2

Active Cyber Defense and Operational Environment Preparation: An Opportunity for Progress

Zoë BRAMMER

Abstract: The prevalence of threats in the cyber domain have become increasingly evident, as signaled by the widespread adoption of military strategies aimed directly at information flows in a race to establish "cyber dominance". These strategies tend to be offensive in orientation, inefficient, and event-specific, causing them to rapidly become outdated. Due to the ever-changing nature of the cyber domain and the inability of a single state to dominate cyberspace, states should begin to adopt stronger defensive orientations in their quest for cybersecurity. This paper highlights two areas of cybersecurity–active cyber defense (ACD) and operational environment preparation (OEP)–that provide ample opportunity for cyber defense improvement. I then make three actionable recommendations, all of which address gaps in both ACD and cyber OEP that together will result in improved cybersecurity. In this way, improving cyber defense capabilities can be resource-efficient, sustainable, and effective.

Keywords: Cybersecurity, cyber defense, active cyber defense, cyber situational awareness, operational environment preparation

Introduction

The exponential speed at which the world has become more interconnected and interdependent is perhaps most directly evident in cyberspace. At the same time, threats originating from the cyber domain have accelerated in both number and sophistication. Such threats are transnational, highly contagious, and have the potential to completely halt the normal day-to-day operations of the international system, making them central to a state's security considerations. As a result, beginning in the first half of the 1990s, US strategic analyses "began to contain a growing number of warnings that national security was increasingly threatened by cyberattacks"[134], leading to the early formation of offensive strategies and doctrines aimed directly at information flows.

There is a fairly abundant body of literature on the emergence and containment of cyber threats, which can be boiled down into two main security considerations. First, many security scholars argue that a "major change in the security environment has occurred"[135]. This is because cyber threats are "increasingly difficult, if not impossible, to peel away from the process of globalization"[136], and the increasing availability of and dependence on computers and the internet across the world. As a result, cyber threats cannot be easily contained. Unlike many security threats that arise in the four traditional military domains (land, sea, air, space), cyber threats "transcend the capacity of a single nation-state to confront them adequately"[137]. Cybersecurity poses a new kind of security challenge to states across the globe and to the international community more broadly, and it requires the cooperation of the public, private, and international sectors.

---

[134] Myiam Dunn Cavelty. "The Politics of Cybersecurity: Balancing Different Roles of the State". *Center for Security Studies ETH Zurich*, 17 June 2019. css.ethz.ch/en/center/CSS-news/2019/06/the-politics-of-cybersecurity-balancing-different-roles-of-the-state-.html.

[135] Richard Sinnott. "Public Opinion and the New Security Environment". *European Union Institute for Security Studies (EUISS),* 1997. N.p.

[136] Paul Rexton Kan et. al. "Lawyers, Guns, and Money: Transnational Threats and U.S. National Security". *Strategic Studies Institute, US Army War College*, 2010. 207.

[137] Ibid.

The second security consideration is that cybersecurity has become deeply integrated into all traditional military security domains as the military becomes increasingly reliant on cyber capabilities and conducts more operations within the cyber domain. The US military's global communications backbone, for example, "consists of 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries"[138]. Over the past 10 years, the frequency and sophistication of intrusions into US military networks have increased exponentially[139], thereby threatening not only cyber operations but military operations in the traditional domains as well. As a result, cybersecurity is and will continue to be a central facet of military security more broadly.

Because the cyber domain exists mostly outside of the physical realm, cyber threats are unique in their propensity to move seamlessly between endangering "individual and collective security, between public authorities and private institutions, [and] between economic and political-military security"[140]. Consequently, it is key to state security to establish effective cyber defense and prepare for offensive cyber operations. Unfortunately, traditional security operations and a large portion of general security studies literature have little to say about how best to prepare for and respond to cyber threats.

To date, the majority of cybersecurity considerations have been offensive in orientation, with the ultimate aim of establishing "cyber dominance". The premise of achieving cyber dominance is defined as a state that "achieves and maintains strategic and tactical dominance in its critical elements of cyberspace"[141], but although a single state can own some of the computers and software in the cyber domain, it certainly cannot own

---

[138] William J. Lynn. "*Defending a New Domain: The Pentagon's Cyberstrategy".* Foreign Affairs 89, no. 5 2010. 98.

[139] Ibid., 100.

[140] Lene Hansen and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53, no. 4 (2009): 1155–175. Accessed August 6, 2020. www.jstor.org/stable/27735139. 1161.

[141] Martin R. Stytz., and Sheila B. Banks. "*Toward Attaining Cyber Dominance*". Strategic Studies Quarterly 8, no. 1. 2014. 55. www.jstor.org/stable/26270605.

a majority of them, and cyberspace itself, as a non-physical entity, cannot be owned by anyone. This is further complicated by the fact that the "vast majority"[142] of critical cyber infrastructure and key resources are owned by the private sector (85 percent in the US[143], for example). In most states, there is a limit to how much control the government is willing to exert over the private sector's decisions regarding cybersecurity. In the United States and the United Kingdom, for example, "the government regards privately owned and operated critical infrastructure as a key element of national security but is reluctant to claim a mandate to oversee network security. At the same time, the private sector is not inclined to accept responsibility or liability for national cyber security"[144]. Because of the hesitation on the part of government to mandate that the private sector adopt stricter security measures, there is a temptation for cybersecurity to become offensive in nature, with states encouraging the development of offensive cyber capabilities without creating effective cyber defense measures. An offensive cyber orientation is appealing because it may require less cooperation between the public and private sectors and can give an illusion of control.

Adopting an offensive orientation towards cybersecurity is problematic however, because actors in cyberspace are extremely difficult to identify, especially in the wake of a cyber-attack (this is known as the attribution problem). The legal framework surrounding cyber warfare also remains unclear, making a cybersecurity approach based around offensive operations and retaliation less than ideal. Although cybersecurity has become "critical to…military operations"[145], the way we approach cybersecurity needs to be reassessed and reoriented towards defense.

At a very basic level, *strategic* cyber defense should aim to prevent penetration of *tactical* cyber defenses. Strategic cyber defense encompasses "*how*

---

[142] Critical Infrastructure Sector Partnerships. 2019, April 23.

[143] Government Accountability Office, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, June 26, 2009. 1.

[144] Madeline Carr. "Public–private partnerships in national cyber-security strategies". *International Affairs*. 43. https://doi.org/10.1111/14682346.12504.

[145] William J. Lynn. "*Defending a New Domain: The Pentagon's Cyberstrategy".* 101.

an organization defends itself and its overall cybersecurity posture"[146], and includes considerations of operational capacity. Tactical cyber defense considers "*what* an organization needs to focus on when responding to incidents"[147], and includes a discussion of technical cyber capabilities. If a cyber-attack penetrates a network system, tactical cyber defense should prevent the attacker from determining the cyber terrain and prevent the attacker's malware from executing. In the event that malware does execute, strategic cyber defense should prevent the malware from accessing its target and/or communicating back to the attacker[148]. Due to the rapidly evolving nature of the cyber domain, creating sustainable and effective cyber defense systems addressing each of these goals is extremely difficult. This paper aims to identify areas of cyber defense that should be the primary focus in developing cybersecurity both within individual states and in the international community more broadly.

Establishing defensive cybersecurity is a massive undertaking, and it is crucial that the pursuit of cyber defense capabilities take into account the realities of the existing limited resource base and the importance of not exposing the network to unnecessary vulnerabilities through the use of too many defense channels within critical networks. This paper develops a functional lexiconic framework for cybersecurity, describes two facets of cyber defense (active cyber defense and operational environment preparation) and identifies areas in which multiple defensive improvements can be accomplished using a single resource set.

Definitions

No study of cybersecurity can be useful without first providing a functional lexiconic framework. Given the fairly recent rise of cybersecurity and the

---

[146] Cyber Stratego: Strategic vs. Tactical Threat Intelligence. *ThreatConnect: Intelligence-Driven Security Operations*. September, 2016. Retrieved August 20, 2020, from https://threatconnect.com/blog/strategic-vs-tactical-threat-intelligence/.

[147] ThreatConnect, "Cyber Stratego".

[148] Martin R. Stytz. et. al. "*Toward Attaining Cyber Dominance*". 64.

cyber domain, many of the accompanying terms are not clearly defined. This is a major hindrance in establishing cybersecurity because it prevents actors from working in concert. Without the strong base of a common lexiconic framework, it is difficult for actors to define issues, let alone work together to solve them. Effectiveness depends on establishing a common terminology for the domain, the actors within the domain, and the threats that come from combining the two. Thus, to achieve operational efficiency, the following definitions should be applied in the staging of active cyber defense and cyber operational environment preparation.

Cyber Relevant Time

Although this definition is slightly dated (originally published in 2014), Herring neatly sums up the vagaries associated with cyber relevant time. Cyber relevant time is a "purposely vague term that accommodates the needs of the battle space"[149]. If the battle space is between two computers of close physical proximity, for example, cyber relevant time is milliseconds to seconds. For a battlespace between two computers on opposite sides of the world via satellite links, cyber-relevant time is seconds. With live operators and delays inherent in cognitive processing, keystrokes, and mouse clicks, cyber relevant time is seconds to minutes[150]. The term simply implies that in different contexts, the speed at which systems operate is different, and the requirements for the speed of effective defense differs as well.

Traditional Military Domains

The four traditional military domains are sea, land, air, and space. They are considered traditional in that for the most part, definitions of security within these domains revolve around physical characteristics like geographical locations or physical equipment.

---

[149] MJ Herring and KD Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense". *Journal of Information Warfare* 13, no. 2 (2014): 46–55. Accessed July 31, 2020. www.jstor.org/stable/26487121.

[150] Ibid., 47.

Active Cyber Defense (ACD)

Active cyber defense is "a set of operating concepts that involve taking the initiative and engaging the adversary in some way"[151] including real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. Active cyber defense often refers to the conduction of operations in networks other than one's own, which sets it apart from passive cyber defense.

Cyber Situational Awareness

Cyber situational awareness has four main components; to know what should be, to track what is, to infer when the two do not match, and to do something about the differences[152]. The goal is to understand the terrain within which cyber operations take place, and to make "risk management decisions based on threats and vulnerabilities to data, applications, systems, and networks that have the highest likelihood of impacting mission assurance"[153].

Operational Environment

Traditionally, an operational environment is a composite of the "conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander"[154]. This usually refers to the weather, enemy, terrain triad (often referred to as W.E.T.). In the cyber domain, conditions, circumstances, and influence are quite different from those in the traditional military domains, but the concept still holds. The specifics of what the cyber operational environment looks like are detailed in a later section.

---

[151] Irving Lachow. *Report*. Center for a New American Security, 2013. 3, Accessed July 31, 2020. www.jstor.org/stable/resrep06088.

[152] Angela Horneman.*Situational Awareness for Cybersecurity*: An Introduction. 2019, September 09. Retrieved August 07, 2020, from https://insights.sei.cmu.edu/sei_blog/2019/09/situational-awareness-for-cybersecurity-an-introduction.html. N.p.

[153] Earl D. Matthews., Harold J. Arata, and Brian L. Hale. "*Cyber Situational Awareness*". The Cyber Defense Review 1, no. 1 2016. 40.

[154] TC 7-102. Operational Environment and Army Learning. 2014.

The Attribution Problem

The attribution problem describes the difficulties that arise when attempting to identify cyber actors, particularly in the wake of a cyber-attack. In short, "the architecture of cyberspace makes it difficult to clearly determine those initially responsible for a cyber-attack as well as to identify motivating factors"[155]. For example, even when it is possible to discover what servers were used for an attack, many states use proxies so it may be impossible to conclude that one specific state ordered the operation.

Active Cyber Defense (ACD)

Active cyber defense (hereafter ACD) focuses on the "integration and automation of services and mechanisms to execute response actions in cyber-relevant time"[156]. Although many definitions of ACD include measures taken outside a state's network, I will be focusing largely on intra-network defense with the ultimate goal of developing recommendations that can be adopted by individual states to better their defensive cybersecurity. Herring and Willett identify six functional aspects of ACD: sensing, sense making, decision making, acting, messaging and control, and mission management. Together, these six aspects provide a "capacity within cyber defense with the unique differentiator of providing situational awareness and response actions within cyber relevant time"[157]. This enables a cyber actor (be it a government, or an organization) to understand the network landscape of the cyber domain in which they are operating in order to create continually updated defenses. Although no state or organization has yet to master all six of these aspects, the key operational gaps are largely found in the area of messaging and control[158].

---

[155] Myriam Dunn Cavelty. *"The Militarization of Cyberspace: Why Less May Be Better".* International Conference on Cyber Conflict, 2012. 146.

[156] MJ Herring, et. al. *"Active Cyber Defense: A Vision for Real-Time Cyber Defense".* 46.

[157] Ibid., 50.

[158] Ibid., 49.

Messaging and control are also crucial to the foundation of ACD; situational awareness, which relies on the ability of a network to communicate within itself and create a system of automated sense-making and response, thereby increasing the capacity for automated response actions. Cyber situational awareness is the result of "a dynamic process of perceiving and comprehending events in an environment"[159] which enables reasonable projections of how the environment may change, and "predictions concerning future circumstances and outcomes"[160]. This ability for event and action projection within the cyber domain is unique to ACD and must be fostered in order to develop effective cyber defense.

Situational awareness is central to all military operations, but it is of particular relevance to ACD because it requires the ability to "understand mission dependencies and threat landscapes"[161] that are unique to the cyber domain and constantly changing. The networks within which the cyber domain operates change constantly, and as a result, cyber defense cannot simply consist of static and dated defense measures such as keeping computers within a network updated (although software and hardware updates are also important). The approach to cyber situational awareness must reflect the ever-changing domain it is attempting to analyze. For all of the abovementioned reasons, addressing the gaps in messaging and control should be a priority if the goal is to establish effective and sustainable cybersecurity.

These gaps are primary a result of a lack of integration, specifically the "lack of a standard communication medium to interconnect all ACD-related tools at cyber relevant speed and scale, interface for tool connection to the common communications medium, and the lack of a standard message set understandable and actionable by all connected tools"[162]. A lack of standardization across a single network can cause inefficiency, and sometimes even miscommunication. The cyber-realm is constantly

---

[159] Martin R. Stytz. et. al. "*Toward Attaining Cyber Dominance*". 61.

[160] Ibid.

[161] Earl D. Matthews., et. al. "*Cyber Situational Awareness*". 39–40.

[162] MJ Herring. "*Active Cyber Defense: A Vision for Real-Time Cyber Defense*". 49–50.

shifting, and this lack of efficiency is at the core of the work that needs to be done by individual states to establish real-time cyber situational awareness and effective ACD.

If this standardization problem can be remedied, all ACD-related tools will "have the ability to make each other aware of current activity…and to coordinate response actions"[163]. The result will be a system of ACD that is increasingly automated, which will not only save limited resources, but also boost the effectiveness of a defense-oriented cybersecurity. By allowing for "automated synthesis of…monitoring information from across your enterprise infrastructure, operational and intelligence processes, and applications"[164], ACD will be able to maintain cyber-relevant speed in its establishment of situational awareness, thereby improving cybersecurity more broadly. I am by no means suggesting that ACD become completely automated as the associated risks are too great. A fully automated defense system would remove the ability of a human to act as an intermediary for decision making. Such a system is at risk of massively miscalculating a threat, which could result either in escalating a relatively benign threat into a full-scale cyber conflict, or, alternatively, undercalculating the risk of a threat. That being said, the increasingly self-sufficient nature of aspects of ACD will allow for human analysts to focus their attention on sense- and decision-making instead of data synthetization and basic communication.

Operational Environmental Preparation (OEP)

Identifying the operational environment in the cyber domain is a complicated task. In traditional military domains, the main characteristics of the operational environment are the weather, the enemy, and the terrain. In the cyber domain, however, the enemy is often obscured (due to the attribution problem). Moreover, considerations of "weather" and "terrain" are necessarily different in a domain that does not always operate in the physical realm. To understand how to better prepare the operational

[163] Ibid., 49.

[164] Earl D. Matthews. et. al. "*Cyber Situational Awareness*". 40.

cyber environment, the concept of operational environmental preparation (hereafter OEP) can be adapted to the cyber domain by analyzing how the ideas of "weather" and "terrain" fit within that construct.

In the cyber domain, "weather" can be understood as patterns of user behavior, which affect the speed and efficiency of a network. Background traffic, for example, is considered "noise" from the standpoint of cyber operations, because it does not directly contribute to a mission and makes it more difficult to focus on a particular behavior[165]. Users "generate traffic in arbitrary manner, but one that still follows a pattern"[166], and as such, behavior can be understood in patterns that can be equated to weather in an abstract sense.

The "terrain" on which users operate in the cyber domain can be seen as the established cyber infrastructure, which includes but is not limited to computing systems, data storage systems, software in use, network policy, and access control rules[167, 168]. These elements are linked together by networks, which make up the cyber "terrain". The ability of the enemy to traverse cyber terrain can be assessed in the way actors are able to navigate the network. The combination of "weather" or behavioral patterns, and "terrain" or the layout of the cyber network together form the cyber OEP, within which all cyber operations occur.

The traditional understanding of OEP again assumes the inevitability of offensive operations. Cyber OEP, however, also possesses the ability to also enhance cyber defense. The concepts of behavioral patterns and network organization are intricately linked and can be used to prepare the cyber OEP for defensive operations. Understanding cyber "weather" and "terrain" allows for the creation of a matrix "linking an enemy's likely course of

---

[165] Antoine Lemay, Scott Knight and Jose Manuel Fernandez. "*Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace".* Journal of Information Warfare 13 no 3. 2014. 49.

[166] Antoine Lemay, et. al. "*Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace".* 49.

[167] William J. Lynn. "*Defending a New Domain: The Pentagon's Cyberstrategy"*. N.p.

[168] Martin R. Stytz. et. al. "*Toward Attaining Cyber Dominance*". N.p.

action, [and] indicators of those courses of action"[169]. By creating indicators that fingerprint an adversary's course of action, it is possible to determine the goal an enemy is pursuing, and even allow for network modification in order to force an enemy into a certain course of action–an extremely valuable ability in the quest to establish effective cyber defense[170].

In order to be able to create course of action indicators, it is essential to understand how an actor's behavior (weather) is affected by a given network (terrain). Real-time cybersecurity exercises "provide an ideal platform for studying adversary-defender interactions"[171]. These exercises can be used to better understand "human behavior, decision making, and adaptation"[172], and can help identify patterns that can be adapted into intrusion chain stages. Key moments of "decision-making, facing hurdles, and corresponding adaptations"[173] allow researchers to capture dynamic aspects of human behavior within the cyber domain, which becomes useful in creating a more robust and resilient operational environment. Although these exercises are not representative of reality given their isolated and controlled nature, they still allow for insights that can be hugely beneficial to establishing cyber OEP.

Acquiring a deep understanding of the cyber operating environment and the relationship between users and the environment should be the primary aim of cyber OEP. The better we are able to understand the cyber operational environment, the easier it will be to develop a course of action indicators, and thereby create stronger cyber defense capabilities. The result will be a transition away from an offensive cyber orientation and towards a defensive orientation, which will be more resource-efficient and sustainable.

---

[169] Antoine Lemay, et. al. "*Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace".* 55.

[170] Ibid.

[171] Geoffrey B. Dobson, Aunshul Rege, and Kathleen Carley. "*Informing Active Cyber Defense with Realistic Adversarial Behaviour*". Journal of Information Warfare 17, no. 2. 2018. 18.

[172] Ibid.

[173] Ibid.

Recommendations

Standardization

There is a pressing need for a common communication medium, standard interface tool, and standard message set in order to ensure that data flows are integrated "into a continuous monitoring platform"[174], thereby boosting network efficiency and heightening situational awareness. Achieving this standardization goal will require engaging governmental agencies, commercial vendors, industry leaders in security and technology research, as well as the appropriate usage of governing bodies, civil agencies, and the intelligence community.

If this standardization is successful, it will allow for data collection to be used more efficiently across cybersecurity priorities. This will enable ACD to be more efficient by allowing for inter-system communication and response, thereby furthering situational awareness. Additionally, this data can help improve cyber operational preparedness by compiling existing patterns of user behavior (weather) from within a network. Standardization can also aid in understanding the layout of cyber infrastructure (terrain) by increasing the efficiency of systems in their ability to understand the networks within which they operate. This will further the ability to predict potential changes in behavioral patterns and the network, thereby improving cyber operational preparedness.

More Cybersecurity Exercises

Executing more cybersecurity exercises and collecting information about how actors behave in the cyber domain is crucial to the pursuit of cyber OEP. These exercises allow for the creation of course of action indicators which can provide clues about an enemy's ultimate aims and enable preemptive defense operations. Cybersecurity exercises also provide an excellent opportunity to assess vulnerabilities in the cyber "terrain" and address them before they can be exploited.

---

[174] Earl D. Matthews. et. al. "*Cyber Situational Awareness*". 40.

Cybersecurity exercises also provide an opportunity to increase situational awareness and integrate ACD with other aspects of cybersecurity. ACD follows the principle of "collect once and reuse many"[175], which means that any data collected through cybersecurity exercises will be used and reused until it is outdated, making it a valuable defense resource. Within ACD there is a great "motivation to reuse…data in as many decision-making paths as is applicable"[176], which promotes smart and efficient workflow. The use of these exercises can increase network efficiency and expose areas of active defense that require further development.

Cyber Security Community

To establish a strong and sustainable defensive cybersecurity orientation, it is necessary to also establish a collective cybersecurity community in which data and best practices are shared. The cyber domain cannot be relegated to geographical boundaries, and as a result, it cannot be fully "owned" by any one state. With the introduction of a network of states, ACD has the ability to take action outside of a single state network, which allows for a host of additional active defense measures. The larger the network of resources in play, the better a given ACD will be, enabling the group to strengthen and prepare the cyber OEP in their own best interest. A cybersecurity community would provide an opportunity to address some of the most basic problems of cybersecurity, such as the creation of clear and cohesive definitions, system of laws surrounding cyber warfare, and addressing the attribution problem. In answering these basic questions, the ability of such a community to create a strong, sustainable defensive cyber operation will be optimized.

Conclusion

Today, there are still massive gaps in the ability of cybersecurity to protect state and organizational networks and adapt to threats in cyber relevant

[175] MJ Herring. et. al. "*Active Cyber Defense: A Vision for Real-Time Cyber Defense*". 48.

[176] Ibid., 49.

time. To create effective and sustainable cybersecurity, a defensive orientation must be adopted. This paper analyzed the most vulnerable areas of ACD and cyber OEP and identified three areas that provide an opportunity for resource overlap to make the pursuit of effective cybersecurity more efficient and less costly. In adopting these recommendations, the quest for effective and sustainable cyber defensive capabilities can be furthered by allowing for the best chance of cyber threat prevention through ACD while analyzing the behavioral patterns and network activity of potential cyber enemies through cyber OEP. The result will be an increasingly resilient, efficient, and sustainable cybersecurity.