A Sensemaking Framework for Defensive Cyber Operations: Filling the Void in Leadership Discourse

Frank Wleklinski and Timothy Shives
Naval Postgraduate School*, Monterey, California, USA
*(The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government.)

frank.wleklinski@nps.edu
timothy.shives@nps.edu

Abstract: In the realm of contemporary warfare dominated by cyber threats, Defensive Cyber Operations (DCO) serve as a linchpin for mitigating risks and ensuring mission assurance. This article delves into the intricate landscape of DCO, focusing on the critical role played by Defensive Cyberspace Forces (DCFs). Despite their significance, the absence of a unified sensemaking framework poses a challenge for leaders responsible for the nuanced development and strategic employment of DCFs. The lacuna in the existing literature revolves around the lack of a comprehensive sensemaking framework tailored for operational and DCF leaders. The inadequacies of current frameworks, either overly broad or excessively specific, hinder effective dialogue and understanding. This deficiency not only obstructs the planning efforts and operational tempo of DCO but also restrains the maturation of DCFs, amplifying residual risks faced by commanders. This paper endeavours to present a purpose-built sensemaking framework crafted for leaders engaged in the dynamic realms of DCF development. Integrating well-established risk mitigation principles with the unique organizational structures and missions of DCFs, the framework fills a crucial void in the literature. Beyond being a decision-support tool, it strives to foster a shared mental model, providing a nuanced lens for leaders to contextualize and prioritize their efforts in the complex landscape of DCO. Through a meticulous critique of existing frameworks, this article introduces a tailored model designed to address identified shortcomings. Emphasizing the practical utility of the proposed framework, the discussion unfolds to elucidate how it not only facilitates the development and employment of DCF but also contributes to organizational resilience and risk mitigation. This article contributes a novel sensemaking framework to the academic discourse on DCO. While acknowledging limitations imposed by an unclassified context, the framework provides valuable insights into the strategic dimensions of DCF development and employment, DCO planning intricacies, and organizational analyses. Future avenues for research include the integration of classified information to refine the framework, ensuring its applicability across diverse DCO mission types and aligning DCF core functions with specific threats, thereby enhancing the efficacy of defensive cyber strategies.

Keywords*:* Defensive Cyber Operations, Sensemaking Framework, Defensive Cyberspace Forces, Cyber Risk Mitigation, Operational Resilience

1. Introduction

In the dynamic and ever-evolving landscape of cybersecurity, the complexity of Defensive Cyberspace Operations (DCO) presents a formidable challenge for leaders and practitioners. The rapid proliferation of cyber threats, coupled with the intricate interplay of technology, data, and networks, necessitates a comprehensive framework that not only clarifies the intricacies but also serves as a common language for decision-makers. This article addresses this imperative need by introducing a groundbreaking sensemaking framework—aptly named a "Sensemaking Framework for Defensive Cyber Operations"—crafted to enhance the efficacy of Defensive Cyber Forces (DCF) in navigating the multifaceted realm of DCO.

The current cybersecurity milieu is inundated with a plethora of risk mitigation frameworks and policy documents, each vying for attention and implementation. However, the existing frameworks often fall short when it comes to providing a cohesive and operationally relevant model for DCO. Recognizing this gap, the authors delve into the intricacies of DCO, emphasizing the critical role of a shared mental model and a standardized language in fostering effective communication and decision-making.

The purpose of this framework is to meticulously cut through the complexity, offering a structured approach to interpret and contextualize DCO within the broader landscape of risk management. As leaders in the field are confronted with diverse cyber systems, technologies, and threat landscapes, this conceptual framework provides a navigational tool that categorizes, prioritizes, and evaluates the myriad aspects of DCO. Its adaptability to various organizational objectives and mission domains positions it as a versatile and indispensable resource for leaders engaged in DCF development, employment, and maintenance.

This article unfolds by examining the limitations of existing frameworks, establishing the rationale for this new framework, and subsequently delving into its components and applications. From enhancing real-time decision-making to serving as a planning tool for organizational development and troubleshooting, the framework

emerges as a comprehensive solution tailored to the nuanced demands of contemporary defensive cyberspace activities. Through this exploration, the article aims to contribute a foundational resource that not only aids in making sense of the intricacies of DCO but also propels the field towards enhanced operational effectiveness and cyber resilience.

2. Problem

Defensive Cyber Operations (DCO) fundamentally aim to mitigate risks for operational commanders, functioning as a cornerstone of mission assurance. In tandem, organizations have developed Defensive Cyberspace Forces (DCFs) as crucial risk mitigation tools, addressing cyber-dependencies in alignment with tactical, operational, and strategic objectives. DCFs, while not typically the primary focus, exist to support the overall mission of commanders. Consequently, leaders and their staffs must make strategic decisions on methods for the development, maintenance, and employment of DCFs.

The challenges faced by these leaders are twofold. Firstly, DCFs are inherently limited, involving costly cyber talent and equipment. Secondly, the constant need for cyber defense arises from the expanding attack surface facilitated by networked hardware and software supporting diverse warfighting functions. DCF leaders must navigate a real-world scenario of trade-offs, strategically allocating limited resources in a zero-sum game to develop and employ DCFs while mitigating risks posed by a growing number of cyber dependencies.

While the existence of well-known cyber risk mitigation frameworks may suggest a solution, the reality is complex. Unfortunately, most frameworks, whether too broad or too narrow, lack practicality for everyday use. This gap in literature highlights a disconnect, as existing frameworks, while beneficial for specific work roles or organizational levels, fail to align with the needs of leaders and planners directly responsible for creating, maturing, and employing DCFs. Furthermore, these frameworks lack a shared model for creating common understanding.

Developing and employing DCFs without a specific framework may seem plausible, as many leaders and planners currently do so, progressively enhancing capabilities. However, this success often relies on sheer will and ingenuity rather than a repeatable and predictable organizational process. The lack of a pragmatic model for DCF employment poses scalability challenges. The consequences of cyber threats and their defense are evident, emphasizing the critical need for a sensemaking framework in DCO. The absence of a shared mental model hampers the development and employment of DCFs, creating a significant artificial barrier to their effective utilization.

The absence of a shared sensemaking framework for operational and Defensive Cyberspace Forces (DCF) leaders and staff hinders collaborative dialogue on the development and employment of DCF. This deficiency is critical because the lack of a unified language and shared mental model organizing the various types and purposes of Defensive Cyber Operations (DCO) impedes the effective utilization of DCF (Camillo and Miranda, 2011; Schrier, 2022). Additionally, the absence of a shared sensemaking model complicates efforts to articulate the purpose behind different types of DCO that DCF can conduct (Moore, Dynes, and Chang, 2015). This collective limitation slows down DCO planning efforts, hampers operational tempo, and constrains the organizational maturation of DCF, ultimately elevating a commander's residual risk.

3. Purpose

This paper aims to address the identified problem by presenting a comprehensive sensemaking framework for Defensive Cyber Operations (DCO), specifically designed to support leaders and staff responsible for developing and employing DCF, referred to as DCF leaders. The framework draws upon well-established risk mitigation principles while integrating DCF organizational structures and missions. While numerous cybersecurity-related policies and issuances exist, often focusing on compliance, high-level programmatic matters, or holistic risk mitigation for enterprise portfolios, the presented framework fills a crucial gap in the literature.

This framework stands out by providing sensemaking and decision-support tools tailored to the unique responsibilities of DCF leaders and planners. It goes beyond existing policies by offering an overarching model that contextualizes and concentrates discussions. Additionally, it contributes to the literature by aiding in the establishment of a shared mental model among DCF leaders. The authors build on previous works, striving to create a cohesive framework for defensive cyber missions (Guion and Reith, 2017; Schrier, 2022; Voice, 2022). This paper represents a valuable addition to the existing body of knowledge in the field.

Next, the authors provide several definitions and the limitations of this paper. Then they discuss the shortcomings of the current frameworks and provide a model to address the problem. Finally, the authors discuss how the proposed Sensemaking Framework aids in developing and employing DCF. Thus, this paper uniquely addresses the critical gap in existing literature by presenting a tailored sensemaking framework for Defensive Cyber Operations (DCO). By integrating risk mitigation principles with Defensive Cyberspace Forces (DCFs) organizational structures, it offers invaluable insights for leaders navigating the complex landscape of cyber defense. This innovative contribution enhances strategic decision-making and organizational resilience, initiating this conversation to the academic community and cyber operations community seeking cutting-edge perspectives on DCO.

4. Definitions

To ensure clarity for both DCF and non-DCF personnel, the authors will establish local definitions, recognizing potential semantic differences from established publications. The paper will strive to identify instances of such divergence for traceability.

Developing DCF. Making force structure decisions on how and why to man, train, and equip DCF in alignment with intended typification of DCO.

Employing DCF. Aligning DCF to cyber systems and deploying them to conduct defensive activities or operations. Also refers to the holistic DCO mission planning process, encompassing activities such as communicating, categorizing, prioritizing, evaluating, and directing various DCF activities.

DCF. Any formation participating in defending cyber-enabled systems, deviating from United States Cyber Command (USCC) definitions to include the United States Department of Defense (DOD) and Service organic Cyber Security Service Providers (CSSP) and DCO formations outside the operational command of USCC. For the DOD audience specifically, the authors define DCF as the DCF identified in USCC CWP 3-33.4 (United States Cyberspace Command (USCC), 2020), namely the various types of Cyber Protection Teams plus DOD and Service organic CSSP and DCO formations outside the operational command of USCC. The authors break from the USCC definitions because this second group consists of units who perform similar cybersecurity and defensive cyber functions for the respective Services (equivalent to DCO-Internal Defense Measures (IDM) Companies or Network Battalions in the Marine Corps), have much or even the same training, share personnel, and are often considered for employment, or compete, with USCC DCF.

DCO. Any activity taken to defend or secure a network, taking a broad approach beyond specific definitions given by USCC.

DCF Leaders. Commanders or staff members directly engaged in building, developing, maintaining, or employing DCF, encompassing those with operational, tactical, or administrative control.

5. Limitations

The authors acknowledge that the true nature of this conceptual framework is best conveyed in briefs or conferences. The written publication serves as an attempt to meet the demand for a published version, recognizing that certain nuances and connections may be lost in written explanations. The primary purpose of this framework is to serve as a decision support tool and discussion aid, with the hope that this publication sparks further discussions leading to additional applications and insights.

6. Existing Risk Mitigation Frameworks

In the expansive realm of cybersecurity, the abundance of risk mitigation frameworks and policy documents has reached a point of complexity that poses challenges for practical use. Even with attempts to organize the Department of Defense's (DoD) cybersecurity policies chart, the resulting visual representation often underscores the intricate web of dependencies and cross-references, making navigation a daunting task. Notwithstanding, credible organizations have contributed noteworthy frameworks aimed at mitigating risks stemming from cyber dependencies. See Figure 1.

One such framework is the DoD-Instruction (DoDI) 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT) (DoD, 2014). While it serves as an overarching document directing the management of the DoD's enterprise IT systems, it relies on external references for implementation guidance, contributing to the challenge of practical applicability. Another significant contributor is the body of NIST Special Publications

(SPs), including the Cybersecurity Framework (Computer Security Division, 2016; NIST, 2018b, 2018a). NIST's RMF principles underpin the DoD IT RMF, focusing on enterprise risk management and providing guidance applicable to both governmental and non-governmental organizations.

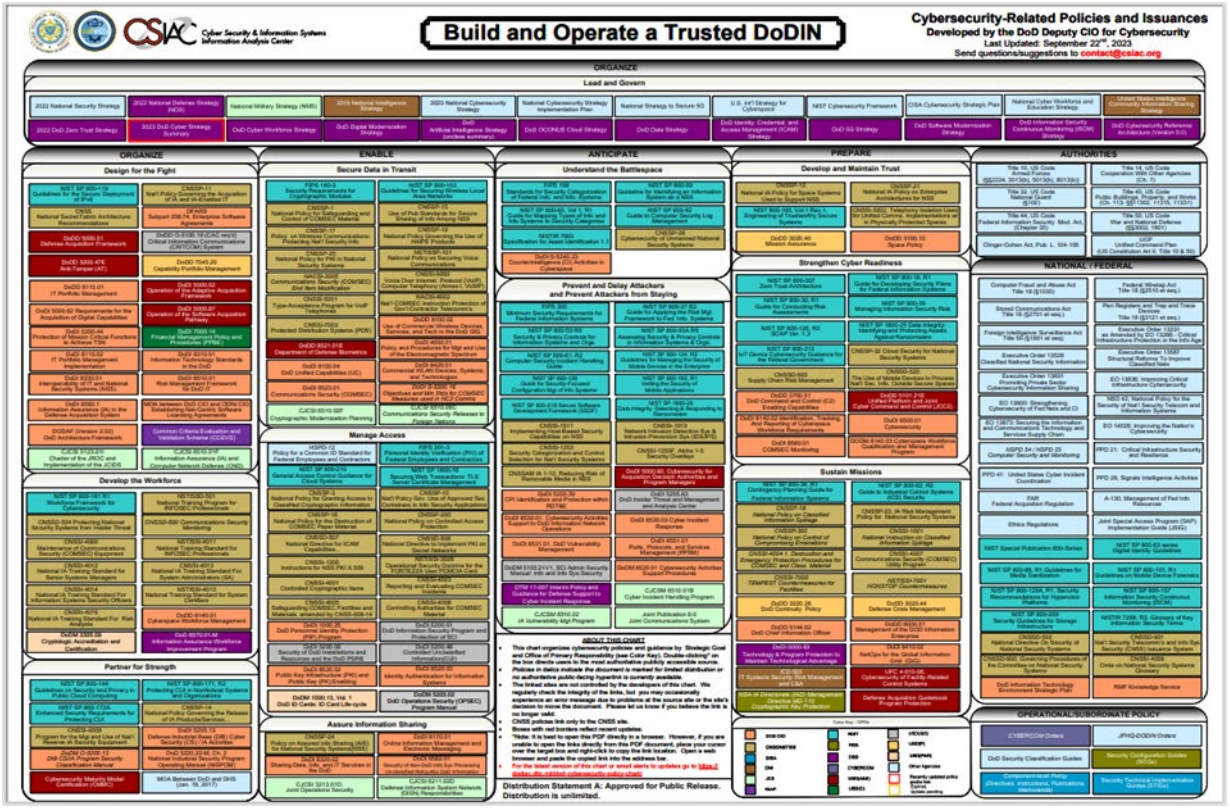

Figure 1: DOD Cybersecurity Chart (DOD, 2023). Available at: https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

The Defense Information Systems Agency (DISA) adds to the landscape with Security Technical Implementation Guides (STIGs), offering government configuration standards for IT systems and software (DISA, 2023). Despite their widespread use as best practices, STIGs are specific and technical, limiting their applicability at operational levels. Additionally, the Institute of Electrical and Electronics Engineers (IEEE) contributes to risk management through its Enterprise Risk Management Program (ERM), acknowledged for its authoritative guidelines (IEEE, 2023).

Despite the rigor and expertise invested in these frameworks, they often fall short when it comes to the specific challenges faced by Defensive Cyberspace Forces (DCF) leaders. Existing frameworks tend to fall into two categories, being either too broad or too narrow, leaving practitioners, operators, and DCF leaders to interpret and implement guidance not always tailored to their specific organizational focus. The high-level framework aims for broad usability, introducing ambiguity and scenario agnosticism. The lower-level frameworks aim for narrow specificity, introducing complex technical dependencies that cannot always be applied perfectly in a real-world production system. The combined deficiencies create a gap in practical decision support aids and shared mental models crucial for the development and employment of DCF.

Within the existing landscape, some frameworks are deemed too high level, serving administrative or bureaucratic purposes, and often conflicting with the realities of the operational environment. On the other hand, there are frameworks that are too narrow, presenting specific checklists for technology or configuration security, which may not be applicable at operational levels or aid in the development and employment of DCF.

In essence, the multitude of frameworks, policies, and directives generates equivocality and uncertainty, hindering practitioners in need of accurate and specific solutions to their operational problems. This situation prevents the establishment of a shared mental model, obstructs the creation of shared meaning, and frustrates meaningful dialogue. While existing documents serve their intended purposes, none comprehensively address the brass-tax needs of operational staff, particularly DCF leaders, operational commanders, and their staffs requiring prompt decisions on limited DCF resources. The forthcoming framework seeks to rectify these issues

by providing a more accurate and specific framework for discussing and describing DCF and Defensive Cyber Operations (DCO).

7. A Proposed Sensemaking Framework for Defensive Cyber Operations

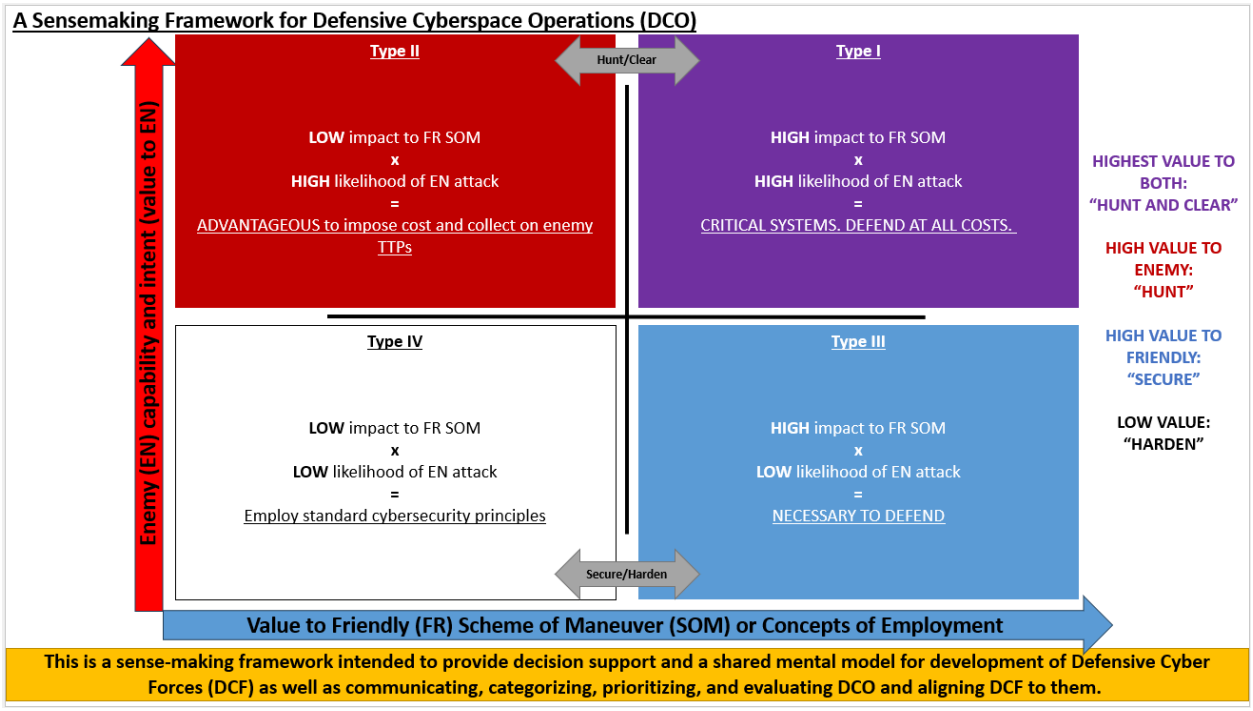

Figure 2: The Sensemaking Framework for Defensive Cyber Operations

Before delving into the utility of this conceptual framework, described by the authors as a "Sensemaking Framework for Defensive Cyber Operations," it is crucial to understand its structure. The following sections provide an explanation of how to interpret The Framework using the accompanying graphic.

7.1 The Horizontal and Vertical Axis

In today's organizational landscape, risk management principles play a pervasive role. The Department of Defense (DoD) mandates that every service member undergo an online class in risk mitigation aligned with their rank/grade. As previously emphasized, cybersecurity and Defensive Cyberspace Forces (DCF) are instrumental in mitigating risks to support an organization's overarching goals. The framework aligns with risk management frameworks by establishing a horizontal and vertical axis corresponding to key risk factors.

On the horizontal (X) axis lies the "Value to Friendly (FR) Scheme of Maneuver (SOM) or Concepts of Employment (CONEMP)." This "value" correlates with the technology, data, or network under consideration and is analogous to the "impact" variable in risk calculations. The higher the value of a technology, data, or network in supporting or enabling FR SOM and CONEMPs, the greater the impact of an incident or intrusion on that entity.

The vertical (Y) axis represents the "Enemy (EN) capability and intent (value to EN)." Similar to the horizontal axis, the "value" pertains to the technology, data, or network and aligns with the "likelihood" variable in risk calculations. The higher the value of the targeted technology, data, or network in supporting the EN's SOMs or CONEMPs, the greater the likelihood of it being targeted. Such definitions align with Joint Operational and Targeting definitions (DoD, 2011; DoD, 2013). Notably, a technology, data, or network valuable to FR objectives may also be deemed valuable to the enemy, such as a High-Pay Off Target (HPV) with asymmetrical impacts. Conversely, the enemy may prioritize a High-Value Target (HVT) valuable to their objectives, even if it doesn't align with FR objectives.

Beyond military metaphors, the "value to EN" variable requires further breakdown, as indicated in its description. From the defender's viewpoint, the likelihood of an EN attack, or its value, depends on both how well such an attack aligns with the EN's objectives (intent) and the EN's capabilities to execute an attack (capability). This necessitates an intelligence-supported assessment of mediating variables like "EN capability"

and “EN intent,” typically backed by an organizational intelligence apparatus in a military setting or open-source threat intelligence in the private sector.

7.2 The Center Quad Chart

Quad charts, a common element in the DoD, find application in this framework by overlaying major risk mitigation axes with a typology for Defensive Cyberspace Operations (DCO) and target data, technology, or networks (systems). The horizontal and vertical axes enable the creation of a standard quad-chart, dividing the chart into four sections, labelled 1 – 4. These numbers serve as nomenclature without indicating relative priority or order. While the authors assigned ordinal risk labels approximating relative priority, it's emphasized that the assignment may vary depending on the using organization and its mission domain. This flexibility is a key advantage of this framework as it is tailored for a military audience—but has applications that can be broadened outside of military cyber operations.

The relative location of the black vertical and horizontal lines forming the borders of these four sections is also arbitrary. Each organization will have to determine for itself where these thresholds are. However, many of the existing frameworks discussed provide useful guidance on what systems fall into which category, and therefore can aid a DCF leader is standardizing these across an organization or within a local discussion. Still, some systems will fall between categories or into more than one depending on temporal organizational and environmental factors. This highlights another advantage of this framework as is forces and fosters a discussion about the value of a given system to both FR and EN SOMs and CONEMPs as well as frames the conversation in terms of standard RMF language, providing a mental model and langue to make such discussions meaningful.

7.2.1 Type I: Defend at all Costs

Situated at the top right, Type I corresponds to critical systems demanding defense at all costs. These systems, supporting national or strategic assets like nuclear command and control or classified data networks, align with Defense Critical Infrastructure (DCI) or Task Critical Assets (TCAs) (CJCS, 2012). Adversaries are likely to develop capabilities and intentions to target these systems, necessitating Hunt and Clear operations specifically tailored to threat intelligences aligning to the assessed EN’s capabilities.

7.2.2 Type II: Advantageous to Impose Cost and Collect on an Adversary

Found in the top left, Type II systems are of lower value to FR SOM or CONEMP but satisfy EN objectives. These systems may include foreign partner or allied systems of interest to the adversary. DCO on these systems, aligned with Hunt and Clear operations, aids in collecting information about adversary capabilities and intentions. It may not always be necessary to clear these systems given intelligence gain/loss considerations.

7.2.3 Type III: Necessary to Defend

Type III systems, located at the bottom left, are of high value to FR SOM but with a low likelihood of EN attack. These systems can asymmetrically disrupt FR operations. While the likelihood of attack is low, the impact could lead to FR mission failure, necessitating defense. DCO typically aligns with Hunt and Clear operations but since EN attack is assessed to be less likely, such operations may be threat actor agnostic.

7.2.4 Type IV: Employ and Enforce Standard Cybersecurity Principles

Situated at the bottom right, Type IV systems have low impact on FR SOM and a low likelihood of EN attack. These systems, representing administrative or quality of life operations, adhere to cybersecurity best practices. They are defended by Cyber Security Service Providers (CSSPs) and receive the lowest priority for defensive cyber maneuver forces. DCO aligns with Secure and Harden operations. Continuous demand for more exquisite defensive maneuver cyber forces on these systems may indicate misclassification of DCO or inappropriate employment of DCF, prompting reassessment by DCF leaders.

Typically, it is not to appropriate employ defensive maneuver cyber forces, such as Cyber Protection Teams (CPTs), against systems of this type unless in a temporary reinforcing role to supplement the standing CSSP. However, if the need to do so arises, it may be a sign that the system was misclassified. If defensive maneuver cyber forces are continually in demand to conduct DCO on this type of systems, it may be a further sign that these systems need to be re-classified. If such forces are continually executing DCO on these systems, it may

also be a sign these forces are not being employed appropriately and should alert DCF leaders to assess if other types of systems, and therefore risks, are being left uncovered.

8. Improving Decision Making

Shared mental models reduce uncertainty and underpin the ability to effectively share meaning (Shannon, 1948; Shannon and Weaver, 1949). Without a shared model, effective communication is difficult. Communication enables joint decision making among teams (Covey and Merrill, 2008). The novel combination of standard risk mitigation language overlaid with impact to friendly and adversary courses of action builds upon reference frames already familiar in defense organizations. This amalgamation establishes a new sensemaking model effective for creating meaning, thereby fostering better development and employment decisions regarding defensive cyber forces (DCF).

This framework fills the gaps left by the extant literature and guidance that are either too broad, too narrow, or were never intended for operational matters in the first place. It is a centralizing tool around which to communicate cyber risk, categorize systems and operations, and prioritize them. It enables categorization, prioritization, evaluation, planning, and analysis, all of which serve to advance the effective employment and development of DCF to mitigate an organization's cyber risk.

8.1 Communicating

This new framework serves as a communication tool by establishing a shared mental model and common language for discussing DCO and DCF. It mitigates ambiguity and equivocality resulting from the vast and diverse publications on cybersecurity and risk mitigation. Synthesizing Department of Defense (DoD) and U.S. Cyber Command (USCC) publications, it aligns with their definitions while offering a contextually relevant interpretation for DCF leaders. Shared language and mental models enhance communication, trust, and interoperability.

8.2 Categorizing

This framework functions as a categorization tool to typify various cyber systems and their associated DCO. Users can plot a system (technology, data, or network) along the horizontal and vertical axes, utilizing defined variables and standard Risk Management Framework (RMF) principles. DCF leaders can establish standard labels for each system, facilitating transparent discussions and providing standardized shorthand for different types.

8.3 Prioritizing

Once typification is established, this conceptual framework serves as a guide for prioritization. DCF leaders can align categories with organizational objectives, aiding force allocation decisions, i.e. which DCF should be aligned to which DCO. When faced with requests for forces (RFFs) or internal operations, this categorization helps decide which operations take precedence based on circumstances and which DCF, based on its man, train, and equip charter, is best suited for that operation. The new framework offers a 'why' behind each DCO, articulating the purpose within the context of risk and organizational objectives and justifying the use of limited DCF resources.

8.4 Evaluating

An established prioritization framework allows for the evaluation of previous, active, planned, or potential DCO. This framework helps answer the question, "Are we doing the right things?" It enables DCF leaders to assess if executed DCO missions align with organizational objectives, providing a basis for measuring performance and termination criteria. The Framework aids in evaluating resource allocation by plotting past and current DCO, ensuring a balanced approach across different types. It also provides a systematic method to assess proposed DCO, helping determine the right missions considering the capabilities of the DCF in question. This framework allows the DCF leader to match specific types of DCF to Types of DCO and corresponding systems, ensuring the appropriate resources are committed to each mission.

8.5 Organizational Planning

This framework not only serves as a reactive tool for DCF leaders to make sense of operational matters in real time but also functions proactively as a powerful planning tool. When an organization is establishing its DCF or deciding on the type of DCF to create, this framework facilitates the analysis of the organization's strategy,

objectives, and existing systems. This analysis helps the DCF leader determine the specific DCF formation and capabilities to invest in, enhanced by using this framework to categorize and prioritize potential DCO.

Similarly, existing DCF can evaluate their capabilities to cover the types of DCO an organization might require based on its objectives and systems. This forecasting assessment becomes a tool to advocate for additional investment or alert organizational leaders to potential risks that the existing DCF might be unable to mitigate.

8.6 Organizational Troubleshooting and Analysis

This conceptual framework also serves as an analytic tool for assessing an organization's cyber risk mitigation efforts. Applying the Evaluation use case retroactively helps answer the question, “Are we doing things right?” By ensuring that the correct DCF aligns with DCO, confirming the execution of the right DCOs, and validating that the reasons behind each DCO align with organizational objectives, this framework identifies potential lapses or violations of best practices in DCF development or employment. Uncovering inefficiencies and deficiencies, it contributes to improving DCF employment, maturing organizational DCF capabilities, and maintaining an appropriate level of risk mitigation. The results of this analysis can be effectively communicated using this conceptual framework as a visual and conceptual aid, fostering common language and a shared mental model.

9. Conclusion

In conclusion, this article addresses a gap in the existing literature and practice by introducing a sensemaking framework for Defensive Cyberspace Operations (DCO) that serves as a shared mental model and facilitates a common language for leaders engaged with Defensive Cyber Forces (DCF). The authors recognize the limitations imposed by the requirement of developing a conceptual framework that is based on real world capabilities, but academically require staying within the confines of unclassified research. However, the authors still assert this framework’s significance in providing clarity and coherence to the complex landscape of DCO.

The proposed framework, aptly described as a “Sensemaking Framework for Defensive Cyber Operations,” is designed to enhance communication, categorization, prioritization, and evaluation within the realm of DCO and DCF. By aligning with existing Department of Defense (DoD) and U.S. Cyber Command (USCC) publications, this framework operationalizes these concepts in a contextually relevant manner for DCF leaders. It establishes a clear and transparent rating scale, introducing standardized labels or “Types” that serve as a shorthand for various cyber systems and their aligning DCO.

The utility of this defensive conceptual framework extends across various use cases, both reactive and proactive. DCF leaders can employ it in real-time operations to make sense of contextual matters, prioritize resource allocation, and articulate the purpose behind each DCO. Additionally, the framework serves as a robust planning tool, aiding in the creation and development of DCF, proposing DCO aligned with organizational objectives, and forecasting potential gaps in coverage.

Furthermore, this defensive framework contributes to organizational troubleshooting and analysis, allowing leaders to assess the effectiveness of cyber risk mitigation efforts retrospectively. It assists in determining whether the right actions are being taken, if DCF resources are appropriately allocated, and if the overall strategy aligns with organizational objectives. The visual and conceptual clarity provided by this framework fosters a shared understanding, improving communication, trust, and interoperability among DCF leaders and their counterparts.

While acknowledging the current limitations and the need for future research to overlay higher classified information, the authors emphasize the framework’s potential to evolve and adapt. The integration of types of systems within the quad chart [FIGURE 2], alignment of DCF to DCO types, and correlation of DCO mission types with Cyber Protection Team (CPT) core functions are identified as areas for further exploration. In essence, this conceptual Sensemaking Framework for Defensive Cyber Operations presents a valuable step forward in enhancing the effectiveness and efficiency of DCO within the contemporary cyber landscape.

References

CJCS (2012) ‘CJCSI 3209.01: Defense Critical Infrastructure Program’. Chairman of the Joint Chiefs of Staff. Available at: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01.pdf?ver=2017-02-08-173222-940 (Accessed: 25 October 2023).

Computer Security Division, I.T.L. (2016) *About the RMF - NIST Risk Management Framework | CSRC | CSRC, CSRC | NIST*. Available at: https://csrc.nist.gov/projects/risk-management/about-rmf (Accessed: 18 October 2023).

Covey, S.R. and Merrill, R.R. (2008) *The SPEED of Trust: The One Thing That Changes Everything*. 1st edition. New York: FREE PRESS.

DISA (2023) *Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange*. Available at: https://public.cyber.mil/stigs/ (Accessed: 25 October 2023).

DoD (2014) 'DoDI - 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT)'. U.S. Department of Defense (DoD), Chief Information Officer.

Guion, J. and Reith, M. (2017) 'Dynamic Cyber Mission Mapping', in *Industrial and Systems Engineering Conference*. *Proceedings of the 2017 Industrial and Systems Engineering Conference*, Wright-Patterson AFB, OH: Center for Cyberspace Research, Air Force Institute of Technology.

IEEE (2023) *IEEE Enterprise Risk Management (ERM) Program*. Available at: https://www.ieee.org/about/volunteers/risk-insurance/enterprise-risk-management.html (Accessed: 18 October 2023).

NIST (2018a) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST CSWP 04162018. Available at: https://doi.org/10.6028/NIST.CSWP.04162018.

NIST (2018b) *Risk management framework for information systems and organizations: a system life cycle approach for security and privacy*. NIST SP 800-37r2. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-37r2. Available at: https://doi.org/10.6028/NIST.SP.800-37r2.

Schrier, R. (2022) 'Demonstrating Value and Use of Language–Normalizing Cyber as a Warfighting Domain'.

Shannon, C.E. (1948) 'A mathematical theory of communication', *The Bell System Technical Journal*, 27(3), pp. 379–423. Available at: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

Shannon, C.E. and Weaver, W. (1949) *The mathematical theory of communication*. University of Illinois Press.

United States Cyberspace Command (USCC) (2020) 'Cyber Warfare Publication 3-33.4: Cyber Protection Team Organizations, Functions, and Employment (U//FOUO)'. U.S. Cyberspace Command (USCC).

Voice, J. (2022) 'Leveraging the Ontology of the Operational Cyber Mission Stack', *Cyber Defense Review* [Preprint], (Fall 2022). Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/07_Voice.pdf?ver=3Yffna2m-5WYvC8tuphmWA%3D%3D (Accessed: 24 October 2023).