Why Should the Brazilian Navy Create a Cyberspace Command?

Wagner Gonçalves Pereira

National Defense University

College of Information and Cyberspace

March 14, 2023

This paper or presentation is my work. Any assistance I received in its preparation is acknowledged within the document or presentation following an academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I cited the sources wholly and entirely in endnotes, footnotes, and bibliography entries. This includes sources that I have quoted or that I have paraphrased.

Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other course in this University or elsewhere or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer-reviewed journal, or professional conference. This is not a draft and is presented for grading to satisfy, in part, the requirements for this course.

In typing my name following the word "Signature," I intend this certification to have the same authority and authenticity as a document executed with my hand-written signature.

Signature: Wagner G. Pereira

Disclaimer: This paper represents the views and opinions of the author. This paper does not represent official NDU, DoD, or USG policy or position.

Introduction

The Brazilian Navy has acknowledged the relevance of cyberspace within the maritime operational domain by integrating cyberspace terrain into its operational plans. Consequently, the Brazilian Navy struggles with dilemmas such as balancing its ends, means, and ways in the cyberspace arena, namely how and where to hire professionals, where to deploy them according to their expertise, and how to build capabilities within cyberspace in accordance with the Brazilian Navy mission. Whereas the US government created specialized agencies to address cyberspace issues in several areas, such as critical maritime infrastructure and conventional warfare domains (air, sea, land), the Brazilian Navy has yet not decided to unify its cyberspace workforce under a command structure. Therefore, with the US approach in mind, whether the Brazilian Navy should activate the Navy Cyberspace Command arises as a research question.

However, that question does not have a simple answer. Experience in cyberspace shows the answer should be yes due to specific threats to any navy's fleet, such as attempts to introduce vulnerabilities into naval systems by intrusions in their supply chain. Even though it may seem a yes or no question, technical, tactical, operational, and particularly strategic reasons underscore a critical part of the decision-making process. Hence, this essay will excerpt conclusions from a refined research question. How would the Navy Cyberspace Command contribute to the Brazilian Navy's mission efficiency?

The research and the application of strategic thinking have shown that devising a specific naval cyberspace strategy is necessary to answer that question, owing to the intersection of cyberspace and maritime terrain. Another discovery was that activating the Navy Cyberspace Command is the most efficient form of organization for the existing cyberspace workforce. Thus,

striving to sway Brazilian Navy decision-makers to strategize before deciding, this article ponders cyberspace risks, ends, means, and ways from a surface warfare officer's perspective.

This work's relevance lies in elaborating specific strategies for each significant project within one company. In this sense, it is worth mentioning that the Brazilian Navy did not have a naval cyberspace strategy published at the submission date of this assignment. That discontinuity may weaken the Brazilian Navy's firepower in the future.[1] Consequently, the Brazilian Navy invests in its military's education to fill knowledge gaps, enabling them to think critically.[2] This way, the Brazilian Navy can obtain a "competitive advantage [that] depends on strategies made by people with knowledge in their field."[3]

As a result of that investment, this article argues that the Brazilian Navy should activate the Navy Cyberspace Command. This command should devise naval techniques, tactics, and procedures for the following purposes: to secure embarked cyberspace, to support the Brazilian Cyberspace Defense Command in protecting critical maritime infrastructure, and to enhance the current integrated deterrence strategy.

Methodology

This essay excerpts insights from cyberspace vulnerabilities specific to ships as those within engine control, combat, and C_2 systems, generically called *naval systems* in this essay, as narrowing boundaries for the research question. This work applies the National War College Strategic Logic[4] to appraise cyberspace warfare within the Brazilian Navy's present context, following Castex's and Lykke's strategy theories.[5] Furthermore, once the decision to activate the Navy Cyberspace Command is ultimately political in Brazil, the research exercises reverse deductions from what is understood to be better performed by a specialized agency underneath the Brazilian Navy's authority.

This approach absorbs concepts from a systematic review of strategies, books, and articles about other countries' cyberspace strategies, especially from the US National Defense University's College of Information and Cyberspace course of study. This essay contrasts the literature with the Brazilian Navy's Policy, Strategy, and Cyberspace Doctrine; the Brazilian Cyber Security Strategy; and personal experience. Further, it organizes those results in an analysis of the Brazilian Navy's strategic context, risks, ends, ways, means, a final assessment, a conclusion, and a suggestion for future research.

Lastly, this essay acknowledges that the 2023 US National Cybersecurity Strategy's[6] publication happened after the bibliographic research had been finished. However, there was enough time to read the new cyber strategy and conclude that it does not present any significant change or conceptual addition to the supporting ideas that would otherwise justify altering the answer to the research question.

The Strategic Context

This section will cover critical conditions affecting the Brazilian Navy's awareness of cyberspace warfare.[7] It will discuss the national documents, authority concerns, vital interests, and threats the Brazilian Navy should address in its cyberspace policy.

As an agency subordinate to the executive power, the Brazilian Navy must follow the president's guidance published in strategies. However, Brazil does not manage its elements of national power (diplomatic, informational, military, and economic) through a grand strategy like the US National Security Strategy.[8] It promotes informational power through a National Cyber Security Strategy and military through National Defense Strategy.[9] Moreover, the Brazilian Navy administers its military power through a Naval Strategy and informational through a Cyberspace Doctrine.[10] The latter is not the best document to galvanize the Brazilian Navy's

efforts in cyberspace because it does not drive the force toward specific military goals. The Brazilian Navy must balance its ends, means, and ways to reduce its risks, recognizing its limits.[11] It must rethink what means it needs, what ends cannot do with current means, how it intends to develop them, how it should organize them, and how the workforce will deploy capabilities. Considering these viewpoints is essential to validate resources and budget claims and to plan the hiring process.

Furthermore, since armed forces are in permanent competition in all domains, not having a cyberspace strategy is detrimental to leveraging the full potential of this terrain. The domain is currently the most contested, so a cyberspace strategy enables an advantage.[12] In cyberspace, peace is an exception once states, advanced persistent threats,[13] and cybercriminals constantly interact. Thus, the Brazilian Navy should plan a measurable and flexible Naval Cyberspace Doctrine because it will better organize and employ its resources under its policies and establish strategic ends based on the performance of the initial plan.[14] The time frame for publishing a new strategy may be between one and five years, as other armed forces have done, due to the evolving technology; techniques, tactics, and procedures; and threat actors.[15] By that token, this research will briefly discuss the sustainability, feasibility, and desirability of organizing the Brazilian Navy's means in one command and the suitability and acceptability of the ways that this command should operate in future sections.[16]

In that manner, it is necessary to identify cyberspace's strategic elements, ways, means, ends, and risks for the Brazilian Navy. Owing to the national strategies' interdependencies, strategists must delineate a clear path in sync with the aforementioned Brazilian documents.[17] That means strategic elements may become others in another strategy because of their dependencies.[18] So, while having a navy is a means to the maritime strategy and warships to the

naval strategy, the warships' naval systems carry vulnerabilities that become a risk to the naval cyberspace strategy, national cyberspace strategy, and national defense strategy. In other words, the Brazilian Navy must properly employ cyberspace means and ways to thwart threats to national defense ultimately. Following the Brazilian Navy's Cyberspace Doctrine, this research assumes cyberspace strategy's means as the workforce and its techniques, tactics, and procedures; information technology; vulnerability stockpile; access to intelligence; and organization.[19] The latter is tested in this essay since the Brazilian Navy preferred to decentralize its cyberspace infrastructure instead of following the US Navy's example.[20]

Similarly, however centralized and with a joint structure, the Brazilian Cyberspace Defense Command lacks the proper authority to protect critical infrastructures, which should also be a Brazilian Navy's concern. For instance, the Brazilian Cyberspace Defense Command's assessment team could not access and inspect the electronic voting machines' hardware components, firmware, and software during the 2022 election.[21] Even though the Brazilian Cyberspace Defense Command's technicians are highly qualified state agents, the Brazilian Superior Electoral Court did not delegate them the authority to perform inspections.[22] Moreover, when granted access to the storage rooms, the workforce could not perform dynamic tests, thwarting the success of the electronic voting machines' cybersecurity inspection process.[23] This defining moment in Brazilian politics indicates that national decision-makers still have difficulty understanding the concepts of threat, risk, and vulnerability in cyberspace and that an agency must require legal concession to operate in cyberspace from Congress. Whether the Brazilian Navy wants to integrate cyberspace operations in its fight capacity fully, it should be aware of authority requirements to increase its reach of influence.[24] Moreover, not having authority obstructs the work of non-dedicated agencies in Brazil; the official report on e-ballots security

demonstrates that. Therefore, the Brazilian Navy must devise a plan to acquire legal authorization to operate within the targets of interest's cyberspace.

By and large, the US faces the same types of vulnerabilities in its critical infrastructure. Thus, it decided to activate specialized agencies to address them, such as the Cybersecurity & Infrastructure Security Agency. That agency is responsible for guiding the US elections' security aspects and critical infrastructure protection, such as ships and ports.[25] Thus, the US Navy Cyberspace Command is not responsible for protecting the maritime sector; its operations are strictly military.[26] Notwithstanding, Brazil does not have an agency like the Cybersecurity & Infrastructure Security Agency. The Brazilian National Cyber Security Strategy defines strategic protection but does not attribute the responsibility for critical infrastructure protection to the armed forces because it is not a law.[27] Therefore, while the Brazilian Congress does not legislate whether Brazil should have a similar agency and the power to conduct cyberspace operations to protect critical maritime infrastructure, the Brazilian Navy should be able to respond to an emergency or war situation.

The reason is that the Brazilian Navy Commandant is the Brazilian Maritime Authority, and according to the National Defense Strategy, the Brazilian Cyberspace Defense Command is responsible for coordinating the Brazilian cyberspace defense. Brazil designed the Brazilian Cyberspace Defense Command as a joint agency to leverage the experiences of the three military branches, with particular attention to protecting critical infrastructures.[28] Further, the Brazilian National Cyber Security Strategy states guidance for cooperation and information exchange between existing regulatory agencies and private companies, such as the maritime transportation sector and the Maritime Authority.[29] The Brazilian Navy Commandant can regulate the maritime sector, which comprises a vital part of the transportation infrastructure. That authority enables

the Brazilian Navy to influence national economic power and defend it directly; nevertheless, it does not grant legal grounds to intervene in the critical maritime infrastructure's cyberspace. Even so, the Brazilian Navy should help the Brazilian Cyberspace Defense Command to coordinate the strategic protection described within the National Cyber Security Strategy because that command does not specialize its workforce in maritime targets. Therefore, the Brazilian Navy's cyberspace workforce must specialize in maritime systems to leverage them during conflicts through previously tested doctrines of operation to achieve the naval cyberspace strategy ends.

In addition, preparing to protect critical maritime infrastructure in cyberspace may also generate offensive abilities for the Brazilian Navy. The force must rethink its approach to the conditions expected within each of its cyberspaces.[30] Peace/tension and war are not a reality in cyberspace; the domain is constantly in conflict.[31] With that in mind, the Brazilian Navy's Cyberspace Naval Warfare System requires an organization revision.[32] Accordingly, the situation escalates from peace to war when the country identifies one nation-state targeting critical infrastructure.[33] Despite what the Brazilian Navy perceives, cyberspace is permanently in conflict because it is an interconnected terrain where states are in constant contact with the potential to influence or affect one another.[34] In cyberspace, criminals can be state-sponsored or operate independently. One cannot choose between peace or war merely because of a state's cyberspace attack. It is necessary to be able to attribute authorship to enable Brazil's self-defense right following an international standard. However, this presents an opportunity. Specializing in naval techniques, tactics, and procedures enhances the ability to conduct offensive cyberspace operations against maritime targets. That improves the Brazilian Navy's operational ability to conduct naval operations synchronized with cyber operations.

Convincing Brazilian decision-makers that there are threats in cyberspace without declaring war and stating enemies or adversaries is challenging, but not recognizing cyberspace threats increases the National Defense Strategy's risk.[35] Therefore, the Brazilian Navy should identify the strategic threats for its cyberspaces; likewise, the US's cyberspace strategies do.[36] Conversely, the Brazilian National Defense Policy and the National Defense Strategy do not point out nation-states as strategic threats. Clearly, they state the purpose of the Brazilian military as a force of deterrence against foreign aggression and security against transnational crimes.[37] Brazil differs from the United States of America in the hierarchy of its documents. The US Navy's Cyber Strategy[38] derives from the US Department of Defense's Strategy, which stems from the National Security Strategy, encompassing all overt national objectives and threats. In contrast, Brazil does not establish a National Security Strategy. Because there are no clear definitions of political ends and threats, there are gaps in understanding between the political and strategic levels. At the same time, despite having a Defense Strategy, the military lack concrete arguments to propose military actions or investments once there is a false perception of peace in cyberspace.

Nonetheless, it is optional to enumerate specific countries. Still, the Brazilian Navy should assume that other armed forces and criminal organizations are natural adversaries exploring its systems' cyberspace vulnerabilities for nefarious purposes. It should recognize that they are willing to and can exploit its vulnerabilities, further acknowledging "the effect of that would happen if they were able to take advantage of these vulnerabilities."[39] Moreover, as in Brazil, cyberspace warfare has been mainly a military concern; this field has also suffered with shortening of budget and low credibility to tackle cyberspace risks from other governmental spheres, such as electronic voting machines and the maritime sector.

Understanding this rupture of hierarchical documents, norms, and laws in Brazil is critical to enable the discussion of whether to activate the Navy Cyberspace Command. So far, the research highlights the need for developing a naval cyberspace strategy to improve the organization of the Brazilian Navy's workforce. Brazil should focus on one specialized agency with proper authority to conduct maritime defensive cyberspace operations. Nevertheless, while Congress does not deliberate on that matter, the Brazilian Navy should pay attention to it, preparing its workforce to address the maritime cyberspace vulnerabilities many threat actors continue to target. Further, it should leverage maritime vulnerabilities for offensive cyberspace operations purposes. In this regard, let us discuss what may cause the naval cyberspace strategy's catastrophic risk.

Critical Risk, Vulnerabilities, and Opportunities

Fundamentally, any research requires scope and limitations. A cyberspace strategy has many risks to tackle; thus, this section will dive into possible vulnerabilities in the maritime domain. These technical issues will keep the research focused on surface warfare vessels. The vulnerabilities addressed in this section will be the ones that result in the fleet's catastrophic risk of being unable to fight at sea due to a massive cyberspace attack on its naval systems.[40] Tactically, a ship without active naval systems is worthless. To mitigate that, the Navy Cyberspace Command would have to focus its defensive cyberspace operations' efforts because it is not feasible to defend every system simultaneously in cyberspace. The selected risk is a product of experience-based insights, objective analysis, and critical judgment to assess what the College of Information and Cyberspace studies have revealed about cyberspace's nature and dynamics for the Brazilian Navy's context.[41] On the other hand, naval risks unveil cyberspace opportunities for deploying offensive cyberspace operations.

In Brazil, discussions about threats can quickly flood into politics. Thus, this chapter will focus on the vulnerabilities that lead to the abovementioned warships' most critical risk due to their possibility of identification and exploitation.[42] For this research, vulnerability is a system imperfection that enables offensive cyberspace operations.[43] Risk is the imbalance among ends, ways, and means that can prevent a strategy from attaining political objectives [44] In other words, to mitigate risk and maintain the ends, strategists must access vulnerabilities and treat them by deploying prepared means in suitable ways for accomplishing the desired end state.[45] By this token, the objective of this section is neither to exhaust all vulnerabilities nor to point out naval systems' zero-days[46] but to create awareness once the accumulation of vulnerabilities or even one, if unidentified or untreated, can cause the selected catastrophic risk.

The Tamandaré frigate project exemplifies the Brazilian Navy's goal of building a modern fleet. Built-in modern naval systems with cyberspace technology acquired through a partnership with German companies, the Tamandaré frigate is the class of modern surface warships selected by the Brazilian Navy to modernize its fleet. This warship will feature an interconnectivity level the force has never previously had.[47] As a result, the Brazilian Navy has considered the value of having a proactive workforce with an agile decision-making process and a dynamic and autonomous structure to respond quickly to cyber actions.[48] Interconnected systems are a paradigm of cyberspace vulnerabilities. Previously, the Brazilian Navy's Fleet conducted naval operations with combat systems that could solely exchange information through radio links or voice and visual signals; however, modern naval warfare requires speed and real-time precision only obtained by an Internet connection. Moreover, with automatization comes the possibility of systems integration, such as engine control with combat operation and communication systems. Maritime transportation companies face the same trend by investing in

long-distance supervision. Some can remotely monitor and control ships' engine control systems to regulate fuel burn, cruise speed, and much more.

With integration, systems have become even more susceptible to offensive cyberspace operations, enabling enormous risk to both navies and the private maritime sector. Nonetheless, vulnerabilities reside in standalone systems, so the Brazilian Navy cannot rely on the myth of air-gapped naval systems.[49] Inversely to what the Brazilian Navy perceives, cyberspace warfare does not begin with the connection of a computerized system to the Internet; it starts with devising cyber resiliency performance parameters for the naval systems the force wants to acquire.[50] Operating disconnected from the Internet or in radio silence is insufficient to prevent a warship from being unable to fight at sea. Hence, the Brazilian Navy should devise means and ways to perform routine cyber security audits in the naval systems.

In that sense, increasing the knowledge about the diversity of vulnerabilities affecting a fleet is essential. Currently, the Brazilian Navy is more concerned about targets within the logic stratum considering the effect on or through cyberspace.[51] Nonetheless, electronic warfare vessels can also enable offensive cyberspace operations through the electromagnetic spectrum.[52] Another example of merging electronic warfare and cyberspace operations is the usage of Serial Advanced Technology Attachment cables as an antenna to deliver cyberspace attacks to air-gapped systems.[53] Cyberspace operations do not begin with network connections.[54] Conversely, they start during the design of the naval systems. Further, the Brazilian doctrine does not recognize that offensive cyberspace operations can occur through electromagnetic emissions, and not acknowledging this concept increases the probability of the Brazilian Navy's most critical risk. Worse, denying the fleet's systems access to the Internet increases the risk of being unable to fight at sea due to the need for real-time access to information in modern warfare.

Besides network-related vulnerabilities, the Brazilian Navy must be concerned about the hardware, firmware, and software, the basic information technology triad. Meltdown is one of the possible exploitation techniques of hardware failures of design, such as processors, that can unexpectedly provide intruders access to data.[55] In addition to the commonly known zero and one-day software vulnerabilities, firmware can also contain programming errors that allow hackers to perform unauthorized activities, such as making a system function improperly.[56] Adversaries can explore these vulnerabilities even when the system has no access to the Internet. The Stuxnet malware is an example of offensive cyberspace operations amongst several other air-gapped systems exfiltration methods found in the literature.[57] Two primary methods to mitigate those vulnerabilities are replacing the defective component or patching the operational system, firmware, and software. The former requires the force to have access to adequate hardware, and the latter reduces the processing time; in combat systems, it means a higher response time in combat. They require an efficient reaction against ammunition such as supersonic missiles. Consequently, the ships' and units' cyberspace workforces should conduct these measures preventively in a cyber security context.

Faults like those above are random, but adversaries can purposely design them to be exploited by electronic warfare techniques enhanced by cyberspace techniques, tactics, and procedures. Supplier nation-states designed the *chipping* technique to enable their military advantage over other countries.[58] In this case, chips may be installed on the motherboard to alter the behavior of naval systems for a specific purpose.[59] The chip's firmware interprets signals without interference with the operating system.[60] Therefore, the Brazilian Navy must carefully examine all computerized systems on foreign-developed ships before accepting them, as this type of hardware can be vulnerable to attacks through various means, such as the Internet or

electromagnetic emissions. Cyberspace auditors must perform penetration testing in all hardware components to identify all preinstalled backdoors. Vulnerability assessments must be frequent, not episodic, to prevent adversaries from creating new or discovering other backdoors.[61] Since the Brazilian Navy buys most of its warships from other countries, verifying how many compromised naval systems are currently in use is of utmost relevance. Further, the Tamandaré frigate class's naval systems must be certified by a specialized cyberspace workforce in a supply chain context.

While Brazil lacks the technical expertise to develop its surface warships, the Brazilian Navy's aim must be to acquire uncompromised naval systems from their development and ensure their resiliency during operations. The computerized nature of naval systems demands more secure development, including scrutinized certification before tests on live operations owing to the ongoing development of techniques, tactics, and procedures that may compromise the Brazilian Navy's mission.[62] Accordingly, the US Navy recognizes how crucial it is to control naval systems' development, assembly, delivery, and actualization processes and promote cyber awareness training.[63] Research and previous studies oriented this essay about how difficult it is to control a supply chain, especially within the technology industry.[64] One combat system can easily have the same motherboard as a home computer, where components are built and fixed in adversary countries. To prevent this, the US closely supervises the quality and line of production of combat components in the most highly secure companies in the country, such as S&K Technologies Inc.[65] Brazil's Defense Industrial Base is in development. Still, the Brazilian Navy will most likely receive compromised naval systems from the German-Brazilian frigate consortium. Therefore, the Brazilian Navy should organize its means to regulate, control, and inspect acquisition processes. The cyberspace workforce must

have expertise in and access to source codes, firmware, software, and hardware to conduct defensive cyberspace operations during naval operations at sea to increase the fleet's resilience.

Maritime critical infrastructure also contains vulnerabilities that may prevent the fleet from being unable to fight at sea. An enemy's offensive cyberspace operation against a port infrastructure, such as a crane, may prevent merchant ships from being converted to transport military gear from unmooring.[66] Further, a cyber-attack against an engine control system may redirect a merchant ship toward a warship, naval base, or bridge, preventing warships from setting sail. Those operations are feasible and already practiced in wargames at the College of Information and Cyberspace and the Brazilian Naval War College.[67] Nevertheless, Brazil is ill-equipped, underfunded, and lacks concrete standards to address the maritime sector like any other country.[68] In addition, it needs an agency such as the Cybersecurity & Infrastructure Security Agency to regulate, supervise, and protect critical maritime infrastructure.[69] For those reasons, the Brazilian Navy should have an organization expert in vulnerabilities within the maritime domain of military operations to protect the Brazilian maritime critical infrastructure and attack adversaries in wartime.

The complexity level of those vulnerabilities and the sophistication of the techniques, tactics, and procedures devised to exploit them require a more dedicated approach than the Brazilian Navy's Cyberspace Naval Warfare System's current organization can offer. By knowing the Brazilian Navy's vulnerability exposure and, by comparison, the adversaries', the cyberspace workforce can fiercely attack and defend the fleet from enemies.[70] By and large, enemies have the same vulnerabilities as the Brazilian Navy in cyberspace. So, at this point, the research could identify the principal vulnerabilities that ships may have by selecting the catastrophic risk of being unable to fight at sea. Critical thinking also revealed offensive

opportunities for the force. By this token, it is safe to assume that the Brazilian Navy has enough reasons to consider a different organization geared towards cyber resiliency and offensive cyberspace operations. The Brazilian Navy should designate personnel on board warships and at bases responsible for cybersecurity. At the same time, the Navy Cyberspace Command should be responsible for cyber resiliency during operations. This agency should specialize in maritime domain vulnerabilities to conduct defensive and offensive cyberspace operations. It should supervise naval systems' acquisition processes, supply chain, and the proper functioning of their components and applications to increase their resiliency in naval operations. Besides technical and tactical aspects of cyberspace, the Navy Cyberspace Command should devise, revise, adapt, and propose the naval cyberspace strategy to the Brazilian Navy's General Staff due to cyberspace warfare's ubiquitous and evolving character.

Discussing Ends

This section will discuss another critical research limiting factor, the Brazilian Navy's desired ends in cyberspace. Decision-makers should consider the ends by comparing them with the existing means and ways.[71] Thus, the Brazilian national documents' technological aims guide this research toward a possible desired end of a naval cyberspace strategy.

Previous research produced two initial objectives: to oppose the fleet's catastrophic risk and to increase the fleet's lethality through resiliency and offensive principles of war.[72] These objectives align with the freedom of maneuver, initiative, and preventing adversarial dominance, priority principles of war in the US Cyberspace Strategy.[73] Following these pillars, The US established its strategic ends of "having a deadlier force, including cyberspace operations into the integrated deterrence and fostering personnel's capacity,"[74] which align with the Brazilian Navy's aspirations.

Regardless of whether the Brazilian political goals are like those of the US, the Brazilian Navy should consider organizing its means in a similar manner. The Brazilian Navy's leadership considered the future of naval warfare and potential outcomes to ensure that the future fleet shall have technologically advanced means and systems for carrying out naval and cyberspace warfare.[75] That objective means that the force shall be more efficient in destroying targets through conventional naval and cyberspace warfare. However, they did not fully anticipate integrating cyberspace into naval operations by reappraising their cyber means in accordance with the cyber ends.[76] Cyberspace operations must aim at military and critical infrastructure targets to deploy the maximum firepower against an enemy.[77] In other words, it is necessary to foster personnel capacity and have a specialized workforce in a dedicated command to deal with critical maritime infrastructure and naval vessels in cyberspace.

Once cyberspace becomes permeable to the maritime domain, the activation of the Navy Cyberspace Command follows the same logic as the existing fighting commands. In other words, the Navy Cyberspace Command may be as important to the naval strategy as the Air and Naval Force, Submarine Force, Fleet's Marines Force, and Surface Force since cyberspace is an emerging fighting domain that enhances the fleet's resiliency and offensiveness. Therefore, the Navy Cyberspace Command should pursue the ends: *maintaining the ability to fight at sea and exploring cyberspace operations against adversaries to increase Brazilian deterrence*. Most importantly, the Navy Cyberspace Command should be responsible for achieving this end and revising its ways.

Assessing Possible Ways

Besides technical or tactical nuances, whether to activate the Navy Cyberspace Command relies on operational and strategic ways. This section will discuss the vogue operational ways in

the US; nevertheless, it will dive deeper into cyberspace theories, namely cyber security, resiliency, deterrence, coercion, espionage, persistence, and narrative, to assess the fourth element of strategic logic, strategic ways.[78] Accordingly, the research will consider the most suitable strategic ways for the Brazilian Navy to conduct cyberspace operations within its strategy.[79]

Operationally, research shows that cyberspace operations require long-standing operations. Regarding operations, the US Cyber Command has deployed campaigns for at least three years because, as a constrained actor, it requires long planning and well-elaborated intelligence operations to achieve its strategic goals of coercion and deterrence through persistent engagement. [80] The US National Defense University's College of Information and Cyberspace and academia have echoed this operation methodology as the most effective to conduct cyberspace operations and deliver results, such as intelligence collection and destruction in the physical world.[81] The most significant difference between the Brazilian Navy's understanding of cyberspace operations and campaigns is that Brazilian offensive and defensive cyberspace operations teams operate as one to practice and conduct operations in sporadic cases. Instead, the Brazilian Navy should consider the benefits and the inevitability of maintaining a mixed and integrated workforce that can exchange experience through constant engagement and coordinate operations to achieve long-term payoffs.

Strategically and regarding defensive cyberspace operations, the Navy Cyberspace Command should not focus on cyber security; instead, it would provide guidance and basic defensive techniques, tactics, and procedures training to local teams. The Brazilian Navy's Cyberspace Doctrine does an excellent job of considering information security but is very limited in its focus on the resiliency of naval systems.[82] Unless a cyberspace attack against the

Brazilian Navy's information technology resources poses the risk of bottling up the fleet, occurrences on the intranet, for example, should not be of significant concern to the Navy Cyberspace Command.[83] The US military branches follow the same principle by leaving the cyber security responsibility to the units.[84] In that vein, the Brazilian Navy does not have to change the authorities of its departments if it decides to activate the Navy Cyberspace Command. Units would still perform cyber security under the Brazilian Navy's Department of Information Technology and Communications guidance. At the same time, the Navy Cyberspace Command would oversee local teams training on the basic techniques, tactics, and procedures to defend their units and revise the Brazilian Navy's Department of Information Technology and Communications' best practices for security.

Moreover, the Navy Cyberspace Command should increase the fleet's resiliency by providing essential information technology patching and protection against acute attacks. The Brazilian Navy's leaders agree that resilience is a critical part of deterrence the same way as the US; notwithstanding, they delegate to the Brazilian Navy's General Directorate for the Navy's Nuclear and Technological Development the task of developing cyberspace protection methods of naval systems.[85] Still, experience shows that the Brazilian Navy's General Directorate for the Navy's Nuclear and Technological Development does not focus its expertise in cyberspace, does not educate its engineers in cyberspace warfare, and does not play a role in the three basic cyberspace tasks the doctrine defines: protection, exploitation, and attack.[86] For this reason, the cyberspace workforce should be responsible for conducting research and development in cyberspace. The Navy Cyberspace Command would be responsible for developing and implementing security patching for naval systems and protecting them while the fleet is deployed in operations to improve its cyber resilience.

Besides resiliency, the Brazilian Navy should develop a solid offensive cyberspace operation capability to increase its fleet's firepower and, ultimately, Brazilian strategic deterrence. The Brazilian Navy shall increase its contribution to deterrence with the Tamandaré class warships; nevertheless, the future Navy must be able to impose costs through offensive cyberspace operations.[87] Cyberspace poses a significant role in deterrence by delivering direct costs through offensive cyberspace operations or combining them with other diplomatic, informational, military, and economic actions. However, for an adversary to consider the Brazilian Navy's cyberspace capabilities as a deterrent in its decision matrix, the cyberspace strategy must define and overtly communicate a clear line that adversaries should not cross and the consequences for crossing it. [88] In addition, discussions in the US National Defense University's College of Information and Cyberspace's seminar classes clarify that cyberspace operations alone cannot deter conventional, kinetic attacks. Still, a reliable capacity increases integrated deterrence. Therefore, the Navy Cyberspace Command, by mastering offensive cyberspace operations, would increase the fleet's deterrence capabilities.

Concerning offensive cyberspace operations, destruction-aimed cyberspace attacks are fundamental to increase the fleet's lethality and coerce adversaries, even though Brazil has no intention of attacking them. Also called *degradation attacks*, they require a centralized structure because of their complexity, high cost, and probability of failure for unforeseen reasons; most importantly, past occurrences demonstrate that their use can indicate a reluctance to start a war.[89] It is crucial to master offensive techniques, tactics, and procedures and have a stockpile of vulnerabilities related to the target and presence within the adversary's systems to enable destruction-aimed cyberspace attacks. Meaning that maritime targets should be the Navy Cyberspace Command's emphasis once it is not the Brazilian Cyberspace Defense Command's.

Further, offensive cyberspace operations are critical in naval operations, thus requiring the same planning, logistics, and synchronization during the operational design methodology. Therefore, the Navy Cyberspace Command would conduct offensive research and development to access backdoors; exploit maritime vulnerabilities; practice naval techniques, tactics, and procedures; and protect the Brazilian Navy's stockpile of vulnerabilities for each target within each previously planned operation.

Furthermore, whether the Brazilian Navy wants to integrate offensive cyberspace operations capabilities fully, it must prioritize espionage operations to build a databank of vulnerabilities, be present in the adversaries' systems, and create tools, such as exploits, to disable maritime targets. While it is not the Brazilian *modus operandi* to proliferate information through espionage, the Brazilian Navy's leadership recognizes that exploitation is necessary to fully leverage cyberspace operations like the US states in its cyber strategy.[90] Cyberspace operations require previous planning, logistics, and specific research and development for each target to consider the probability of success, side effects, and the utility of the offensive cyberspace operations for a pre-planned operation.[91] Exploitation operations demand more coordination than currently observed in the Brazilian Navy's Cyberspace Naval Warfare System. Poorly conducted espionage can result in negative consequences, such as becoming a target of the adversary's offensive cyberspace operations in retaliation or facing political repercussions. Accordingly, defensive and offensive teams must continuously develop and update cyberspace capabilities under the same authority and coordinated control. The Navy Cyberspace Command would identify maritime targets of interest for each pre-planned operation and perform research and development to access their backdoors and remain within their systems. In that manner, the

Brazilian Navy should centralize its investments and coordinate the employment of explorers, protectors, and attackers in campaigns to reduce cyberspace operations risks.

In the clashing domain of cyberspace, the Brazilian Navy should consider the requirements and implications of a persistent engagement. At least since 2018, the US cyber agencies have been persistently operating to disrupt threats preemptively and ensure strategic advantage against adversary states.[92] Persistent engagement is a requirement, not a choice, to increase cyber security and enable leveraging targets' vulnerabilities through constant contact in campaigns.[93] Further, strategically, it is the most suitable and acceptable way to achieve the ends due to the complexity of conducting cyberspace operations, their variables, and research and development requirements.[94] That is because cyber persistence encompasses increasing integrated deterrence by improving cyber security, resiliency, espionage, and coercion capacities, particularly with regard to lethality enhancement. Persistent engagement is the requirement for offensive cyberspace operations due to the possibility of losing access to an adversary's system for unbeknown reasons. In other words, offensive cyberspace operations must be continuously and actively maintained to be effective. Backdoors may be closed outside anyone's control, such as by an operational system automatic update. This tactical concern influences the strategic decision of activating the Navy Cyberspace Command to sustain real-time control of backdoors for offensive purposes on any given day. On the other hand, constant contact increases the probability of targets' reactions and political repercussions.

Moreover, the Brazilian Navy's cyberspace strategy should encompass cyber persistence to enable the workforce to compete and contest adversaries globally, continuously, and at scale, engaging more effectively against advanced persistent threats and occult adversaries. A cyber force is crucial to ensuring the Brazilian Navy's resiliency and military superiority while

adversaries operate continuously against the Brazilian Navy's Naval Systems in search of strategic advantage. Hence, having a specialized, dedicated agency with proper authority is crucial to allay the impact of potential outcomes and ensure that an offensive cyberspace operation is effective and consistent.

It is necessary to devise a narrative to show Brazilian authorities the relevance of having a specialized agency in maritime cyberspace operations. A narrative does not serve only for information warfare purposes within or outside a war scenario; it should delineate the strategy the Brazilian Navy will require to operate in cyberspace.[95] A narrative resembles the Brazilian Navy's doctrinal concept of mission. In this sense, the Navy Cyberspace Command's mission must convey precise arguments for decision-making, signal the Brazilian Navy's resolve and ability to destroy adversaries' assets, and guide the cyberspace workforce's preparedness. Therefore, the proposed narrative is: *The Navy Cyberspace Command will increase the Brazilian Navy's fleet lethality by persistently conducting the full spectrum of cyberspace operations, support the Brazilian Cyberspace Defense Command by protecting critical maritime infrastructures, and contribute to Brazilian integrated deterrence.*

The study and refinement of cyberspace strategy hinge on the knowledge of tactical and technical nuances available only to the cyberspace workforce. Once cyberspace operations are classified, the Navy Cyberspace Command is the most suitable agency to concentrate experiences, conduct proof of concepts, and test theories.[96] Granting the Navy Cyberspace Command the authority to engage in persistent cyberspace operations is the most acceptable way to enable the Brazilian Navy to conduct such operations and maintain naval combat capabilities during wartime. Further, this allows the Navy Cyberspace Command to continuously improve and evolve its strategies and tactics in cyberspace operations. Activating the Navy Cyberspace

Command also requires reasons concerning the current means and aspects that suggest another organization of the Brazilian Navy's Cyberspace Naval Warfare System.

Identifying Means

This section will support the research thesis by covering a significant part of the research scope: the existing Brazilian Navy means and how they should be organized in comparison to the strategies employed by other countries in cyberspace warfare. By examining these topics, this section will provide insight into the strengths and weaknesses of the Brazilian Navy's current approach and identify potential areas for improvement. So, it is relevant to consider the intersection of the informational and military instruments of national power regarding cyberspace at the strategic level.[97] The means should operate in both instruments of power, namely through cyberspace operations to increase the military's power, conduct intelligence gathering, and deploy information campaigns.

First and foremost, cyberspace operations may be conducted within international terrain, willingly or not. Brazil is a constrained actor bounded by non-interventionism in its international relations policy.[98] So, to conduct cyberspace operations, the Brazilian Navy needs authority to allay international repercussions when its workforce operates within international terrain. It is common for a cyberspace workforce to realize that it is operating within another country's system only after successfully penetrating it. By that token, the Brazilian Congress should concede the authority to conduct cyberspace operations regarding critical maritime infrastructure, persistent engagement for forward defense, intelligence gathering, and military power enhancement to the Brazilian Navy. When considering integrating the full spectrum of cyberspace operations with the conventional naval force, leaders must be aware of this issue. Most importantly, even the current Brazilian Navy's Cyberspace Naval Warfare System's

organization demands authority to conduct offensive cyberspace operations, namely by the Brazilian Navy's Naval Command of Special Operations and the Brazilian Navy's Intelligence Center.

Building cyberspace capability is the most complex process the Navy Cyberspace Command shall accomplish because it requires computer science, operations, strategy, and political knowledge. Whether the Navy Cyberspace Command will be activated or not, the Brazilian Navy should entrust artifact crafting entirely to one of its cyberspace workforces instead of the Brazilian Navy's General Directorate for the Navy's Nuclear and Technological Development, as the current doctrine determines.[99] A fully integrated cyberspace capability depends on more than developing exploits and tools tailored for specific missions that do not follow industry standards.[100] It requires persistent engagement against targets of interest and presence within adversaries' systems. Cyberspace capability also requires integrating people, infrastructure, and organization and developing techniques, tactics, and procedures to degrade the target systems, gather intelligence, mitigate outcomes, and match different types of operations with political goals.[101] Additionally, expertise in attribution, or identifying the source of a cyberspace attack, is crucial to hold parties accountable for their actions in cyberspace effectively.[102] The Brazilian Navy's General Staff's education section has observed that the Brazilian Navy's General Directorate for the Navy's Nuclear and Technological Development does not invest in cyberspace courses since it is not the leading organization of cyberspace knowledge and does not participate in cyberspace operations. Building cyberspace capability demands a new leading organization of cyberspace knowledge comprised of experienced experts in defensive and offensive cyberspace operations; developing exploits and techniques, tactics, and procedures; and political and strategic nuances of cyberspace operations.

Moreover, the cyberspace workforce requires highly specialized personnel. A cyberspace command employs vulnerability analysts, developers, operators, system administrators, testers, frontline support, linguists, administrators, strategists, targeteers, remote personnel, consultants, and general staff, especially when it comes to critical maritime infrastructure cyberspace experts.[103] Targeting is essential for operational planning and demands strategic thinking, logistics, and intelligence deployed under the same authority and coordination. In that regard, the Brazilian Navy should consider a different approach regarding hiring. Since cyberspace operations do not require physical strength, the Brazilian Navy could broaden its hiring pool by considering civilians and individuals with disabilities of a wider range of ages. The Navy Cyberspace Command should also hire strategists, cyberspace lawyers, and operational planning specialists to transcribe technical and tactical nuances for the political leaders. They should amplify the awareness of and minimize collateral damage whereas connecting cyberspace operations to political ends.[104] Some of these professionals already exist in the Brazilian Navy but are spread throughout many units and departments. The Brazilian Navy's Department of Information Technology and Communications focuses on defensive cyberspace operations but does not practice cyberspace resiliency of naval systems. At the same time, the Brazilian Navy's Naval Command of Special Operations and the Brazilian Navy's Intelligence Center conduct attack and exploitation. Once all activities are integrated and aligned, their experts should collaborate to enable cyberspace campaigns.

The cyberspace capability also relies on logistics, procurement, and well-designed infrastructure. Offensive cyberspace operations create trade-offs, such as intelligence losses following an effective operation.[105] Because of that, the cyberspace warfare infrastructure must enable targeting, research and development, hardware engineering, software development,

analysis, and training.[106] Moreover, to mitigate losses and protect themselves, states do not reveal their cyberspace weapons and prevent private intelligence companies from selling weaponizable information the same way the US regulates semiconductor exportation.[107] Still, one can acquire cyberspace weapons by learning from failed offensive cyberspace operations, adversary's capability exploitation, leaking, talent recruitment, and the black market.[108] In that vein, senior leaders should acknowledge that the workforce needs to experiment, practice, research and development, and proof concepts to build cyberspace capability. So, they require anonymity when accessing the Internet; requisites such as layers of security and anonymity procedures that are not typical for a regular base or warship, such as private access to the Internet, IP masking techniques, and secret access places, even internationally. Thus, the Brazilian Navy's Naval Command of Special Operations and the Brazilian Navy's Intelligence Center may not have the best infrastructure to support offensive cyberspace operations.

Furthermore, offensive cyberspace operations may require access to multiple backdoors. Accordingly, the cyberspace workforce must create and secure their stockpile of vulnerabilities because buying them in the black market costs millions of dollars.[109] This prerequisite is decisive to accessing the adversary's system and enabling degradation attacks, meaning that it is mandatory to preposition the workforce within the target's system, which is not feasible without knowing the system's vulnerabilities.[110] The stockpile is a long-time building task that relies on cyberspace exploitations, research and development, intelligence, and contracts with private cyberspace intelligence companies, such as CrowdStrike. Thus, the Brazilian Navy requires a specific budget for cyberspace operations that might demand a leading executor agency, such as the Navy Cyberspace Command, to conduct cyberspace research, cyber weapons engineering, technology procurement, and cyberspace-wise logistics, such as maintaining intelligence assets

and the official Navy Cyberspace Command infrastructure or secret places of operation. Eventually, the Navy Cyberspace Command can better manage these requirements.

Activating the Navy Cyberspace Command may also be a question of posture concerning how the Brazilian Navy should operate in cyberspace. Once developing exploits takes little time, the job of defense teams becomes even more complex, compelling them to emphasize their efforts in controlling the impact of possible attacks rather than fixing vulnerabilities.[111] Experts' opinions merge on the compulsion of exceeding collaboration and coordination for, at the same time, conducting cyberspace campaigns, keeping discoveries secret, and sharing tools and techniques.[112] Under a defensive posture, specialists can work within the same structure or separately. Still, offensive and defensive cyberspace operations teams better share their discoveries when operating together. Notwithstanding, offensive posture requires excellent coordination to achieve results and mitigate backfire. Regarding training, the combination of experiences is already in trend in the Brazilian Army. The Brazilian Cyberspace Defense Command and other tactical units experiment with cyber weapons and techniques, tactics, and procedures in the Brazilian Army's cyberspace laboratory, enabling the exchange of knowledge and enhancing combined capabilities, which are key requirements for forming cyberspace campaign teams.

Cyberspace campaigns are long-standing, long-term payoff operations that require persistent engagement from dedicated cyberspace commands. The US Cyber Command and the Brazilian Cyberspace Defense Command similarly organize their workforce, working at the tactical, operational, and strategic decision levels, exchanging intelligence on a need-to-know basis, mastering the full spectrum of cyberspace operations, and taking advantage of everyone's abilities.[113] Under the same decision-making process, that managerial organization enables

campaigns encompassing massive intelligence gathering and extensive planning to employ techniques, tactics, and procedures and deploy proof-tested weapons that can be triggered when desired.[114] This concept assembles defense and offensive experts in synergy, enabling trust, experience leveling, and exchange of techniques, tactics, and procedures, ultimately increasing American systems' resilience and the lethality of the armed forces.

In addition, a cyberspace command can bring union between all workforce members regardless of their specialty, mitigating sentiments of over or less relative importance within cyberspace warfare campaign teams. It can also increase resiliency because all teams devise patching for proprietary and open code systems. The Navy Cyberspace Command could mitigate the excess of intelligence segregation; set training standards; reduce the impact of blowback once defensive teams are already in operation; and enhance offensive cyberspace operations' efficiency with defensive knowledge.[115] The Brazilian Navy's Cyberspace Naval Warfare System most likely cannot achieve this level of coordination once cyberspace operations are not under the same decision-making process and their budget is not centralized. Further, while the Brazilian Navy's General Directorate of Navy's Material can effectively provide cyber security to administrative systems, research shows that without better coordination, the Brazilian Navy could potentially undermine the resiliency of naval systems and limit the offensive capabilities of the fleet in cyberspace.

As previously discussed, the US has taken a specialized approach to cyberspace operations, with separate agencies responsible for different focus areas. By studying the US Navy's approach, it may be possible to gain insight into best practices for organizing and implementing a comprehensive cyberspace program. That force publicizes that it is fundamental to fully integrate the cyberspace commands' warfighting capabilities into the maritime warfare

domain for enhancing firepower. [116] Further, the US Navy employs its workforce under the cyber persistence theory to deliver warfighting effects, conducts information warfare, and collaborates in joint cyberspace operations.[117] The US Navy also acknowledges not being able to protect all systems, thus embedding cyber security techniques and enabling cyber protection teams to improve the resiliency of prioritized systems.[118]

Comparing the Brazilian Navy with the US Navy is logical, as the two navies have many similarities and may face similar challenges in the realm of cyberspace operations. By this approach, the US Navy incorporated means and security procedures, such as activating cyber commands and establishing zero-trust principles to increase the security and resiliency of its naval systems in ten years.[119] Further, with the Navy Cyber Forces and the Fleet Cyber Command, the US Navy extended the potential of cyberspace and information warfare.[120] That decision improved the cyberspace workforce's techniques, tactics, and procedures development; supply chain; and procurement.[121] Despite the enormous disparity in budget with the Brazilian Navy, the US navy also struggles to maximize results in all areas. To increase its firepower, it decided to treat cyberspace as a fighting command the same way the Brazilian Navy chose to organize air, surface, and submarine domains. So, on a smaller scale, the Brazilian Navy could activate the Navy Cyberspace Command at the same hierarchic level as the Brazilian Navy's Surface Force Command; however, the Brazilian Navy's Fleet's Command-in-Chief's hierarchical level would be adequate to encompass cyberspace operations in support of the amphibious force.

In the maritime domain, electronic and cyberspace warfare intersection demands more research and development from navies. The US Fleet Cyber Command envisions merging electronic warfare with cyberspace warfare.[122] This idea is coherent owing to the electronic

warfare aircraft performing offensive cyberspace operations via radio frequencies in the maritime domain.[123] Recognizing that research and development is a crucial step in moving from an idea to a fully realized technology or capability is essential, especially when it comes to electronic warfare and cyberspace techniques, tactics, and procedures. That may be the most effective form of leveraging cyberspace vulnerabilities at sea when a warship has no access to the Internet. Consequently, the Brazilian Navy should consider involving its Electronic Warfare Center in its Cyberspace Naval Warfare System, particularly for research and development in cyberspace and electronic warfare merging techniques. Another possibility is to merge the Brazilian Navy's Electronic Warfare Center with the Navy Cyberspace Command at the Brazilian Navy's Fleet's Command-in-Chief's hierarchical level.

Considering what has been exposed, the activation of the Navy Cyberspace Command is feasible because the Brazilian Navy already has the essential means; logistically, the initial assets need only rearrangement in another infrastructure.[124] The Navy Cyberspace Command is desirable once it is the most efficient means to fulfill the ends of maintaining the ability to fight at sea and exploring cyberspace operations against adversaries to increase Brazilian deterrence.[125] Lastly, the Navy Cyberspace Command is sustainable since it is the better means to achieve results in long-term payoff operations.[126]

Final Assessment

In order to fully address the research question, it was necessary to take a holistic approach that considered a range of factors and variables. Activating the Navy Cyberspace Command requires strategic justification once it is ultimately the operational means to achieve the strategic ends through selected ways of operation. It was necessary to review Brazilian policies and strategies and the Brazilian Navy's documents, comparing them with the US's

similar ones to find the most suitable answer regarding strategic thinking. Research indicates that the Brazilian Navy should organize its cyberspace capacity in a naval cyberspace strategy to accomplish the cyber ends of sustaining resilient warships' fighting ability and efficient offensive cyberspace operation ability. Those ends contrast the fleet's most critical risk, which is the inability to fight at sea due to a cyberattack on its naval systems. Similarly, the ability to perform cyberspace attacks on maritime targets derives from the force lethality requirements.

In addition, the naval cyberspace strategy intersects with the Brazilian Cyber Security Strategy in support of joint operations and strategic cybersecurity. Thus, the Navy Cyberspace Command should play a critical role in the national cyberspace strategy by supporting the Brazilian Cyberspace Defense Command in its responsibility to protect critical maritime infrastructure in wartime. Pre-planned operations require the branches' integration in joint operations where the Brazilian Cyberspace Defense Command is responsible for the cyberspace force at the operational and strategic levels. The Navy Cyberspace Command should dispatch teams to support that command and the maritime task forces to produce synchronized operational and tactical results.

Devising the ways to perform cyberspace operations hinge on strategic theories. That eventually requires understanding the operational terrain, situation awareness in the cyber domain, preconditions of operations, what to expect regarding the political implication of cyberspace operations, and overall objectives. This research suggests that a dedicated cyberspace workforce will better propose how to produce significant results for the Brazilian Navy. The main concepts, coercion, espionage, deterrence, persistence, and narrative, play an essential part in the decision process. All theories support how the Navy Cyberspace Command should operate to attain the Brazilian Navy's cyber ends by increasing the force's resiliency and firepower. That

avenue relies on research, development, and exploitation operations for intelligence gathering through a persistent posture. That should increase Brazilian military deterrence and readiness to operate under and with cyber influence. Therefore, the Brazilian Navy should create the Navy Cyberspace Command and publicize its cyberspace strategy. The Brazilian Navy should also endorse its decision by the following narrative: *The Navy Cyberspace Command will increase the Brazilian Navy's fleet lethality by persistently conducting the full spectrum of cyberspace operations, support the Brazilian Cyberspace Defense Command by protecting critical maritime infrastructures, and contribute to Brazilian deterrence.*

A cyberspace workforce is a research and development group by nature and thus must be focused on that because cyberspace operations require software patching capacity; offensive techniques, tactics, and procedures; and a stockpile of constantly shifting vulnerabilities. Regarding defensive operations, mastering naval systems' software, firmware, and hardware is a key requirement for the resilience teams to keep warships' fighting ability when underway. Naval systems demand routine cyber assessment to certify that they function only in the way they are supposed to. So, the Navy Cyberspace Command must have the logistics, training, technology, and capable personnel to perform tests, patch vulnerabilities, and maintain the systems functioning under cyberspace attacks. Regarding cybersecurity, technical teams on board warships and bases must ensure access to the Internet, intranet, proprietary applications, and operational system. Conversely, the Navy Cyberspace Command should be responsible for research and development, security requirements and policies, readiness alarms, patching development and distribution, and personnel reinforcements to tackle incidents capable of leaving the fleet stranded. In some cases, responding to a cyberspace incident may require using offensive operations, which may be outside the expertise of the information technology

professionals who are usually responsible for handling these issues. In such situations, it may be necessary to call on additional resources or specialized expertise to thwart the attacker and protect the fleet effectively. By working closely with the Navy Cyberspace Command and other specialized agencies, it is possible to access the necessary skills and knowledge to defend against and respond to cyber threats effectively. Similarly, the Navy Cyberspace Command defensive teams would be the most qualified personnel to deal with the backlash of failed offensive cyberspace operations.

Research and development become even more critical concerning offensive cyberspace operations because a cyberspace attack involves many variables, like technological intelligence; specific techniques, tactics, and procedures; a stockpile of vulnerabilities; and previous positioning of backdoors in the target's system. Persistence within one system is unpredictable. A cyberspace workforce cannot estimate the duration of an exploitation operation once it entails access through backdoors that can be closed anytime, with or without the target's knowledge. Exploitation is a key aspect of offensive cyber operations, as it involves gaining access to and establishing a presence within the target system to gather information and prepare for subsequent actions. Further, it requires a sophisticated set of techniques, tactics, and procedures; a deep understanding of the targeted system's vulnerabilities; and the workforce's ability to collaborate effectively. Undertaking operations with that complexity entails teams with specific schooling, dedication, research, training, and availability. Therefore, the Brazilian Navy should designate the Navy Cyberspace Command to oversee the cyberspace domain at the operational level.

Conclusion

This research concludes that it is of utter relevance to coalesce the Brazilian Navy's Electronic Warfare Center and the Brazilian Navy's Cyberspace Naval Warfare System's

cyberspace workforce into a unified command with proper authority, budget, and infrastructure. The Navy Cyberspace Command should conduct defensive cyberspace operations, protecting naval systems while the fleet is at sea to increase its cyberspace resiliency. Although, warships and units should have organic teams in charge of cyber security. Further, the Navy Cyberspace Command must have legal authorization to protect critical maritime infrastructure when needed and requested until the Brazilian Congress creates another agency for that purpose. Furthermore, the Brazilian Navy leadership must recognize that offensive cyberspace operations may require accessing systems outside the national territory, which demands political consent. Offensive cyberspace operations may involve obtaining the necessary legal approvals and working with other branches of the military and specialized agencies to develop and execute a plan of action. Lastly, activating the Naval Cyberspace Command is the most suitable, acceptable, feasible, desirable, and sustainable solution to enable the Brazilian Navy to operate in the full spectrum of cyberspace operations.

Directions for Future Research

The US currently discusses whether to unite cyberspace and information warfare in a unified command. As stated in the US Congressional Research Service reports, "Information Warfare Command may be able to remove operational stovepipes that exist between EMS [electromagnetic spectrum] and cyberspace operations, particularly as both cyberspace and the electromagnetic spectrum exist as dimensions of the information environment."[127] Therefore, the Brazilian Navy should consider researching how to integrate information warfare strategy into naval warfare. By investing in this research and development, the Brazilian Navy can enhance its capabilities in the realm of information warfare and better prepare itself to defend against and respond to cyber threats in the maritime domain.

Notes

[1] Mintzberg, Henry. "Crafting Strategy." Strategic Planning. Harward Business Review. July 1987. https://hbr.org/1987/07/crafting-strategy.

[2] Ibid.

[3] Ibid.

[4] Heffington, Steve. Oler, Adam. Tretler, David. "A National Security Strategy Primer". National Defense University Press. Washington, DC. 2021. p. 1-6.

[5] Wedin, Lars. "Maritime Strstegies for the 21st Century: The Contribution by Admiral Castex. Kindle's Edition. 2017.

Lykke Jr, Arthur F. "Defining Military Strategy". Military Review. May 1989. https://cgsc.contentdm.oclc.org/digital/api/collection/p124201coll1/id/504/download. Accessed on April 16, 2021.

[6] The US. "National Cybersecurity Strategy." March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[7] Heffington, Steve. Oler, Adam. Tretler, David. "A National Security Strategy Primer". National Defense University Press. Washington, DC. 2021. p. 7-14.

[8] Wedin, Lars. "Maritime Strstegies for the 21st Century: The Contribution by Admiral Castex. Kindle's Edition. 2017.

Biden Jr, Joseph R. "National Security Strategy." Washington DC, October 12, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[9] Brazil. "Estratégia Nacional de Segurança Cibernética". 2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm.

Brazil. "Política Nacional de Defesa e Estartégia Nacional de Defesa". 2016. https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf.

[10] Brazil. "Plano Estratégico da Marinha 2040." Marinha do Brasil. p. 51. https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/arquivo.pdf

Brazil. "Doutrina Cibernética da Marinha (EMA-419)". Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021.

[11] Freedman, Lawrence. "Strategy: A History". Oxford University Press. New York. 2013. p. 610.

[12] Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. "Cyber Strategy: The Evolving Character of Power and Coercion." Oxford University Press. New York. 2018. p. 31-32.

[13] Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. "Cyber Persistence Theory Redefining National Security in Cyberspace". Oxford University Press. New York. 2022. p. 59-60.

[14] Siegel, Carol A. Sweeney, Mark. "Cyber Strategy - Risk-Driven Security and Resiliency". Taylor & Francis Group. Florida. 2020. p. 86.

National Security Strategy Course. "Lesson 12, Plenary Class. Costs, Risks, and Strategy Assessments." November 21, 2022.

[15] Siegel, Carol A. Sweeney, Mark. "Cyber Strategy - Risk-Driven Security and Resiliency". Taylor & Francis Group. Florida. 2020. p. 9.

The US Fleet Cyber Command. "Strategic Plan 2020-2025". https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d.

[16] National Security Strategy Course. "Lesson 12, Required Reading. Evaluating Strategy - Adapted from the work of COL Greg Schultz, USA, NWC Faculty, original work." August 22, 2012. Available on Blackboard.

[17] Wedin, Lars. "Maritime Strstegies for the 21st Century: The Contribution by Admiral Castex. Kindle's Edition. 2017.

[18] Lykke Jr, Arthur F. "Defining Military Strategy". Military Review. May 1989. https://cgsc.contentdm.oclc.org/digital/api/collection/p124201coll1/id/504/download. Accessed on April 16, 2021.

[19] Brazil. "Doutrina Cibernética da Marinha (EMA-419)". Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. Charter 1. p. 2-2 and B-3.

Fanelli, R. "On the Role of Malware Analysis for Technical Intelligence in Active Cyber Defense." Journal of Information Warfare 14, no. 2 (2015): 69–81. https://www.jstor.org/stable/26487495.

[20] Brazil. "Doutrina Cibernética da Marinha (EMA-419)". Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-11.

The US Navy. "U.S. Fleet Cyber Command/U.S. TENTH Fleet." Webpage. Accessed on December 17, 2022. https://www.fcc.navy.mil/

[21] The Brazilian Ministry of Defense. "Ofício 29126/GM-MD - Fiscalização do Sistema Eletrônico de Votação." Brasília. Novembro 9, 2022.

[22] Ibid.

[23] Ibid.

[24] Cyberlaw Course. "Plenary and Seminar Discussions." October 2022.

[25] "Election Infrastructure Cyber Risk Assessment." Cybersecurity and Infrastructure Security Agency. July 28, 2020. p. 9. https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf

The US Department of Homeland Security. "Assessments: Cyber Resilience Review." Cybersecurity & Infrastructure Security Agency's Webpage. Accessed on November 14, 2022. https://www.cisa.gov/uscert/resources/assessments.

Fundaments of the Information Environment Course. "Seminar Discussions." October 2022.

[26] The US Navy. "U.S. Fleet Cyber Command/U.S. TENTH Fleet." Webpage. Accessed on December 17, 2022. https://www.fcc.navy.mil/

[27] Brazil. "Estratégia Nacional de Segurança Cibernética." Decree 10.222. February 5, 2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm

[28] Brazil. "Política e Estratégia Nacional de Defesa." October 31, 2022. p. 61. https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf

[29] Brazil. "Estratégia Nacional de Segurança Cibernética." Decree 10.222. February 5, 2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm

[30] Brazil. "Doutrina Cibernética da Marinha (EMA-419)". Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-10 – 1-12.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. "Cyber Persistence Theory Redefining National Security in Cyberspace". Oxford University Press. New York. 2022. p. 30

[35] Lykke Jr, Arthur F. "Defining Military Strategy". Military Review. May 1989. https://cgsc.contentdm.oclc.org/digital/api/collection/p124201coll1/id/504/download. Accessed on April 16, 2021.

[36] Singer, Peter W. Friedman, Allan. "Cybersecurity: What everyone needs to know". Oxford University Press. New York. 2014. p. 138.

The US Department of Defense. "Cyber Strategy". 2018. p. 1. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[37] Brazil. "Política Nacional de Defesa e Estartégia Nacional de Defesa". 2016. https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf.

[38] The US Fleet Cyber Command. “Strategic Plan 2020-2025”. https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d.

[39] Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 148.

[40] Pereira, Wagner G. “What should a senior naval leader be concerned about regarding indicators in cyberspace warfare?” Fundaments of the Information Environment End-of-Course Paper. December 16, 2022.

Hubbard, Douglas W. “The failure of risk management: why it's broken and how to fix it.” John Wiley & Sons, Inc. 2nd ed. New Jersey. 2020. Chapter 1.

Siegel, Carol A. Sweeney, Mark. “Cyber Strategy - Risk-Driven Security and Resiliency”. Taylor & Francis Group. Florida. 2020. p. 86.

[41] Heffington, Steve. Oler, Adam. Tretler, David. “A National Security Strategy Primer”. National Defense University Press. Washington, DC. 2021. p. 43-46.

[42] Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 148.

[43] Siegel, Carol A. Sweeney, Mark. “Cyber Strategy - Risk-Driven Security and Resiliency”. Taylor & Francis Group. Florida. 2020. p. 86-87.

[44] Lykke Jr, Arthur F. “Defining Military Strategy”. Military Review. May 1989. https://cgsc.contentdm.oclc.org/digital/api/collection/p124201coll1/id/504/download. Accessed on April 16, 2021.

[45] Siegel, Carol A. Sweeney, Mark. “Cyber Strategy - Risk-Driven Security and Resiliency”. Taylor & Francis Group. Florida. 2020. p. 92.

[46] Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 299.

[47] Brazil. “Política Naval.” Marinha do Brasil. https://www.marinha.mil.br/sites/default/files/politicanaval_site.zip

Brazil. “Plano Estratégico da Marinha 2040.” Marinha do Brasil. p. 51. https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/arquivo.pdf

Naval Technology. “Tamandare-Class Frigates, Brazil.” Webpage. July 19, 2021. https://www.naval-technology.com/projects/tamandare-class-frigates-brazil/

[48] Brazil. “Plano Estratégico da Marinha 2040.” Marinha do Brasil. p. 43. https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/arquivo.pdf

Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-12.

[49] Quinn T. “What Is a Standalone System?” ConnectPOS Webpage. February 15, 2022. https://www.connectpos.com/what-is-a-standalone-system/

Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 293.

[50] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 2-3.

Montgomery, Mark. Borghard, Erica. “Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence,” Joint Force Quarterly 102, 3rd Quarter. 2021, 79-89. p. 84. https://www.ndu.edu/Portals/68/Documents/jfq/jfq-102/jfq-102_79-89_Features-Cyber_Threats.pdf

[51] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 2-3.

[52] Pomerleau, Mark. “US military to blend electronic warfare with cyber capabilities.” C4ISRNET. April 14, 2021. https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/

The US Congressional Research Service. “Convergence of Cyberspace Operations and Electronic Warfare”. In Focus. August 13, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11292.

[53] Lakshmanan, Ravie. “New Air-Gap Attack Uses SATA Cable as an Antenna to Transfer Radio Signals”. The Hacker News. July 19, 2022. https://thehackernews.com/2022/07/new-air-gap-attack-uses-sata-cable-as.html.

[54] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-6.

[55] Moritz Lipp et al., “Meltdown: Reading Kernel Memory from User Space,” in 27th USENIX Security Symposium (USENIX Security 18), 2018. https://meltdownattack.com/meltdown.pdf

[56] Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 42.

Dullien, Thomas F. “Weird machines, exploitability, and provable unexploitability”. IEEE Transactions on Emerging Topics in Computing, December 19, 2017. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8226852

[57] Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 63.

Vigliarolo, Brandon. “Smartphone gyroscopes threaten air-gapped systems, researcher finds Network interface card LEDs are a risk too by blinking in Morse code”. The Register. August 23, 2022. https://www.theregister.com/2022/08/23/phone_gyroscopes_airgapped_systems/

[58] Clarke, Richard Alan. Knake, Robert K. “Cyber war”. Harper Collins e-books, 2014. P. 53. https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to

%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf

[59] Robertson, Jordan. Riley, Micha el. "China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies," Bloomberg. October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[60] Lee, Micah. Moltik, Henrik. "Everybody does it: The Messy Truth about Infiltrating Computer Supply Chains." The Intercept. January 24, 2019. https://theintercept.com/2019/01/24/computer-supply-chain-attacks/

Singer, Peter W. Friedman, Allan. "Cybersecurity: What everyone needs to know". Oxford University Press. New York. 2014. p. 42.

[61] Montgomery, Mark. Borghard, Erica. "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence," Joint Force Quarterly 102, 3rd Quarter. 2021, 79-89. p. 83. https://www.ndu.edu/Portals/68/Documents/jfq/jfq-102/jfq-102_79-89_Features-Cyber_Threats.pdf

[62] McQuade, J. Michael. Murray, Richard M. Louie, Gilman. Medin, Milo. Pahlka, Jennifer. Stephens, Trae. "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage." Defense Innovation Board. March 21, 2019. p. 4-12. https://media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF

[63] Ackerman, Robert K. "Navy Amasses Digital Armada." SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. "Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships." SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

[64] Singer, Peter W. Friedman, Allan. "Cybersecurity: What everyone needs to know". Oxford University Press. New York. 2014. p. 203-204.

[65] American Studies Foundations. "Montana Field Trip." July 22-28, 2022.

[66] Fundaments of the Information Enviroment Course. "Tabletop Exercise." December 6-13, 2022.

[67] Ibid.

[68] Trimble, Daniel. Monken, Jonathan. Sand, Alexander F. L. "A framework for cybersecurity assessments of critical port infrastructure." International Conference on Cyber Conflict (CyCon U.S.). 2017. p. 1. https://ndu.blackboard.com/bbcswebdav/pid-2048921-dt-content-rid-4098094_2/xid-4098094_2

[69] Ibid. p. 6.

[70] Sun Tzu. "The Art of War". Translated by Lionel Giles. Edited by Aggott Hönsch István. Pax Librorum Publishing House. 2009. p. 13.

[71] Heffington, Steve. Oler, Adam. Tretler, David. "A National Security Strategy Primer". National Defense University Press. Washington, DC. 2021. p. 15-17.

[72] Pereira, Wagner G. "What should a senior naval leader be concerned about regarding indicators in cyberspace warfare?" Fundaments of the Information Environment End-of-Course Paper. December 16, 2022.

[73] Singer, Peter W. Friedman, Allan. "Cybersecurity: What everyone needs to know". Oxford University Press. New York. 2014. p. 134-135.

[74] The US Department of Defense. "Cyber Strategy". 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[75] Freedman, Lawrence. "Strategy: A History". Oxford University Press. 2013. p. 611.

Brazil. "Política Naval." Marinha do Brasil. p. 34. https://www.marinha.mil.br/sites/default/files/politicanaval_site.zip

[76] Freedman, Lawrence. "Strategy: A History". Oxford University Press. 2013. p. 611.

Brazil. "Política Naval." Marinha do Brasil. p. 34. https://www.marinha.mil.br/sites/default/files/politicanaval_site.zip

[77] Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. "Cyber Strategy: The Evolving Character of Power and Coercion." Oxford University Press. New York. 2018. p. 70-72.

[78] Heffington, Steve. Oler, Adam. Tretler, David. "A National Security Strategy Primer." National Defense University Press. Washington, DC. 2021. p. 37-42.

[79] Freedman, Lawrence. "Strategy: A History." Oxford University Press. 2013. p. 622.

[80] Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. "Cyber Persistence Theory Redefining National Security in Cyberspace." Oxford University Press. New York. 2022. p. 101

Fundaments of the Information Environment Course. "Seminar Discussions." November 15, 2022.

Smeets, Max. "No Shortcuts. Why States Struggle to Develop a Military Cyber-Force" C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 160

[81] Fundaments of the Information Environment Course. "Seminar Discussions." 2022.

Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. "Cyber Persistence Theory Redefining National Security in Cyberspace". Oxford University Press. New York. 2022. p. 101

Smeets, Max. "No Shortcuts. Why States Struggle to Develop a Military Cyber-Force" C. Hurst & Co. (Publishers) Ltd. London. 2022.

Moore, Daniel. "Offensive Cyber Operations: Understanding Intangible Warfare." Oxford University Press, 2022.

[82] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021.

[83] Pereira, Wagner G. “What should a senior naval leader be concerned about regarding indicators in cyberspace warfare?” Fundaments of the Information Environment End-of-Course Paper. December 16, 2022.

[84] Fundaments of the Information Environment Course. “Seminar Discussions.” October 2022.

[85] The US Department of Defense. “National Defense Strategy 2022.” 2022. p. 8. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-5 and 5-3.

[86] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021.

[87] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 4-2.

Trump, Donald J. “National Cyber Strategy of the United States of America.” September 2018. p. 20-21. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The US Department of Defense. “National Defense Strategy 2022.” 2022. p. 9. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[88] Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. “Cyber Persistence Theory Redefining National Security in Cyberspace”. Oxford University Press. New York. 2022. p. 16-17.

McKenzie, Timothy M. “Is Cyber Deterrence Possible?” Air University Press, 2017. p. 13. https://apps.dtic.mil/sti/pdfs/AD1122446.pdf

Goodman, Will. “Cyber Deterrence: Tougher in Theory than in Practice?” Strategic Studies Quarterly 4, no. 3. 2010. p. 128-129. http://www.jstor.org/stable/26269789.

Singer, Peter W. Friedman, Allan. “Cybersecurity: What everyone needs to know”. Oxford University Press. New York. 2014. p. 152.

Soesanto, Stefan. "Cyber Deterrence Revisited." Perspectives on Cyber Power. 2022. p. 26. https://apps.dtic.mil/sti/pdfs/AD1122446.pdf

[89] Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. “Cyber Strategy: The Evolving Character of Power and Coercion.” Oxford University Press. New York. 2018. p. 66-130.

Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 42

[90] Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. “Cyber Strategy: The Evolving Character of Power and Coercion.” Oxford University Press. New York. 2018. p. 169-199.

Brazil. “Política Naval.” Marinha do Brasil. p. 38. https://www.marinha.mil.br/sites/default/files/politicanaval_site.zip

The US Department of Defense. “Cyber Strategy”. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[91] Buchanan, Ben. “The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.” Oxford University Press. New York. 2016. p. 86-87.

[92] Trump, Donald J. “National Cyber Strategy of the United States of America.” September 2018. p. 20-21. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The US Department of Defense. “Cyber Strategy”. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

The US Fleet Cyber Command. “Strategic Plan 2020-2025”. https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d.

[93] Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. “Cyber Persistence Theory Redefining National Security in Cyberspace”. Oxford University Press. New York. 2022. p. 26-60

[94] National Security Strategy Course “Lesson 12, Required Reading. Evaluating Strategy - Adapted from the work of COL Greg Schultz, USA, NWC Faculty, original work.” August 22, 2012. Available on Blackboard.

[95] Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. “Cyber Strategy: The Evolving Character of Power and Coercion.” Oxford University Press. New York. 2018. p. 133-167.

Freedman, Lawrence. “Strategy: A History”. Oxford University Press. 2013. p. 615-617.

Clark, Howard Gambrill. “Narrative and Warfare (AY2023SLFC20)”. Influence Warfare. July 17, 2022. https://howardgambrillclark.podbean.com/e/narrative-and-warfare-ay2023slfc20/.

[96] National Security Strategy Course Lesson 12, Required Reading. “Evaluating Strategy - Adapted from the work of COL Greg Schultz, USA, NWC Faculty, original work.” August 22, 2012. Available on Blackboard.

[97] Heffington, Steve. Oler, Adam. Tretler, David. “A National Security Strategy Primer”. National Defense University Press. Washington, DC. 2021. p. 19-35.

[98] Brazil. “Constituição da República Federativa do Brasil de 1988.” https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm

Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 160

[99] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-6 – 1-14.

[100] Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília-DF: 2021. p. 1-6 – 1-14.

[101] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 161

[102] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 161

[103] Trimble, Daniel. Monken, Jonathan. Sand, Alexander F. L. “A framework for cybersecurity assessments of critical port infrastructure.” International Conference on Cyber Conflict (CyCon U.S.). 2017. p. 5-6. https://ndu.blackboard.com/bbcswebdav/pid-2048921-dt-content-rid-4098094_2/xid-4098094_2

Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 78-81

[104] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 160

[105] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 160

[106] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 78-81

[107] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 162

Khan, Saif M. "US Semiconductor Exports to China: Current Policies and Trends." Washington, DC: Center for Security and Emerging Technology, October. 2020. https://cset.georgetown.edu/wp-content/uploads/U.S.-Semiconductor-Exports-to-China-Current-Policies-and-Trends.pdf

Fundaments of the Information Environment Course. “Seminar Discussions.” November 2022.

[108] Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 162

[109] Ablon, Lillian. Bogart Andy. "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits". RAND Corporation. 2017. p. 4. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

Fundaments of the Information Environment Course. “Lesson 1”. September 13, 2023.

[110] Buchanan, Ben. “The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.” Oxford University Press. New York. 2016. p. 77-81.

[111] Ablon, Lillian. Bogart Andy. "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits". RAND Corporation. 2017. p. 57-61. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf.

[112] Fundaments of the Information Environment Course. “Lesson 1”. September 13, 2023.

Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. “Cyber Strategy: The Evolving Character of Power and Coercion.” Oxford University Press. New York. 2018. p. 39.

[113] The US Cyber Command. “Brownbag.” October 9, 2022.

The US Cyber Command. “CYBER 101 – Cyber Mission Force.” Webpage. Accessed on December 27, 2022. https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3206393%2Fcyber-101-cyber-mission-force%2F

[114] The US Cyber Command. “Brownbag.” October 9, 2022.

The US Cyber Command. “CYBER 101 – Cyber Mission Force.” Webpage. Accessed on December 27, 2022. https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3206393%2Fcyber-101-cyber-mission-force%2F

Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022. p. 160

[115] Fundaments of the Information Environment Course. “Lesson 14, Seminar Discussions.” November 15, 2022.

[116] The US Fleet Cyber Command. “Strategic Plan 2020-2025”. https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d.

[117] Ibid.

[118] Ackerman, Robert K. “Navy Amasses Digital Armada.” SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. “Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships.” SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

[119] Ackerman, Robert K. “Navy Amasses Digital Armada.” SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. “Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships.” SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

[120] Ackerman, Robert K. “Navy Amasses Digital Armada.” SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. “Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships.” SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

[121] Ackerman, Robert K. “Navy Amasses Digital Armada.” SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. “Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships.” SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

[122] White, Timothy J. “Navy Cryptologic & Cyber Warfare Community Vision.” February 8, 2019. https://permanent.fdlp.gov/gpo147594/CW_COMMUNITY_VISION.PDF

[123] The US Congressional Research Service. “Convergence of Cyberspace Operations and Electronic Warfare”. In Focus. August 13, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11292.

[124] National Security Strategy Course Lesson 12, Required Reading. “Evaluating Strategy - Adapted from the work of COL Greg Schultz, USA, NWC Faculty, original work.” August 22, 2012. Available on Blackboard.

[125] Ibid.

[126] Ibid.

[127] The US Congressional Research Service. “Convergence of Cyberspace Operations and Electronic Warfare”. In Focus. August 13, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11292.

The US Congressional Research Service. “Defense Primer: Cyberspace Operations”. In Focus. December 1, 2021. https://crsreports.congress.gov/product/pdf/IF/IF10537.

Bibliography

Ablon, Lillian. Bogart Andy. "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits." RAND Corporation. 2017. Accessed on October 24, 2022. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

Ackerman, Robert K. “Navy Amasses Digital Armada.” SIGNAL Magazine. December 1st, 2011. https://www.afcea.org/signal-media/west-22/navy-amasses-digital-armada

Ackerman, Robert K. “Navy Fights to Keep Ahead of Cyber Adversaries - The fleet seeks interoperable security tools to add to the mix of ships.” SIGNAL Magazine. July 1st, 2021. https://www.afcea.org/signal-media/cyber-edge/navy-fights-keep-ahead-cyber-adversaries

Biden Jr, Joseph R. "National Security Strategy." Washington, DC, October 12, 2022. Accessed October 24, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Brazil. “Doutrina Cibernética da Marinha (EMA-419)”. Marinha do Brasil. Estado-Maior da Armada, Brasília. 2021

Brazil. “Estratégia Nacional de Segurança Cibernética”. 2020. Accessed October 24, 2022. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm

Brazil. “Plano Estratégico da Marinha 2040.” Marinha do Brasil. Accessed October 24, 2022. https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/arquivo.pdf

Brazil. “Política Nacional de Defesa e Estartégia Nacional de Defesa”. 2016. Accessed October 24, 2022. https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf

Brazil. “Política Naval.” Marinha do Brasil. Accessed October 24, 2022. https://www.marinha.mil.br/sites/default/files/politicanaval_site.zip

Buchanan, Ben. “The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.” Oxford University Press. New York. 2016

Clark, Howard Gambrill. “Narrative and Warfare (AY2023SLFC20)”. Influence Warfare. July 17, 2022. Accessed October 24, 2022. https://howardgambrillclark.podbean.com/e/narrative-and-warfare-ay2023slfc20/.

Clarke, Richard Alan. Knake, Robert K. “Cyber war”. Harper Collins e-books, 2014. Accessed October 24, 2022. https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf

Fischerkeller, Michael P. Goldman, Emily O. Harknett, Richard J. "Cyber Persistence Theory Redefining National Security in Cyberspace." Oxford University Press. New York. 2022

Freedman, Lawrence. "Strategy: A History." Oxford University Press. New York. 2013

Heffington, Steve. Oler, Adam. Tretler, David. "A National Security Strategy Primer." National Defense University Press. Washington, DC. 2021

Lakshmanan, Ravie. "New Air-Gap Attack Uses SATA Cable as an Antenna to Transfer Radio Signals." July 19, 2022. Accessed October 24, 2022. https://thehackernews.com/2022/07/new-air-gap-attack-uses-sata-cable-as.html

Lee, Micah. Moltik, Henrik. "Everybody does it: The Messy Truth about Infiltrating Computer Supply Chains." The Intercept. January 24, 2019. Accessed October 24, 2022. https://theintercept.com/2019/01/24/computer-supply-chain-attacks/

Lykke Jr, Arthur F. "Defining Military Strategy." Military Review. May 1989. Accessed October 24, 2022. https://cgsc.contentdm.oclc.org/digital/api/collection/p124201coll1/id/504/download

Mintzberg, Henry. "Crafting Strategy." Strategic Planning. Harward Business Review. July 1987. Accessed October 24, 2022. https://hbr.org/1987/07/crafting-strategy

Montgomery, Mark. Borghard, Erica. “Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence,” Joint Force Quarterly 102, 3rd Quarter. 2021, 79-89.

Moore, Daniel. “Offensive Cyber Operations: Understanding Intangible Warfare.” Oxford University Press, 2022.

Moritz Lipp et al., “Meltdown: Reading Kernel Memory from User Space,” in 27th USENIX Security Symposium (USENIX Security 18), 2018. Accessed October 24, 2022. https://meltdownattack.com/meltdown.pdf

Pereira, Wagner G. “What should a senior naval leader be concerned about regarding indicators in cyberspace warfare?” Fundaments of the Information Environment End-of-Course Paper. December 16, 2022.

Pomerleau, Mark. “US military to blend electronic warfare with cyber capabilities.” C4ISRNET. April 14, 2021. Accessed October 24, 2022. https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/

Robertson, Jordan. Riley, Micha el. “China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies,” Bloomberg. October 4, 2018. Accessed October 24, 2022. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Siegel, Carol A. Sweeney, Mark. "Cyber Strategy - Risk-Driven Security and Resiliency." Taylor & Francis Group. Florida. 2020

Singer, Peter W. Friedman, Allan. "Cybersecurity: What everyone needs to know." Oxford University Press. New York. 2014

Smeets, Max. “No Shortcuts. Why States Struggle to Develop a Military Cyber-Force” C. Hurst & Co. (Publishers) Ltd. London. 2022.

Sun Tzu. "The Art of War." Translated by Lionel Giles. Edited by Aggott Hönsch István. Pax Librorum Publishing House. 2009

The International Institute for Strategic Studies. “Cyber Capabilities and National Power: A Net Assessment.” June 28, 2021. Accessed October 24, 2022. https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf?la=en&hash=832036F094A4C489C313AC617643369E07FAE9F8

The US. “National Cybersecurity Strategy.” March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The US College of Information and Cyberspace. “Fundaments of the Information Environment Course: Lesson 1”. September 13, 2022

The US Congressional Research Service. "Defense Primer: Cyberspace Operations." In Focus. December 1, 2021. Accessed October 24, 2022. https://crsreports.congress.gov/product/pdf/IF/IF10537

The US Congressional Research Service. "Convergence of Cyberspace Operations and Electronic Warfare." In Focus. August 13, 2019. Accessed October 24, 2022. https://crsreports.congress.gov/product/pdf/IF/IF11292

The US Department of Defense. "Cyber Strategy." 2018. Accessed October 24, 2022. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

The US Fleet Cyber Command. “Strategic Plan 2020-2025”. Accessed October 24, 2022. https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d

The US Department of Defense. “National Defense Strategy 2022.” 2022. p. 20. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

Trimble, Daniel. Monken, Jonathan. Sand, Alexander F. L. “A framework for cybersecurity assessments of critical port infrastructure.” International Conference on Cyber Conflict (CyCon U.S.). 2017. p. 1. https://ndu.blackboard.com/bbcswebdav/pid-2048921-dt-content-rid-4098094_2/xid-4098094_2

Valeriano, Brandon. Jensen, Benjamin. Maness, Ryan C. “Cyber Strategy: The Evolving Character of Power and Coercion.” Oxford University Press. New York. 2018

Vigliarolo, Brandon. "Smartphone gyroscopes threaten air-gapped systems, researcher finds Network interface card LEDs are a risk too by blinking in Morse code." The Register.

August 23, 2022. Accessed October 24, 2022. https://www.theregister.com/2022/08/23/phone_gyroscopes_airgapped_systems/

Wedin, Lars. “Maritime Strategies for the 21st Century: The Contribution by Admiral Castex.” Kindle’s Edition. 2017