



ARL-MR-1132 • JULY 2025



Cyberspace Windows of Superiority: Gaps and Challenges

by M. A. Thomas and Stephen Raio

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.



Cyberspace Windows of Superiority: Gaps and Challenges

M. A. Thomas and Stephen Raio
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

1. REPORT DATE		2. REPORT TYPE		3. DATES COVERED	
July 2025		Memorandum Report		START DATE May 1, 2024	END DATE May 20, 2025
4. TITLE AND SUBTITLE Cyberspace Windows of Superiority: Gaps and Challenges					
5a. CONTRACT NUMBER		5b. GRANT NUMBER		5c. PROGRAM ELEMENT NUMBER	
5d. PROJECT NUMBER		5e. TASK NUMBER		5f. WORK UNIT NUMBER	
6. AUTHOR(S) M. A. Thomas and Stephen Raio					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DEVCOM Army Research Laboratory ATTN: FCDD-RLA-ND Adelphi, MD 20783				8. PERFORMING ORGANIZATION REPORT NUMBER ARL-MR-1132	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.					
13. SUPPLEMENTARY NOTES ORCID: M. A. Thomas, 0000-0002-9141-4043					
14. ABSTRACT This report defines a cyberspace window of superiority (CWoS) as a window limited in time and scope when prohibitive interference with mission execution from the cyberspace domain is precluded. Tactical commanders require the capability to identify, predict, and create a CWoS. This report considers existing literature and tools for mission-centric and mission-based cyber risk assessments as a point of departure for further research. However, the purpose and scope of a CWoS estimate differs from most of the existing examples in that it is intended to inform the multidomain decisions of a tactical commander. Moreover, the tactical use case requires methodologies that 1) enable rapid prediction and updating, 2) explicitly model and convey uncertainty, 3) are explainable, 4) support modular modeling, 5) enable defensible fusion of different types of information, 6) are capable of verification and validation, and 7) are achievable with the limited analytic resources at the edge. Data availability for modeling remains a principal challenge, and relevant data is required to produce estimates certain enough to be useful. Future research will explore the use of mission templates and prebuilt, probabilistic, modular models that can be locally populated.					
15. SUBJECT TERMS Network, Cyber, and Computational Sciences; windows of superiority; mission-based cyber risk assessments; multidomain operations; windows of opportunity; cyberspace					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 40	
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			
19a. NAME OF RESPONSIBLE PERSON M. A. Thomas				19b. PHONE NUMBER (Include area code) (520) 713-7868	

STANDARD FORM 298 (REV. 5/2020)

Prescribed by ANSI Std. Z39.18

Contents

List of Figures	iv
List of Tables	iv
1. Introduction	1
2. Cyberspace Windows of Superiority	2
3. Mission-Based Cyber Risk Assessments	5
3.1 Cyber Risk	6
3.2 Cyber Risk to Missions	7
3.3 Mission Decomposition and Mapping	8
3.4 MBCRA for System Decisions	10
3.4.1 MRAP-C	10
3.4.2 DoD Cyber Table Top	11
3.5 MBCRA for Decisions about Missions	12
3.5.1 USCYBERCOM RAM	12
3.5.2 CORT	12
3.6 Mission-Centric Risk Analyses	13
4. Gaps and Challenges	16
5. Conclusions and Future Directions	23
6. References	26
List of Symbols, Abbreviations, and Acronyms	33
Distribution List	34

List of Figures

Figure 1. A mission is decomposed into tasks, tasks are ranked, and systems are mapped to tasks.....	9
--	---

List of Tables

Table 1. A CWoS precludes prohibitive interference in the cyberspace domain.....	3
Table 2. Mission impact criteria.	9

1. Introduction

Army doctrine defines “multidomain operations” as “[t]he combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders” (Headquarters, Department of the Army 2022, Glossary-10). “All operations are multidomain operations,” employing capabilities in the land, air, sea, space, and cyberspace domains (Headquarters, Department of the Army 2022, p. 1–3).

Multidomain operations will be used to create “windows of superiority” that provide freedom of maneuver to friendly forces. According to *The U.S. Army in Multi-Domain Operations* (U.S. Army Training and Doctrine Command 2018, p. x–xii), windows of superiority will “create dilemmas for the enemy while protecting the ability to conduct friendly operations in degraded, disrupted, and/or denied operational environments.”

The cyberspace domain is integral to most operations, either as the primary mission domain or to enable capabilities and operations in other domains. Although windows of superiority need not be restricted to a single domain, a cyberspace window of superiority (CWoS) is one type of window. To enable multidomain operations, tactical commanders require the ability to identify, predict, and create a CWoS. The development of such capabilities is consistent with the Secretary of Defense’s direction to “improve long-range precision fires, air and missile defense including through the Golden Dome for America, cyber, electronic warfare, and counter-space capabilities.” (Secretary of Defense 2025).

This report examines the literature and relevant tools to conduct a gap analysis to identify the requirements for a CWoS model or tool that would enable commanders of tactical missions to better identify, predict, and create CWoS. Section 2 further describes CWoS and notes the lack of doctrinal guidance for identifying or predicting it. Section 3 examines some of the literature on mission-based and mission-centric cyber risk assessments, most of which is designed to serve end users who must make decisions about systems, rather than missions. Section 4 describes the gaps and challenges. Section 5 describes possible directions for further research.

This report concludes that aspects of existing tools and methodologies for assessing cyber risk to missions may be usefully leveraged. However, a CWoS estimate differs from most of the existing approaches in its purpose, which is to inform the decisions of a tactical commander; in its anticipated high-risk use case, which requires explainability, defensibility, and communication of uncertainty;

and in the need to accommodate the limited time and constrained resources at the tactical edge.

2. Cyberspace Windows of Superiority

The Army defines the “cyberspace domain” as “[t]he interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum” (Headquarters, Department of the Army 2022, Glossary-5).^{*} Joint doctrine defines “cyberspace superiority” as “[t]he degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference” (DoD 2024, p. 49). It notes that any such superiority would be localized and temporary (Joint Chiefs of Staff 2022, p. I-1 and I-2).

Instead of “dominance,” Raio (2023, p. 5) advances a spectrum of advantage, in which cyberspace superiority permits friendly operations without prohibitive interference from the cyberspace domain, while “cyberspace supremacy” would guarantee it.

This report defines a “cyberspace window of superiority” as a window limited in time and scope in which friendly forces have cyberspace superiority (Raio 2023, p. 5). The scope of a window may be physical, where friendly forces have a CWoS within a geographic area; or virtual, where friendly forces have a CWoS on a network or system; or it may refer to certain capabilities or activities in cyberspace, such as file transfer; or the scope may be any combination thereof.

Interference is “prohibitive” when a system that provides a mission-critical functionality or condition can no longer do so because of an external action or event that leads to failed mission execution (Table 1). (“Mission execution” means the execution of the intended mission actions; it does not necessarily mean achievement of mission objectives.) For interference to be in the cyberspace domain, the action or event affects a cyberspace system, or a cyberspace action or event indirectly affects a non-cyberspace system, including a human or social group.

“Cyberspace superiority” is an advantage that makes it unlikely that mission execution will face prohibitive interference in the cyberspace domain in a specific

^{*} This definition differs from the DoD dictionary definition of “cyberspace” in that it includes relevant portions of electromagnetic spectrum (Department of Defense 2024, p. 48).

context. Cyberspace superiority is a predictor, not the sole determinant. Other predictors could include actions of intervening forces, environmental variables, or whether any action or event took place that could have caused prohibitive interference.

In this report, a “CWoS estimate” is an estimate of the likelihood that the mission will face prohibitive interference in the cyberspace domain, agnostic to advantage or cause. This estimate is uncertain, reflecting irreducible uncertainty from inherently random processes (aleatory uncertainty) and lack of knowledge of relevant factors (epistemic uncertainty) that theoretically can be reduced through observation. Future work may seek to focus specifically on identifying and predicting the degree of advantage.

Table 1. A CWoS precludes prohibitive interference in the cyberspace domain.

		Prohibitive interference caused by a(n) . . .	
		Cyberspace action or event	Non-cyberspace action or event
Affecting a friendly, mission-critical . . .	Cyberspace system	In scope	In scope
	Non-cyberspace system	In scope	Out of scope

The purpose of a CWoS estimate is to inform commander action. The commander may take actions to improve the probability of a CWoS, or the duration or scope of the CWoS, or make informed trade-offs to engage in other beneficial actions that reduce the probability of a CWoS. The commander could make changes to the mission, such as changing the timing or approach of the mission;* changing the assignment of systems to support the mission; hardening or protecting friendly systems; taking steps to improve system or mission resilience; or reducing an adversary’s ability to engage in actions that cause prohibitive interference. The commander’s defensive and offensive actions to improve the probability of a CWoS are not limited to the cyberspace domain. For example, a commander could deny an adversary access to a network by cable cutting. Finally, information about the probability of a CWoS may enable efforts to establish a multidomain window of superiority or a window of opportunity, in which friendly forces take advantage of favorable conditions.

* “Branches” are “[t]he contingency options built into the base plan used for changing the mission, orientation, or direction of movement of a force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions and reactions” (Department of Defense 2024, p. 22).

A CWoS may be the direct or nth-order result of friendly actions. It may be the outcome of an exchange with an adversary, meaning that the adversary may get a vote in efforts to create a CWoS.

To choose actions that alter the chance or scope of a CWoS, commanders require a means to identify and predict it. Identification is an estimate of the chance of a CWoS at the current moment in time. A CWoS prediction is an estimate of the chance of a CWoS during a specified future period of time.

There is no current doctrinal guidance for identifying and predicting a CWoS. Intelligence products support the command staff's conceptual and detailed planning and the commander's decisions.* Current intelligence products do not seek to identify and predict a CWoS, although they do address some relevant cyberspace considerations, with particular attention to adversary capabilities, intentions, and actions.

The intelligence preparation of the operational environment (IPOE) (formerly called "intelligence preparation of the battlefield") supports operational planning and includes cyberspace considerations (Headquarters, Department of the Army 2019b, Appendix D). Army doctrine defines the following steps for integrating cyberspace considerations into IPOE: "define the [operational environment]," "describe environmental effects on operations," "[e]valuate threats and [high-value targets] . . . by performing critical factors analysis," and "determine threat courses of action" (COAs) (Headquarters, Department of the Army 2019b, p. D-1). Determination of threat COAs is done by incorporating data on historical threat COAs and identifying high-value cyberspace targets and "friendly networks that require protection" (Headquarters, Department of the Army 2019b, p. D-1). The purpose of this type of analysis is to "inform decisions and provide realistic assessments of operational and tactical risk. . . . This support assists the commander and staff in deciding when and where to concentrate sufficient combat power to defeat the threat while mitigating risk" (Headquarters, Department of the Army 2019a, p. 5-4).

The analysis reflects several doctrinal definitions. Cyberspace is defined as a domain within the information environment. The "information environment" is defined as follows:

[t]he aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning

* Conceptual planning involves "understanding the operational environment and the problem, determining the operation's end state, and visualizing an operational approach. Detailed planning translates the broad operational approach into a complete and practical plan" (Headquarters, Department of the Army 2019a, p. 3-3).

from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information (DoD 2024, p. 92).

The cyberspace domain has three layers: “the physical network, logical network, and cyber-persona” layer (Headquarters, Department of the Army 2019b, p. D-2).

Accordingly, cyberspace considerations include an itemization of significant cyber assets, possible access points to friendly networks, the Internet activity and cyber personas of key civil leaders and landowners, “data and information consumers in the [area of operations],” “weather, light, and illumination data,” a terrain analysis of the cyberspace domain using traditional methods (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment), and a list of nonmilitary groups and institutions that can influence the area of operations (Headquarters, Department of the Army 2019b, p. D1–D18). The analysis is threat focused; there is little consideration of the specific vulnerabilities of cyber assets and the impact on the mission if they are compromised or degraded.

3. Mission-Based Cyber Risk Assessments

The literature offers methodologies and tools on which to draw in developing a CWoS model and estimate. There is substantial literature on risk and specific literature on mission-based or mission-centric cyber risk assessment. This literature is relevant because a CWoS estimate can be seen as a risk assessment focused on the chance of a single impact: that execution of a tactical mission will be precluded by prohibitive interference in the cyberspace domain. However, the purpose and scope of a CWoS estimate differs from most of the existing examples in that it is intended to inform the multidomain decisions of a tactical commander, including decisions about trade-offs. Most examples are intended to inform decisions about systems rather than missions. At its broadest, the CWoS estimate would include an assessment of the negative impact of cyber actions or events on non-cyber systems, whereas the existing literature focuses specifically on cyber systems. Moreover, the tactical use case imposes specific requirements for and constraints on the methodology and model, which are not addressed in the examples we reviewed. The gaps and challenges of this literature (analyzed in Section 4) can suggest directions for future research.

3.1 Cyber Risk

There is wide-ranging literature on cybersecurity and information security risk assessment. “Risk” is defined by the National Institute of Standards and Technology (NIST) as follows:

[a] measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (National Institute of Standards and Technology 2012, p. B-9).

In this context, “likelihood” refers to a score produced by subject matter experts (SMEs), not a statistical function (NIST 2012, p. G-1, footnote 55).

The purpose of a cyber risk analysis is to inform decisions about risk mitigation and response given limited resources. NIST SP 800-30 *Guide for Conducting Risk Assessment: Information Security* states, “Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems” (NIST 2012, p. 1).

There are three tiers of risk assessment:

Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level). At Tiers 1 and 2, organizations use risk assessments to evaluate, for example, systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs. At Tier 3, organizations use risk assessments to more effectively support the implementation of the Risk Management Framework (i.e., security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring) (National Institute of Standards and Technology 2012, p. 1).

The guide defines a “risk assessment methodology” as comprised of a risk assessment process, a risk model, an assessment approach that populates the model, and “an *analysis approach* (e.g., threat-oriented, asset/impact-oriented, or vulnerability-oriented), describing how combinations of risk factors are identified/analyzed to ensure adequate coverage of the problem space at a consistent level of detail” (NIST 2012, p. 7). Risk models determine risk as a function of factors including “threat, vulnerability, impact, likelihood, and predisposing condition” (NIST 2012, p. 8). The guide further defines threats,

assets, vulnerabilities, likelihood, and impact, and describes ways in which assessment can be approached. The guide also offers tables to map ordinal scores of threats, vulnerabilities, and likelihood to real numbers to facilitate the analysis of ordinal data using mathematical operations for real numbers (which some approaches do). Risk is represented as a five-by-five matrix indexed by ordinal values for likelihood and impact (NIST 2012, p. I–1).

Although NIST SP 800-30 (NIST 2012) is advisory, not binding, it not only describes but shapes the field of existing cybersecurity risk assessment methodologies. The Federal Information Security Modernization Act of 2014 requires U.S. agencies to follow risk-informed cybersecurity procedures.* NIST cybersecurity standards are mandatory for civilian government agencies. Defense and intelligence agencies can set standards for mission-critical systems but may choose to align with NIST cybersecurity standards and guidance. NIST’s role as a standards setter makes its recommendations influential in both civilian and military organizations.

3.2 Cyber Risk to Missions

Within the cybersecurity risk literature, “mission-based cyber risk assessments” (MBCRAs)—sometimes called “mission-centric” or “mission-focused” cyber risk assessments—inform decisions as a function of the cyber risks to a mission. For DoD, “MBCRA is an analytical, iterative process that identifies, estimates, assesses, and prioritizes the risks of cyber effects to DoD operational missions” (DoD 2025, p. 15).

Although MBCRAs have in common an assessment of mission impact as a determinant of how to prioritize actions, they may differ in their purposes, the decision makers they serve, the decisions they inform, how they define missions, and their methods. Most MBCRAs are conducted to inform and prioritize decisions about systems, including the acquisition, design, development, testing, and evaluation of systems. However, MBCRAs may also be conducted to inform operational decisions taken by cybersecurity operators or mission commanders.

Differences in MBCRA definitions and methodologies led to efforts to map the methodological space, create criteria for the selection of an approach, consolidate and standardize methodologies, and identify best practices and areas for improvement. The Institute for Defense Analyses conducted comparative studies of DoD MBCRA methodologies for the test and evaluation community (Ambroso and Hutton 2017; Kuzio de Naray and Galvin 2020; Kuzio de Naray and

* The Federal Information Security Modernization Act of 2014, 44 U.S.C. §3533.

Buytendyk 2022a, 2022b). The Air Force Operational Test and Evaluation Center organized a meeting of Air Force organizations to create a single, standardized methodology, resulting in the creation of the Mission-Based Risk Assessment Process for Cyber (MRAP-C) (Monroe and Olinger 2020). The Naval Information Warfare Center Pacific conducted a comparative assessment of MBCRA Model-Based Systems Engineering Tools (McPhillips et al. 2022).

3.3 Mission Decomposition and Mapping

The purpose of the MBCRA determines the scope of the assessment and what kind of information is gathered. For example, an assessment that informs decisions about a specific system or set of systems traces the relationship of the identified system(s) to the mission to determine the impact of an adverse system event on the mission (“bottom up”).

In contrast, an assessment that informs decisions either about the conduct of a mission (similar to a CWoS estimate) or about all systems that support a mission must first trace the relationship of the mission to supporting systems to identify the systems of interest (“top down”). Once the supporting systems have been identified, they are typically prioritized based on the criticality of the functionality they provide and the mission task they support. The assessment will then proceed to investigate the impact of events affecting those mission-critical systems on the mission (bottom up). For DoD, this tracing of relationships from the mission to supporting systems is consistent with DoD’s broader approach to risk management through “mission assurance” (MA).

MA is a “process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions” (DoD 2024). DoD uses MA to identify, prioritize, and mitigate risk to mission execution across the enterprise (see DoD 2012; Office of the Under Secretary of Defense for Policy 2018, 2022; Chairman of the Joint Chiefs of Staff 2023).

MA prioritizes capabilities and assets as a function of their criticality to the mission. (Figure 1). First, the mission is identified and its tasks are itemized in “mission decomposition” (Chairman of the Joint Chiefs of Staff 2023, p. C1), which is sometimes called “mission mapping” (Jabbour and Muccio 2011). Missions are typically decomposed into tasks using task lists, such as the Universal Joint Task List or the Army Universal Task List. The capabilities and assets that support the mission tasks are identified, with attention to cross-

dependencies, external dependencies, and nth-order effects of failure (DoD 2012).

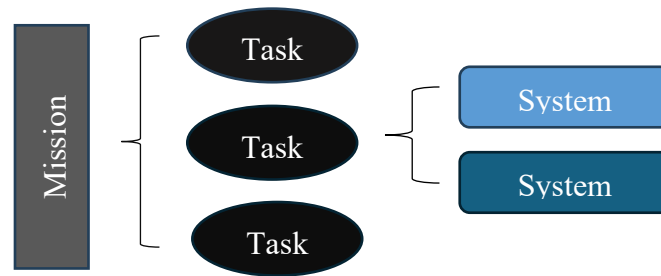


Figure 1. A mission is decomposed into tasks, tasks are ranked, and systems are mapped to tasks.

These capabilities and assets are then scored according to their importance to the mission, with higher-scoring capabilities and assets prioritized for attention. The terms “mission critical,” “mission essential,” and “mission enhancing” are often used to express descending levels of importance to the mission, and therefore of prioritization, although the terms are defined differently in different contexts (see Table 2 for one set of definitions).

Table 2. Mission impact criteria.^a

Term	Mission impact
Mission Critical	Prevents accomplishment of mission or leads to direct impact on mission failure; no work-around or alternative exists. Capability needed immediately to mitigate risk.
Mission Essential	Adversely affects the accomplishment of, or degrades mission accomplishment, and no acceptable work-around or alternative solutions exist; requirement is needed to maintain sufficient military capability or readiness and is needed no later than a specific date to prevent the loss/degradation of capability or readiness.
Mission Improvement	Employment of capability increases mission accomplishment or mitigates threats to mission and mission essential capability and work-around/alternative solution have been identified.
Mission Enhancement	Addresses enhancements not critical or essential for mission accomplishment; increases efficiency, addresses user/operator annoyance with system functions beyond a help desk or problem report to resolve.

^a Definitions quoted from Chairman of the Joint Chiefs of Staff (2019, p. 2).

The prioritized capabilities and assets are then assessed for vulnerabilities and gaps. Acceptable levels of risk are determined, and suggestions are made for risk remediation. Finally, both the conduct of the process and the operational status of the task-critical assets are monitored (Chairman of the Joint Chiefs of Staff 2023).

Because prohibitive interference in cyberspace would necessarily affect some mission-critical system, a CWoS analysis must map the mission to supporting systems as part of the problem definition. There are multiple methodologies for decomposing and mapping missions and mapping them to cyber assets, which,

following joint doctrine, some literature calls “mapping key cyber terrain” (e.g., see Schulz et al. 2015; Heinbockel et al. 2016; Guion and Reith 2017; Thompson and Harang 2017; Barreto and Costa 2019; Martínez et al. 2021). There are also tools that visualize mission cyber dependencies, such as the U.S. Army Space and Missile Defense Command [SMDC]’s Cyber Operational Readiness Tool (CORT) and Johns Hopkins Applied Physics Laboratory’s DAGGER (U.S. Army Space and Missile Defense Command n.d.; Dagger LiveLab 2019; Jiang et al. 2022).

The work by Snyder et al. (2022) outlines some of the features of mission mapping that make it difficult, especially in the cyber domain. These include the need for scalability; the rate of change of concepts of operations, systems, and threats; the dependence of asset criticality on a particular scenario; the need for explainability; the fact that, in the cyberspace domain, redundancy (here, meaning a second, identical, and identically configured system) does not make a system more robust;^{*} and the fact that mission failure can be caused not only by damage but also by loss of control of an asset (Snyder et al. 2022, p. viii). In cyberspace, even temporary loss of control can cause mission failure.

3.4 MBCRA for System Decisions

The scope of most MBCRAs is one or more cyberspace systems. These MBCRAs are intended to inform decisions about the systems, prioritizing risk mitigation based on the impact of system degradation, disruption, or compromise on a mission or organization. These analyses support the acquisitions, research and development, systems engineering, and test and evaluation communities, which decide whether to buy or how to design, use, test, or improve cyberspace systems. All DoD acquisition programs are advised to perform a MBCRA as part of the test and evaluation process (DoD 2025, p. 15). Two examples of this type of system-focused MBCRA are the MRAP-C and the DoD Cyber Table Top (CTT).

3.4.1 MRAP-C

MRAP-C is designed to support system requirements, design, “development, risk management, programmatic decisions, and test through actionable summaries of system-specific vulnerability exploitation in the form of vignettes. . . . MRAP-C provides the path to deliver computational components that can survive both combat usage and adversary attacks” (Air Force 2021, p. 8–9). After the scope of the analysis is determined as a set of systems under test, MRAP-C maps possible

^{*} This claim should be qualified to say that redundancy does not necessarily contribute to robustness against cyberspace attacks. This depends on the type of cyberspace attack.

attack vectors from entry points in the systems to the first reachable system nodes and then to system nodes and connections that handle critical information. For each combination of entry point and initial system node, SMEs score the mission impact of exploitation, the technical likelihood of exploitation, and the threat capabilities for exploitation from one to five. These ordinal scores are multiplied to give a score of overall risk (Air Force 2011, p. 75–81). High-risk combinations are identified from scores, and vignettes are drafted describing exploitation and mission impact for these combinations, which are then the subject of table-top exercises, recommendations for mitigation, and reports. MRAP-C envisions that the analysis, vignette-building, testing, and report writing will involve a team of experts.

3.4.2 DoD Cyber Table Top

“The purpose of the [Cyber Table Top] process is to provide Program Managers, [Information System Security Managers], [Information System Security Engineers], system engineers, testers, and other analysts with actionable information on cyber threats to mission execution” (Director of Defense Research and Engineering (Advanced Capabilities) et al. 2021, p. 5). Under CTT, the scope of the exercise is defined as a set of systems or functions of interest, and a mission is selected from among those that the system or set of systems supports. SMEs are divided into a team that simulates executing the operational mission and an opposing force team that simulates attacks on the systems supporting the operational mission. The teams draw on intelligence and systems documentation. A mission impact methodology is selected, and the SMEs provide an ordinal score of mission impact from one to five. A likelihood methodology is selected, and the SMEs provide an ordinal score of likelihood from one to five. The output of the process is a five-by-five risk matrix as described by NIST SP 800-30 (NIST 2012) and recommendations to improve “resistance and resilience to cyberattacks.” These include recommendations to improve test events and operator, defender, and maintainer training and to assess “the contributing effects and impacts of supporting platforms, systems, and stakeholders in a mission context” (Director of Defense Research and Engineering (Advanced Capabilities) et al. 2021, p. 5). Notably, the guide directs that exercise organizers select methodologies for analysis; it does not provide methodologies for analysis or discuss them in any detail. However, the worksheets provided to support scoring include considerations such as “operational impact,” “mission impact,” “attack cost/level of effort,” “attack success likelihood,” and “capabilities or mitigations in place.”

3.5 MBCRA for Decisions about Missions

There are also MBCRAs that seek to inform the decisions of a military commander. This research has identified only two examples of MBCRAs for warfighting decisions: the U.S. Cyber Command Risk Assessment Methodology (USCYBERCOM RAM) and CORT.

3.5.1 USCYBERCOM RAM

The USCYBERCOM RAM is used to assess cyber risk to the DoD Information Network (DODIN) (United States Cyber Command 2016). The results are used to inform defensive cyberspace operations.

This qualitative assessment methodology is based on NIST SP 800-30 (NIST 2012). Threat, vulnerability, and impact are scored from “very low” to “very high.” The scores are the results of assessments drawing on available intelligence to answer provided questions. For example, a consideration for mission impact is whether the impact is local, regional, or global; another is whether the impact is temporary or permanent. These scores are then mapped to an ordinal risk level using a provided “decision support matrix” (table) to prioritize risk mitigation. Risk assessments are also accompanied by an assessment of confidence level as low, medium, or high.

The USCYBERCOM RAM is intended to be conducted sequentially, with an initial assessment within 4 to 24 h of the occurrence of an event, followed by update assessments every 24 to 72 h. The methodology is designed to “assess large network environments within a limited amount of time” (United States Cyber Command 2016, p. 5).

3.5.2 CORT

CORT is a government off-the-shelf tool developed for the U.S. Army Materiel Command and further developed by the SMDC (U.S. Army Space and Missile Defense Command n.d.). While the USCYBERCOM RAM analyzes risks to a cyberspace system (the DODIN) to inform a mission commander whose mission is to protect it, CORT’s focus is on the risk to the operational mission itself. It uses a mission assurance approach to decompose missions and the SMDC key terrain-cyber mapping methodology to identify and map key cyber terrain. It then visualizes the results for commanders.

Under the dashboard, CORT relies on existing risk management frameworks. It uses the following: the U.S. Army Security Control Assessor-Validator risk assessment process for vulnerability; the U.S. Army Cyber Command Activity

Capability Access Resources Expertise (ACARE) Model for threat (e.g., see Pomerleau 2017); the USCYBERCOM RAM to combine risk factors to develop scores for vulnerability, threat, and impact; and NIST SP 800-30 (NIST 2012) to convert the ordinal scores from the USCYBERCOM RAM to numbers on which it performs mathematical operations.

3.6 Mission-Centric Risk Analyses

In addition to DoD MBCRAs, there is academic and gray literature on methods and tools for assessing the mission impact of cyber events. Although this research did not find any literature proposing methods to estimate the existence of a CWoS per se, some of the approaches reviewed could inform the development of a methodology or tool to produce a CWoS estimate. A full literature review is outside of the scope of this paper.

One strand of literature calls for creating “cyber situation(al) awareness” of mission impact to inform cybersecurity decisions, while other literature is rooted in mission assurance (e.g., see Saydjari 2004; Jajodia et al. 2010; Jabbour and Muccio 2011; Noel and Heinbockel 2015; Peterson 2016). The methodologies map systems to missions and illustrate the mission consequences of system compromise or failure. Information may be entered manually or produced by sensors or data streams. Manual entry allows the exploration of hypothetical scenarios.

The initial step is to map mission cyber dependencies. Guion and Reith (2017) is an older literature review of tools and approaches for cyber mission. It noted that most of the reviewed tools require substantial data input and the creation of mission models takes weeks, although this time can be reduced if the tool allows the reuse of objects in different mission models. The review concluded that the tools do not account for the fluidity of missions, do not consider time as an important determinant of system criticality, and do not model the effects of information compromise on missions.

Bakirtzis et al. (2017) proposed MISSION AWARE, a methodology for informing system designers of the impact of their decisions on the vulnerability of the mission to cyberattacks. It begins by gathering input from stakeholders, including “supervisory staff, commanders, operations staff, end users, and subject domain experts” (Bakirtzis et al. 2017, p. 2). The input includes information about “mission goals, objectives, unacceptable outcomes, expectations, and procedures,” (Bakirtzis et al. 2017, p. 3) as well as possible threats. Then the “target mission, behavior, and architecture” are modeled, including “functionality, mission constraints and requirements of [cyber-physical systems],

admissible behaviors, restrictions, and hazards” (Bakirtzis et al. 2017, p. 2). Critical system components and their relationship to the mission are identified. The methodology uses Systems Theoretic Process Analysis for Security, which maps hardware and software to mission requirements and represents unacceptable impacts and the conditions and circumstances that lead to them. Simultaneously, relevant information on vulnerabilities and threats is gathered from public databases. Models of mission requirements, system function, system structure, mission specification, and attack vector space are produced and represented in Systems Modeling Language. Finally, a determination is made of whether the risks, vulnerabilities, and threats can have a significant impact on the mission by using graphical modeling. Possible attack chains across the system structure are identified to capture the impact of sequential attacks. Paths that result in mission impacts are reported to stakeholders. The approach was evaluated by application to a military use test case of a reconnaissance mission with an unmanned aerial vehicle.

Barreto and Costa (2019) proposed Cyber-ARGUS. Cyber-ARGUS is a mission assurance framework to evaluate how actions in the cyberspace domain affect operations. An analyst models the mission, supplements the model with relevant mission and cyber data, capturing these in a knowledge base, and evaluates the mission impact of cyber events. Cyber-ARGUS was evaluated on a simulated air traffic control case study in a test-bed environment.

The mission is represented as an impact graph that represents dependencies between the mission, tasks, services, and cyber assets. Cyber-ARGUS adopted the DoD Architecture Framework (DoD Deputy Information Officer 2010) as a mission ontology to allow reuse of all or parts of mission models, extended to include more detailed cyber domain concepts. A mission is modeled as a set of tasks united by a common purpose. Tasks are carried out by performers using resources. One type of performer is a service provided by a cyber asset, which is a resource. Resources have vulnerabilities, which can be exploited by threats. Events are triggered by a set of conditions. The tasks, the relationships between them, and the performers are represented using Business Process Model Notation, a graphical notation. The model is further developed with information about cyber assets and their provided services pulled from a services database or discovered using a network discovery tool. Data about system vulnerabilities is pulled from a database, such as the one used by Open Vulnerability Assessment Scanner (OpenVAS), and stored in the knowledge base, supplemented with a calculated Common Vulnerability Scoring System (CVSS) score.

Each node in the Impact Graph becomes a node in a Bayesian network Reasoning Model that is used to assess mission impact with uncertainty. The Bayesian

Reasoning Model uses ranked nodes as described by Fenton et al. (2007), where nodes represent discrete ordinal variables mapped to intervals to simplify the calculation of probability tables. Edges represent simple, AND, and OR relationships. The node weights reflect the importance of the node to the mission and are added manually by the analyst or extracted from service-level information collected by the analyst. Nodes have “infrastructure capacity,” the capacity to deliver required functionality, which is a value based on the node’s security index and exploit index. The security index is based on aggregated and normalized sensor data provided by the mission analyst and reflects node confidentiality, integrity, and availability. The exploit index reflects the existence of attack paths across node vulnerabilities. The model is updated on an ongoing basis with data from devices such as firewalls, intrusion detection systems, and security log systems.

Finally, in response to cyberattacks or other events, the model and associated information are used to generate impact graphs that reflect the dependence of the mission on assets and the influence each node has on the mission, from the confidentiality, integrity, and availability perspective. The analyst decides which tasks to assess and the scope of the analysis. At the highest level, the impact graphs can be aggregated to model belief in mission success using a Bayesian network, while a node-level view would provide an explanation of the results.

Javorník et al. (2019) proposed a method to inform cybersecurity operator decisions as a function of enterprise mission risk, framing the problem as one of choosing an optimal system configuration given decision-maker preferences. The proposed method decomposes the mission into mission-supportive processes, which in turn are mapped to supporting informational technology processes, and then to supporting cyber components. Because there are multiple possible configurations of components to achieve missions, mission configuration alternatives are expressed using AND/OR nodes. The interests of decision-makers are expressed as utility functions and constraints that define the set of acceptable mission configurations. Bayesian attack graphs are developed by drawing on the mission model and publicly available data about system vulnerability such as from the National Vulnerabilities Database (NVD). The unconditional probabilities of attack are generated from CVSS Attack Complexity scores. Finally, optimal reconfigurations for mission resilience and countermeasures are recommended, given decision-maker constraints and the current security situation.

There is a large body of work assessing risk in cyberspace and applying those assessments to systems and missions. However, this report identified only a few mission-focused approaches that closely relate to the identification, prediction,

and creation of a CWoS for a tactical mission. The most CWoS-aligned MBCRA tool found in this research is the Cyber Operational Readiness Tool, which seeks to inform command decisions, offers the user situational awareness of mission impact, and visualizes network layout and status. Academic research yielded Cyber-ARGUS, which offers a thorough investigation of cyber risk to mission and is well aligned, in principle, to the goals of CWoS estimation. The existing work may be usefully leveraged to develop a CWoS estimation methodology.

However, neither offers the complete set of desired capabilities for CWoS estimation for tactical missions. Neither CORT nor Cyber-ARGUS capture the entire scope of a CWoS as expressed in Table 1. They do not model time or mission phase and cannot be used to make predictions of mission impact at a future time. CORT does not represent and propagate uncertainty. The CORT backend depends on current mainstream cyber risk assessment approaches that depend on ordinal scoring by SMEs and, in some cases, map ordinals to real numbers to perform mathematical operations. No methodology reviewed sufficiently addresses the constraints at the tactical edge in time, data, personnel, and computational resources.

The review of existing work was nevertheless useful both in highlighting desired capabilities, suggesting approaches, and helping to better formulate the problem of developing a methodology for CWoS estimation for tactical missions. The following section describes the challenges in more detail.

4. Gaps and Challenges

This research did not find any methodology or tool to identify, predict, or create a CWoS for a tactical mission. However, the review highlights gaps in the literature, desired qualities of a CWoS methodology, and the considerable challenges that must be overcome. Current methodologies differ in purpose and scope and do not accommodate the constraints at the tactical edge. Lack of hard data is the principal challenge in developing a CWoS model and is the reason why so many cyber risk methodologies rely on SME scoring, which in turn may have implications for the explainability and defensibility of estimates.

A CWoS estimate is intended to be used to inform warfighting decisions, a high-risk use case, and must be both explainable and defensible. The analytic cost of existing methodologies is considerable and exceeds the resources at the tactical edge. Mission decomposition and mapping may be even more analytically costly and difficult at the tactical edge. A CWoS model will need to look beyond cyber vulnerabilities and incorporate information about environmental variables that could affect cyberspace systems. It will need to be able to model changes in

relationships over time and over phases of a mission. Uncertainty over the CWoS estimate must be represented, propagated, and communicated. Finally, it must be capable of verification and validation.

Purpose. Most of the existing literature on MBCRAs and mission-centric cybersecurity advances methodologies that are not intended to support the needs and decisions of a tactical commander and staff. A CWoS methodology should inform and facilitate command decisions such as decisions to redefine a mission or change its timing or to trade cyber risk for other benefits, as well as decisions to assign different systems to support the mission. Most MBCRAs support decisions about the design, acquisition, use, or maintenance of systems, while most of the mission-centric cybersecurity literature is focused on informing the decisions of cybersecurity personnel. As previously discussed, this affects how the analysis is scoped, whether top-down mission mapping is conducted, the type of information that is modeled, and the sensitivity of the modeling process to some of the requirements and constraints relevant to the tactical use case.

Scope. In addition, the scope of a CWoS estimate is broader than that of most of the analytic methods examined. A CWoS estimate is not limited to consideration of the cyber vulnerabilities of cyber systems but includes adverse events or kinetic actions that affect mission-critical cyber systems and the effects of cyber actions on non-cyber systems.

Data availability and quality. The conduct of an MBCRA requires a substantial amount of data, which increases with the complexity and size of a mission. Focusing only on information required from users for MBCRAs for the test community, the Institute for Defense Analyses summarized the data required by 25% or more of MBCRA processes studied (Kuzio de Naray and Buytendyk 2022b, p. 2-3 and 2-4). This includes the information about the mission and tasks required for mission decomposition and mapping; information about the systems, including system architecture, components, functions, protocols, and vulnerabilities; and information about threats, including adversary means, capabilities, opportunities, tactics, and intent (Kuzio de Naray and Buytendyk 2022b, p. 2-5). Data may be required from model developers, maintainers, and testers as well as users.

Lack of data is a frequently mentioned challenge (Cremer et al. 2022) and a motivation for reliance on SME judgments and modeling assumptions. Data may not be available because it does not exist, has not been collected, is not of sufficient quality or is not comparable, or is not available to those charged with conducting an analysis for reasons of classification or lack of authorities (e.g., Snyder et al. 2021, p. 21) (lack of authorities and jurisdiction as an impediment

to information access). Granular data regarding the design or manufacture of DoD-purchased systems may be proprietary or unavailable, depending on the contract and the relationship between the prime and any subcontractors or suppliers. It is also difficult to find data useful for predicting the actions of adversaries. Many actions or events that could negatively affect cyberspace systems are rare, and it is difficult to find data to support estimates of the chance of rare events or even to itemize rare events to seek data about them.

There is some public data on known cyber vulnerabilities of systems, such as that in the NVD, although the vulnerabilities of Army-specific tactical systems may not be represented in such databases. Partner vendors and researchers report discovered vulnerabilities and exploits to the Common Vulnerabilities and Exposures (CVE) Program (CVE 25 Years 2025). NIST then draws on the CVE list to populate the NVD after enriching the data and putting it in a format suitable for ingestion by automated cybersecurity programs (National Vulnerability Database – General Information. 2024). However, even this data is partial. The Exploit Database (2025) is another public database of exploits, maintained by OffSec, an information security training company. Chen (2020) found that only 26% of public exploits in the Exploit Database had mapped CVE numbers, and, of those, 80% were published before the CVEs were published. Additional sources for exploits include Metasploit and Pastebin. Public data on vulnerability does not share a standard format, leading to multiple efforts to use machine learning to ingest unstructured cyber threat intelligence (e.g., see Abdeen et al. 2024; Schwartz et al. 2024).

An important consideration regarding data availability is concept drift, the tendency of relationships between variables to change over time. Cyberspace reflects human behavior, which is dynamic, causing collected data and models to expire. This means that any method to identify or predict a CWoS must have a way of identifying and discounting information that has aged out. It may be difficult to ensure that SME judgment is keeping pace with the rate of change.

It is not only threats and vulnerabilities that change over time, but also missions, tasks, and supporting systems, which can change midstream and would make a CWoS estimate obsolete. This implies that any model or tool must be able to produce such estimates quickly. It also raises the question of how sensitive the model should be to factors that might change quickly. If the rate of change is greater than the speed of data collection and prediction, useful prediction is impossible.

Explainability and defensibility. A CWoS estimate is intended to inform a tactical warfighting mission. Accordingly, a model or method that identifies or

predicts a CWoS should be explainable and defensible. Its assumptions and conclusions should be clearly articulated and supported by evidence or reasoning that allows the mission owner to decide whether to have confidence in the results. It should also be reproducible (“different experts...produce the same results from the same data”) and repeatable (future assessments are “consistent with and hence comparable to prior assessments”) (NIST 2012, p. 7 footnote 19).

Perhaps in part because of data scarcity, commonly used cyber risk assessment methodologies may not meet these criteria. Reliance on SME scores, poorly documented or proprietary methodologies, the lack of methods for compensating for SME bias, or reliance on external data of uncertain quality may reduce explainability and defensibility. Some cyber risk methodologies map ordinal scores to real numbers and add, multiply, or divide them. This practice is encouraged by NIST SP 800-30 (NIST 2012), which provides tables that map ordinals to real numbers for this purpose. However, because the set of possible mappings is infinite (“low,” “medium,” and “high” could be mapped to 1, 2, and 1000 or 1, 2, and 3 with equal justification), the outcome of such operations is a consequence of both the original ordinal scores and the arbitrary mapping choice (Thomas 2019; Spring et al. 2021). This may make model results inexplicable and indefensible.

Analytic cost. A viable analytic framework or tool for identifying and predicting a CWoS must take into account the cost of analysis in time and resources. Costs include those associated with the collection and cleaning of data, recruitment and training of personnel, model building and maintenance, required computational resources, and, because of data sensitivity, appropriately cleared personnel, networks, and storage.

Most MBCRAs are analytically costly. The DoD CTT Guide estimates that preparation and conduct of the exercise would take a team of SMEs 63 to 155 days (Director of Defense Research and Engineering (Advanced Capabilities) et al. 2021, p. 7). The MRAP-C process takes a team of SMEs an average of 24 weeks for the first iteration (Monroe and Olinger 2020, p. 231).

Pomerleau (2017) reported that Cyber Protection Teams (CPTs) from U.S. Central Command (CENTCOM) engaged in IPOE were applying the ACARE model, scoring adversaries from one to five on activity, capability, access, resources, and expertise. The model was used to prioritize adversary groups for defensive operations. However, because of the large number of adversary groups, the work of synthesizing the data reduced CPTs to no more than two missions per year. CENTCOM modified the model by adding a variable to capture intent (Pomerleau 2017). By focusing the analysis on actors with offensive intent,

analysis time was reduced by 85% and the number of missions that CPTs could complete increased substantially. The model was subsequently adopted by the U.S. Northern Command and U.S. Africa Command.

The Air Force has also wrestled with analytic cost. In 2015, the Air Force organized Mission Defense Teams (MDTs) to use cyber mission assurance to assess the risk to mission presented by the vulnerabilities of weapons systems (Snyder et al. 2021). MDTs had difficulty recruiting and training personnel and retaining trained personnel. RAND reported that MDTs “found the training nearly useless for conducting a functional mission analysis . . .” (Snyder et al. 2021, p. 36) because of lack of examples, lack of realism, lack of support (no reachback), lack of skilled practitioners, and lack of quality control.

In response to these challenges, the Air Force moved to a more centralized approach. In 2022, there were 84 MDTs spread across Air Force bases (Franks 2024). In 2024, the Air Force reduced the number of MDTs to 19 (Franks 2024). The new approach relied on local sensors with centralized data and data analysis.

“Across the service’s six big data platforms obviously there’s been many successes, but the one closest to my heart is ELIXIR,” Gen. Snoddy said.

“That is 16th Air Forces’ cybersecurity big data platform and is how we maintain enterprise level data. We can actually query against that data as enterprise to look for adversarial [cyber] activity. We have big data scientists, whether they be from the industry or inside the department or otherwise, that have helped develop ways to query against that data. We look for anomalous activity that can clue us in to adversary activity that we frankly could never see on an installation-by-installation basis before.” (Underwood 2024)

Analytic cost is a particular concern at the tactical edge, where time, computational power, and trained personnel are limited. For detailed day-to-day planning, the Future Operations planning cell, which has the longest time horizon of the staff planning cells, generally has up to 48 h at battalion, up to 72 h at division level, and up to 96 h at the corps echelon (Corbett 2024).

The two MBCRAs for mission decisions were designed to be less time consuming. The USCYBERCOM RAM was designed to be performed sequentially within a 72-h window and there is no expectation of the assembly of a large team of SMEs. However, this is likely to come with its own trade-offs with respect to reusability, replicability, and defensibility of results. CORT is automated and integrates vulnerability information from a data feed. This would greatly speed up the production of estimates, although Guion and Reith (2017) noted that mission mapping alone can take weeks.

Mission decomposition and mapping. The fluidity of tactical missions and the analytic cost of mission decomposition and mapping have already been noted. In addition, unless mission decomposition and mapping use a common ontology, each analysis is a bespoke creation of the mission owner and analyses cannot benefit from each other. Forcing reliance on the joint and service universal task lists may be a way to create interoperability, but the task lists are not at the level of granularity required for system mapping. One possible solution is to provide default templates for common missions, but there is a tradeoff between standardization and suitability for individual missions. At the same time, tactical mission owners and staff may not have full visibility and awareness of, or access to data about, their own cyber dependencies, whether at a granular level or outside their unit. This raises the question of the value of partially informed CWoS estimates.

Time and mission phase. A CWoS estimation method for tactical missions must be able to capture and represent qualities and relationships that change over time. This is necessary to enable prediction of a CWoS for the purpose of mission planning. In addition, it must model mission phases. The criticality of assets to mission execution may depend on the phase of a mission, such that compromise of a given cyberspace system in one phase constitutes prohibitive interference but is inconsequential in other phases.

Environmental variables. Environmental variables may affect the likelihood of prohibitive interference in the cyberspace domain or the extent of impact and so must be considered for modeling. For example, physical effects on cyberspace systems could be influenced by weather, whereas the probability of prohibitive interference may depend on the identity and capabilities of an adversary.

Uncertainty. The existence of a CWoS is subject to both aleatory and epistemic uncertainty. Commanders require a defensible measure of the uncertainty of the CWoS estimate to know how much confidence to place in it. If there are many variables whose values are uncertain, the uncertainty of the final estimate may be so great that the estimate is not useful.

Most examined mission-centric or mission-based cyber risk assessments do not model uncertainty. The USCYBERCOM RAM requires a score that reflects the level of confidence in the results (“low,” “medium,” or “high”). However, the basis for such scores is not clear.

Verification and validation. Mission-centric and mission-based cyber risk assessments use models to produce risk assessments. A model is “[a] physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process” (Office of the Under Secretary of Defense for Research

and Engineering 2024, p. 10). DoD requires that models be verified and validated prior to accreditation for use (Office of the Under Secretary of Defense for Research and Engineering 2024, p. 3). “Verification” is “[t]he process of determining that a model, simulation, or distributed simulation, and associated data accurately represent the developer’s conceptual description and specifications” (Office of the Under Secretary of Defense for Research and Engineering 2024, p. 11). “Validation” is “[t]he process of determining the degree to which a model or simulation and its associated data are an accurate representation of the real world from the perspective of the intended uses of the model” (Office of the Under Secretary of Defense for Research and Engineering 2024, p. 11). “Accreditation” is “[t]he official certification that a model, simulation, or distributed simulation is acceptable for use for a specific purpose” (Office of the Under Secretary of Defense for Research and Engineering 2024, p. 9). Verification and validation are not afterthoughts. They are performed throughout the lifecycle of the model or simulation, including in development (Office of the Undersecretary of Defense for Research and Engineering 2011, p. 19). They are particularly important for models used to make high-risk decisions, like a model used to produce a CWoS estimate.

In the ideal case, models are validated by checking their predictions against real-world data. But cyber risk models would be challenging to validate. They involve modeling human behavior; rare events, such as adversarial cyberspace actions; and unique events, such as the impact of a cyber compromise on a specific mission. Data is scarce and uncertainty is high. When models cannot be validated against real-world data, other methods are used, including face validation by SMEs, comparison of model performance to that of other models, and piecewise validation (Department of the Army 1999). However, these methods of validation may have less evidentiary value in the cyberspace domain, which lacks unbreakable laws like those of physics.

It is not always clear how or whether existing mission-centric and mission-based cyber risk models are validated or how their outputs relate to objective data. Models assess risk as a function of likelihood and impact and often include considerations of threats and vulnerabilities. NIST SP 800-30 (NIST 2012) does not define “likelihood”; “impact” scores are necessarily subjective; and “threat” is an abstract, unobservable construct.

Again, lack of data is currently the principal challenge. Assuming requisite data is identified or produced to allow modeling, the development of a CWoS methodology would likely involve tradeoffs between desired capabilities given constraints at the tactical edge.

5. Conclusions and Future Directions

There does not appear to be existing work that meets the requirements and constraints of the tactical commander seeking to identify, predict, or create a CWoS. A CWoS estimate could be considered as a type of mission-focused cyber risk assessment that is concerned with only one possible impact: the failure of mission execution due to prohibitive interference in the cyberspace domain that affects mission-critical systems. Accordingly, this work is an estimate of likelihood, and it considers the likelihood without consideration of cause. Future work should focus on assessing advantage as an important predictor.

Production of a CWoS estimate requires a definition of successful mission execution that identifies mission-critical tasks and the standards to which they must be performed. Like other mission-based risk approaches, it also requires an approach to mission decomposition and mapping and a mapping of supporting systems. It is possible that this will be prohibitively time-consuming for tactical commanders and their staff. One possible solution is the creation of mission templates that could be used off the shelf or tailored by mission owners.

However, no estimate can be developed without data. Data is a prerequisite for modeling, and the lack of data is the greatest barrier to producing a CWoS estimate. The broader the scope of the model and the rarer the events that are modeled, the more data is required. Some types of risks to cyberspace systems, such as jamming, are relatively common, whereas others are rare or never-before-seen, but potentially highly impactful. The lack of hard data is one reason why most mission-based, cyber-risk approaches rely on SME judgments. However, this introduces problems of defensibility, explainability, and reproducibility. It is also not possible at the tactical edge.

Such data would require a common ontology for actions and events that affect missions from cyberspace. No such common ontology exists, but there are several that have been developed for data exchange for simulations that could perhaps be leveraged (e.g., Cyber Data Exchange Model (DEM) Product Development Group 2024; Dignitas Technologies 2022; Simulation Interoperability Standards Organization, Inc. 2024).

Whether it is possible to collect such data to build a model is an open question given the rate of concept drift. A better understanding of the modeled processes and their rate of change is needed. A typical example in cyberspace is the rate of new vulnerability discovery and time frames for system patching. However, in cyberspace, long-forgotten vulnerabilities can reemerge, making older data relevant once more.

If data were available, a defensible CWoS estimate could be developed using mathematics. Given the high-risk use case of the CWoS estimate, it must be done in such a way as to propagate and convey uncertainty to the commander. A Bayesian statistical approach may be well suited. Bayesian approaches have been used to model cybersecurity risk and mission risk previously, as in Cyber-ARGUS. A Bayesian approach would also permit the incorporation of diverse forms of existing knowledge, including SME judgments, in the form of a prior probability model (“prior”) (Johnson et al. 2022). When data are available from observations, this model can then be updated to a posterior probability model (“posterior”) based on a likelihood function.

Because Bayesian statistics produces probability distributions, uncertainty is always represented. Predictive model components could be developed where there is insufficient data for a causal model, but a causal model is needed to support commander efforts to create a CWoS.

A Bayesian approach is not a panacea. There are still assumptions that underpin Bayesian models, such as the choice of priors. In theory, if sufficient observational data is obtained for updating the model, the choice of prior will not matter. However, without such data, a Bayesian model will simply reflect the original prior, which may be wrong. If the prior is not informative, the associated uncertainty may be too great to make estimates valuable for command decisions.

Bayesian inference can also be computationally costly. The cost can quickly become prohibitive for more complex models. This may require the use of less computationally intensive imprecise probability methods, which would generate greater uncertainty in the final estimate.

Assuming that a model can be developed that is computationally tractable, methods must be developed to minimize computational and analytic cost at the tactical edge. For example, commanders could be given reach back to a library of prebuilt missions and models, which they would then populate with data specific to their missions to produce a CWoS estimate. However, this would limit the 1) ability to customize CWoS estimates for different missions, with different objectives, 2) criteria for successful mission execution, and 3) environmental conditions supported by different cyber systems. The use of templates could make unit actions more predictable, whereas updating the model with local data could cause different units with the same missions to have different assessments of possible prohibited interference in the cyberspace domain.

It may also be possible to reduce computational costs by modular modeling. Like object-oriented programming, breaking a complex model into smaller pieces that feed upward to a final CWoS estimate would allow modelers to work in parallel

and could minimize the cost of model updates. A well-defined interface would also allow the overall model to be agnostic to changes within modules. Although validating a CWoS model may be difficult because of data scarcity, a modular model may facilitate piecewise validation (validation of submodules). However, because modularity implies independence, further research is required to determine what independence assumptions can be made. Alternately, it would be possible to forego independence assumptions at the cost of greater uncertainty in the final estimate.

Model development and updating can also require substantial human intervention and judgment. The problem definition may change as missions change and supporting systems are lost or swapped out, as more is learned about environmental conditions, or as adversaries change their behavior. To be useful, any methodology for generating CWoS estimates and predictions must facilitate rapid problem redefinition as well as rapid estimation. Automated modeling will be required to the extent feasible, and the right level of granularity must be chosen. A CWoS model intended to inform command decisions needs to be modeled only to the level that would affect or be affected by those decisions.

These challenges and options can be explored in future research. It is unknown whether a model can be developed that meets the needs of tactical commanders subject to their constraints. Accordingly, the initial effort to estimate the existence of a CWoS must be very modestly scoped and data must be collected to support it. The result may be a more limited, but more defensible and useful, model.

6. References

- Abdeen B, Al-Shaer E, Singhal A, Khan L, Hamlen KW. SMET: semantic mapping of CTI reports and CVE to ATT&CK for advanced threat intelligence. *J Comput Sec.* 2024;1:1–20. <https://doi.org/10.3233/JCS-230218>
- Air Force. Mission-based risk assessment process for cyber (MRAP-C) guidebook. Air Force (US); 2021.
- Ambroso MA, Hutton RT. Comparative review of DoD mission-based cyber risk assessment methodologies. Institute for Defense Analyses (US); 2017 Dec. Report No.: P-8736.
- Bakirtzis G, Carter BT, Fleming CH, Elks CR. MISSION AWARE: evidence-based, mission-centric cybersecurity analysis. *arXiv*; 2017 Dec 5. *arXiv.1712.01448*. <https://doi.org/10.48550/arXiv.1712.01448>
- Barreto AB, Costa PCG. Cyber-ARGUS - a mission assurance framework. *J Netw Comput Appl.* 2019;133:86–108. <https://www.sciencedirect.com/science/article/pii/S1084804519300451>
- Chairman of the Joint Chiefs of Staff. Requirements management process for mission partner environment. Joint Chiefs of Staff (US); 2019. Document No: CJCSI 6290.01.
- Chairman of the Joint Chiefs of Staff. Mission assurance construct implementation. Joint Chiefs of Staff (US); 2023. Document No.: CJCS 3209.01A.
- Chen J. The state of exploit development: 80% of exploits publish faster than CVEs. Palo Alto Networks; 2020 [accessed 2024 Aug 29]. <https://unit42.paloaltonetworks.com/state-of-exploit-development/>
- Corbett M. U.S. Army Cyber Institute at West Point. Personal communication, 2024 Sep 17.
- Cremer F et al. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap R I-ISS P.* 2022;47(3):698. <https://doi.org/10.1057/s41288-022-00266-6>
- CVE 25 Years. Frequently asked questions (FAQs). 2024 The MITRE Corporation; c2025 [accessed 2024 Aug 29]. <https://www.cve.org/ResourcesSupport/FAQs>

Cyber Data Exchange Model (DEM) Product Development Group. Reference for cyber data exchange model (DEM) base objects, networks, effects, & specifications (BONES). Simulation Interoperability Standards Organization, Inc.; 2024. Report No.: SISO-REF-072-2024. https://cdn.ymaws.com/www.sisostandards.org/resource/resmgr/reference_documents_/siso-ref-072-2024.pdf

Dagger LiveLab. Mission impact situation awareness modeling and visualization. Johns Hopkins Applied Physics Laboratory; 2019. <https://www.jhuapl.edu/dagger/documents/DaggerFactSheet.pdf>

Department of the Army. Verification, validation, and accreditation of Army models and simulations. Department of Defense (US); 1999. Pamphlet No.: Pamphlet 5-11.

Dignitas Technologies. CyberBOSS. Dignitas Technologies, LLC.; c2022 [accessed 2025 Apr 17]. <https://www.dignitastechnologies.com/cyberboss>

Director of Defense Research and Engineering (Advanced Capabilities), Deputy Director for Engineering, Deputy Assistant Secretary of Defense Developmental Test, Evaluation, and Assessments. The Department of Defense cyber table top guide, version 2.0. Department of Defense (US); 2021. <https://www.cto.mil/wp-content/uploads/2023/06/DoD-Cyber-Table-Top-Guide-v2-2021.pdf>

[DoD] Department of Defense. Mission assurance strategy. Department of Defense (US); 2012. https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf

[DoD] Department of Defense. DoD dictionary of military and associated terms. Department of Defense (US); 2024.

[DoD] Department of Defense. Cyber operational test and evaluation guidebook. Department of Defense (US); 2025. [https://www.dote.osd.mil/Portals/97/pub/guidebooks/2025/Cyber%20Operational%20Test%20and%20Evaluation%20Guidebook%2020250206%20w-cover%20memo%20\(29625\).pdf](https://www.dote.osd.mil/Portals/97/pub/guidebooks/2025/Cyber%20Operational%20Test%20and%20Evaluation%20Guidebook%2020250206%20w-cover%20memo%20(29625).pdf)

DoD Deputy Information Officer. DoDAF - DoD architecture framework version 2.02 - DOD Deputy Chief Information Officer. Chief Information Officer, Department of Defense (US); 2010 Aug [accessed 2025 Apr 23]. <https://dodcio.defense.gov/Library/DoD-Architecture-Framework/>

Exploit Database. OffSec Services Limited. c2025 [accessed 2024 Aug 30]. <https://www.exploit-db.com/>

- Fenton NE, Neil M, Caballero JG. Using ranked nodes to model qualitative judgments in Bayesian networks. *IEEE Trans Knowl Data Eng.* 2007;19(10):1420–1432. <https://doi.org/10.1109/TKDE.2007.1073>
- Franks A. Improving the U.S. Air Force’s cyber defense strategy – CSIAC. CSIAC Cybersecurity & Information Systems Information Analysis Center (US); 2024 [accessed 2024 Sep 24]. <https://csiac.org/articles/improving-the-u-s-air-forces-cyber-defense-strategy-2/>
- Guion J, Reith M. Cyber terrain mission mapping: tools and methodologies. 2017 International Conference on Cyber Conflict (CyCon US); 2017 Nov 7–8; Washington, DC. IEEE; c2017. p. 105–111. <https://ieeexplore.ieee.org/abstract/document/8167504/>
- Headquarters, Department of the Army. Intelligence. Department of the Army (US); 2019a. Army Doctrine Publication No.: ADP 2-0. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18009-ADP_2-0-000-WEB-2.pdf
- Headquarters, Department of the Army. Intelligence preparation of the operational environment. Headquarters, Department of the Army (US); 2019b. Army Techniques Publication No.: ATP 2-01.3. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN40083-ATP_2-01.3-002-WEB-6.pdf
- Headquarters, Department of the Army. Operations. Department of the Army (US); 2022. Field Manual No.: FM 3-0. https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1025593
- Heinbockel W, Noel S, Curbo J. Mission dependency modeling for cyber situational awareness. NATO IST-148 Symposium on Cyber Defence Situation Awareness; 2016 Oct 3–4; Sofia, Bulgaria. p. 1–14. https://csis.gmu.edu/noel/pubs/2016_NATO_IST_148.pdf
- Jabbour K, Muccio S. The science of mission assurance. *J Strat Sec.* 2011;4(2):61–74. <https://www.jstor.org/stable/26463927>
- Jajodia S, Liu P, Swarup V, Wang C, editors. Cyber situational awareness: issues and research. Springer US (Advances in Information Security); 2010. <https://link.springer.com/10.1007/978-1-4419-0140-8>
- Javorník M, Komárková J, Husák M. Decision support for mission-centric cyber defence. Proceedings of the 14th International Conference on Availability Reliability and Security; 2019 Aug 26–29; Canterbury, United Kingdom. p. 1–8. ACM; <https://dl.acm.org/doi/10.1145/3339252.3340522>

- Jiang L et al. Systematic literature review on cyber situational awareness visualizations. IEEE Access. 2022;10:57525–57554. <https://ieeexplore.ieee.org/abstract/document/9782400/>
- Johnson A, Ott MQ, Dogucu M. Bayes rules! An introduction to applied Bayesian modeling. CRC Press; 2022.
- Joint Chiefs of Staff. Joint cyberspace operations. Joint Chiefs of Staff; 2022. Joint Publication No.: JP 3-12.
- Kuzio de Naray R, Buytendyk AM. Analysis of mission based cyber risk assessments (MBCRAs) usage in DoD’s cyber test & evaluation. Institute for Defense Analyses (US); 2022a. IDA Publication No.: P-33109.
- Kuzio de Naray R, Buytendyk AM. A cross-reference of mission-based cyber risk assessment (MBCRA) inputs and outputs. Institute for Defense Analyses (US); 2022b. IDA Document No.: P-32941.
- Kuzio de Naray R, Galvin K. A comparative review of DoD MBCRAs: 2020 updates and new methodologies. Institute for Defense Analyses (US); 2020 Sep. Report No.: P-14309.
- Martínez ÁL, Vidal JM, González VAV. Understanding and assessment of mission-centric key cyber terrains for joint military operations. arXiv; 2021 Nov 13. arXiv.2111.07005. <https://doi.org/10.48550/arXiv.2111.07005>
- McPhillips S, Golmassian R, Patterson M. Analysis of mission-based cyber risk assessment (MBCRA) model-based systems engineering (MBSE) tools. Naval Information Warfare Center Pacific (US); 2022. NAO Study No.: 21-089.
- Monroe M, Olinger J. Mission-based risk assessment process for cyber (MRAP-C). ITEA J Test Eval. 2020;41:229–232. https://www.itea.org/wp-content/uploads/2021/02/ITEA_Journal_Dec20-Mission-Based-Risk-Assessment-Process-for-Cyber-MRAP-C.pdf
- National Vulnerability Database – General Information. National Institute of Standards and Technology (US); 2024 June 27 [accessed 2024 Aug 26]. <https://nvd.nist.gov/general>
- [NIST] National Institute of Standards and Technology. Guide for conducting risk assessments. Department of Commerce (US); 2012. NIST Special Publication No.: 800-30 Revision 1. <https://csrc.nist.gov/pubs/sp/800/30/r1/final>

- Noel S, Heinbockel W. An overview of MITRE cyber situational awareness solutions. The MITRE Corporation; 2015 Sep 10 [accessed 2025 Apr 23]. <https://www.mitre.org/news-insights/publication/overview-mitre-cyber-situational-awareness-solutions>
- Office of the Under Secretary of Defense for Policy. Mission assurance. Department of Defense (US); 2018. DoD Directive No.: 3020.40. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983>
- Office of the Under Secretary of Defense for Policy. Mission assurance construct. Department of Defense (US); 2022. DoD Instruction No.: 3020.45. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=4Jg-492hgfA2cDsUPGmREA%3D%3D>
- Office of the Undersecretary of Defense for Research and Engineering. M&S VV&A RPG core document: introduction v. 1. Department of Defense (US); 2011. <https://www.de-bok.org/search?query=eyJzZWZyY2hOYW1IjoiUmVzb3VyY2VzIiwidHlwZSI6IiNFQVJDSF9PVE1NIiwidGVyYSI6Iiwia2V5LXBvLnBkZlwiIiwia2V5d29yZHMhOltldLCJzZWZyY2hDb25kaXRpb25zIjpudWxsL0aXRzZSI6IiJlc291cmNlcyIsImZpbHRlcniMiOltldLCJzb3J0Ijp7ImklIjoiREVVGQVVMVC5SRUxkFVkfOQ0UiLCJvcml6ImRlc2NfIn0sInBhZ2luYXRpb24iOnsiYWN0aXZlUGFnZSI6MSwiY3VycmVudFBhZ2UiOjEsInBhZ2VMaW1pdCI6NTAsInRvdGFsUmVzdWx0cyI6MX19>
- Office of the Under Secretary of Defense for Research and Engineering. DoD modeling and simulation verification, validation, and accreditation. Department of Defense (US); 2024. DoD Instruction No.: 5000.61.
- Peterson E. Dagger: modeling and visualization for mission impact situation awareness. MILCOM 2016-2016 IEEE Military Communications Conference; 2016 Nov 1–3. Baltimore, MD. IEEE; p. 25–30. <https://ieeexplore.ieee.org/abstract/document/7795296>
- Pomerleau M. Defensive cyber teams take on more missions under new model. C4ISRNet; 2017 Aug 16 [accessed 2024 Aug 26]. <https://www.c4isrnet.com/show-reporter/dodiis/2017/08/16/defensive-cyber-teams-take-on-more-missions-under-new-model>
- Raio S. Toward a conceptual framework for cyberspace windows of advantage. DEVCOM Army Research Laboratory Report (US); 2023. Report No.: ARL-MR-1080. <https://apps.dtic.mil/sti/trecms/pdf/AD1208205.pdf>

- Saydjari OS. Cyber defense: art to science. *Commun ACM*. 2004;47(3):52–57. <https://doi.org/10.1145/971617.971645>
- Schulz AE, Kotson MC, Zipkin JR. Cyber network mission dependencies. Lincoln Laboratory, Massachusetts Institute of Technology; 2015. Report No.: Technical Report No.: 1189. <https://www.ll.mit.edu/sites/default/files/publication/doc/2018-04/2015-Schultz-TR-1189.pdf>
- Schwartz Y, Benshimol L, Mimran D, Elovici Y, Shabtai A. LLMCloudHunter: harnessing LLMs for automated extraction of detection rules from cloud-based CTI. *arXiv*; 2024 Jul 6. arXiv:2407.05194. <https://doi.org/10.48550/arXiv.2407.05194>
- Secretary of Defense. Memorandum for senior Pentagon leadership: Army transformation and acquisition reform. Department of Defense (US); 2025. <https://media.defense.gov/2025/May/01/2003702281/-1/-1/1/army-transformation-and-acquisition-reform.pdf>
- Simulation Interoperability Standards Organization, Inc. Final report for the electronic warfare (EW) data exchange model (DEM) study group (SG). Simulation Interoperability Standards Organization, Inc.; 2024. Report No.: SISO-REF-081-2024. https://cdn.ymaws.com/www.sisostandards.org/resource/resmgr/reference_documents_/siso-ref-081-2024.pdf
- Snyder D et al. Cyber mission thread analysis: a prototype framework for assessing impact to missions from cyber attacks to weapon systems. RAND Corporation; 2022 [accessed 2025 Mar 24]. https://www.rand.org/pubs/research_reports/RR3188z1.html
- Snyder D et al. Wing-level mission assurance for a cyber-contested environment. RAND Corporation; 2021 [accessed 2024 Aug 9]. https://www.rand.org/pubs/research_reports/RRA580-1.html
- Spring J, Hatleback E, Householder A, Manion A, Shick D. Time to change the CVSS? *IEEE Secur Priv*. 2021;19(2):74–78. <https://ieeexplore.ieee.org/abstract/document/9382369>
- Thomas MA. Mathematization, not measurement: a critique of Stevens’ scales of measurement. *J Meth Meas Soc Sci*. 2019;10(2):76–94. <https://journals.uair.arizona.edu/index.php/jmmss/article/view/23785/0>
- Thompson B, Harang R. Identifying key cyber-physical terrain. *Proceedings of the 3rd ACM on International Workshop on Security and Privacy Analytics*; 2017 Mar 24; Scottsdale, AZ. p. 23–28. ACM. <https://dl.acm.org/doi/10.1145/3041008.3041015>

Underwood K. Air Force cyber mission defense teams 2.0: an evolving concept | AFCEA International. The Cyber Edge by Signal; 2024 Jan 5. <https://www.afcea.org/signal-media/cyber-edge/air-force-cyber-mission-defense-teams-20-evolving-concept>

United States Cyber Command. Risk assessment methodology (RAM) guideline, version 1.0. United States Cyber Command; 2016.

U.S. Army Space and Missile Defense Command. Cyber operational risk tool (CORT). Army Space and Missile Defense Command (US); n.d. https://www.smdc.army.mil/Portals/38/Documents/Publications/Fact_Sheets/Archived_Fact_Sheets/CORT.pdf

U.S. Army Training and Doctrine Command. The U.S. Army in multi-domain operations 2028. US Army Training and Doctrine Command; 2018. TRADOC Pamphlet No.: 525-3-1.

List of Symbols, Abbreviations, and Acronyms

ACARE	U.S. Army Cyber Command Activity Capability Access Resources Expertise
CENTCOM	U.S. Central Command
COA	course of action
CORT	Cyber Operational Readiness Tool
CPT	Cyber Protection Team
CTT	Cyber Table Top
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWoS	cyberspace window of superiority
DoD	Department of Defense
DODIN	DoD Information Network
IPOE	intelligence preparation of the operational environment
MA	mission assurance
MBCRA	mission-based cyber risk assessment
MDT	Mission Defense Team
MRAP-C	Mission-Based Risk Assessment Process for Cyber
NIST	National Institute of Standards and Technology
NVD	National Vulnerabilities Database
OpenVAS	Open Vulnerability Assessment Scanner
SMDC	U.S. Army Space and Missile Defense Command
SME	subject matter expert
USCYBERCOM RAM	U.S. Cyber Command Risk Assessment Methodology

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

1 DEVCOM ARL
(PDF) FCDD RLB CI
TECH LIB