspectives on international cybersecurity*. 252–259.

Sebekin, S. (2020). Choosing between persistent engagement and deterrence in the American cybersecurity strategy. *Mezhdunarodnye Protsessy, 18*(3), 96–125. https://doi.org/10.17994/IT.2020.18.3.62.3