ARL-MR-1080 ● AUG 2023

DEVCOM ARMY RESEARCH LABORATORY

Toward a Conceptual Framework for Cyberspace Windows of Advantage

by 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.

ARL-MR-1080 ● AUG 2023

Toward a Conceptual Framework for Cyberspace Windows of Advantage

Stephen Raio
DEVCOM Army Research Laboratory

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

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
August 2023	Memorandum Report	October 25, 2022	June 21, 2023

4. TITLE AND SUBTITLE
Toward a Conceptual Framework for Cyberspace Windows of Advantage

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Stephen Raio

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
DEVCOM Army Research Laboratory ATTN: FCDD-RLA-ND Aberdeen Proving Ground, MD 21005	ARL-MR-1080

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

14. ABSTRACT
This memorandum report proposes initial definitions and key concepts toward developing a conceptual framework for cyberspace advantage and, more specifically, temporally constrained cyberspace windows of advantage. Multidomain operations can be more efficiently and effectively planned and executed given capabilities to create, predict, and identify cyberspace windows of advantage. This report captures interim progress toward facilitating common understanding and a structured exploration of the cyberspace windows of advantage concept.

15. SUBJECT TERMS
cyberspace, window of advantage, window of superiority, window of disadvantage, window of X, Network, Cyber, Computational Sciences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UU	25

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Stephen Raio	(410) 278-9276

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

1 Introduction

Cyberspace superiority is defined in Joint Publication 3-12[1] as, "The 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 by an adversary." Cyberspace is both its own domain and a critical enabler in all other warfighting domains. Therefore, attaining cyberspace superiority seems necessary to successfully carry out multidomain operations. This raises certain questions, such as:

- How does one obtain cyberspace superiority?
- Is sustained cyberspace superiority a realistic goal?
- Is cyberspace superiority always necessary, or are lesser or greater degrees of advantage appropriate in some cases?

To begin to answer these questions and a plethora of additional basic research questions surrounding cyberspace superiority, we must first explore the concepts behind cyberspace superiority and, more generally, cyberspace advantage. This work aims to provide initial definitions and key concepts toward developing a conceptual framework for cyberspace advantage and, more specifically, temporally constrained cyberspace windows of advantage (CWoA).

2 Methods, Assumptions, and Procedures

2.1 Frameworks

Frameworks for CWoA are required to facilitate common understanding and a structured exploration of the concept, similar to Lockheed Martin's Cyber Kill Chain framework or MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, which help provide the conceptual and analytical frameworks necessary for these respective areas.

Theoretical, conceptual, and analytical frameworks for CWoA are needed before we can advance scientifically in leveraging CWoA in multidomain operations and possibly creating new military capabilities around the CWoA concept. A theoretical framework is helpful in reviewing existing theories that play a role in this line of thinking and achieving consensus on what, if anything, is missing from existing theories that can help us study CWoA and achieve desired capabilities. For example, prior work on key cyber terrain and control points[2] is likely to prove

useful for exploiting superiority in cyberspace. In this report, we make progress toward a conceptual framework, which will define all the key concepts involved in CWoA. Finally, building on the prior frameworks, an analytical framework will provide the model for conducting the analyses necessary to achieve the desired capabilities of identifying, predicting, and creating CWoA, which will be discussed further in the Sections 2.2 and 3.2.

The focus of the CWoA frameworks must first be directed toward human comprehension. The current focus is not on building out technical tools for automation and application of CWoA capabilities but on analytical tools for forming the construct by which we, as humans, can understand and explore the CWoA concept. However, it is important to formulate frameworks in a way that does not preclude or hinder our ability to automate the processes needed for machine speed cyberspace operations and ultimately multidomain operations support using CWoA.

2.2 Assumptions

Through reliable and rapid creation, prediction, and identification of CWoA, we can plan and carry out multidomain operations more efficiently and effectively. Similarly, when we operate in a disadvantaged state, that is, a window of disadvantage, we can enact appropriate cyber-defense and resilience mechanisms. These include cyberspace misrepresentation and adversarial machine learning techniques to mitigate threats in operationally relevant timelines within the cyberspace domain of an operational environment (see the depiction in Fig. 1).

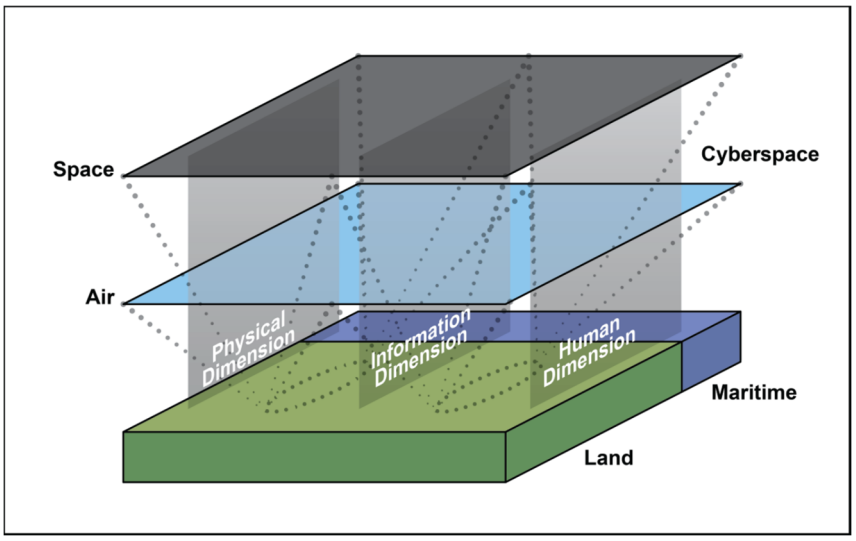

Fig. 1 Domains of an operational environment (image reprinted from Army Field Manual 3-0)[3]

The cyberspace domain consists of a physical network layer, a logical network layer, and a cyber persona layer (see Fig. 2). Considering the complexity, diversity, and scope of cyberspace, continuously sustained cyberspace superiority is an unrealistic expectation. Thus, the current focus is on cyberspace windows of superiority (CWoS) or, more holistically speaking, CWoA. Windows of superiority are discussed in more detail throughout Army Training and Doctrine Command Pamphlet 525-3-1.[4] However, because we are focusing on cyberspace and expanding the concept to the advantage spectrum, we will elaborate on how we currently view the terminology, with an understanding that our current views are subject to change as this research progresses.

2.3 Procedures

Several existing relevant definitions and terms (see Appendix) from the Department of Defense (DoD) and service components were reviewed to develop a proposed consensus of terms and term relationships for CWoA. The focus was on use of advantage, dominance, superiority, and supremacy. To summarize, all services seem to use the term "superiority" similarly. The term "dominance" is also used consistently within the information environment to mean supremacy. Outside of the information environment, however, the Army and Joint Terminology seems to use the term "dominance" as a synonym for any level of advantage, not just the highest possible level. The Air Force relates their advantage or disadvantage to a spectrum of air control, which ranges from adversary air supremacy to air parity and friendly air supremacy. Note that air superiority is a condition on the spectrum of air control. Furthermore, Space Force uses the term "supremacy" as the highest level of advantage.

Based on this review, Section 3.1 proposes term definitions that attempt to maintain maximum consistency with existing Army and Joint utilization. Section 3.1 also differentiates each term as part of an advantage spectrum that can help guide scientific exploration.

Finally, to help relate these terms and relationships to their use in cyberspace operations, a use case was crafted. The use case describes how CWoA can be leveraged toward efficient and effective achievement of military objectives.

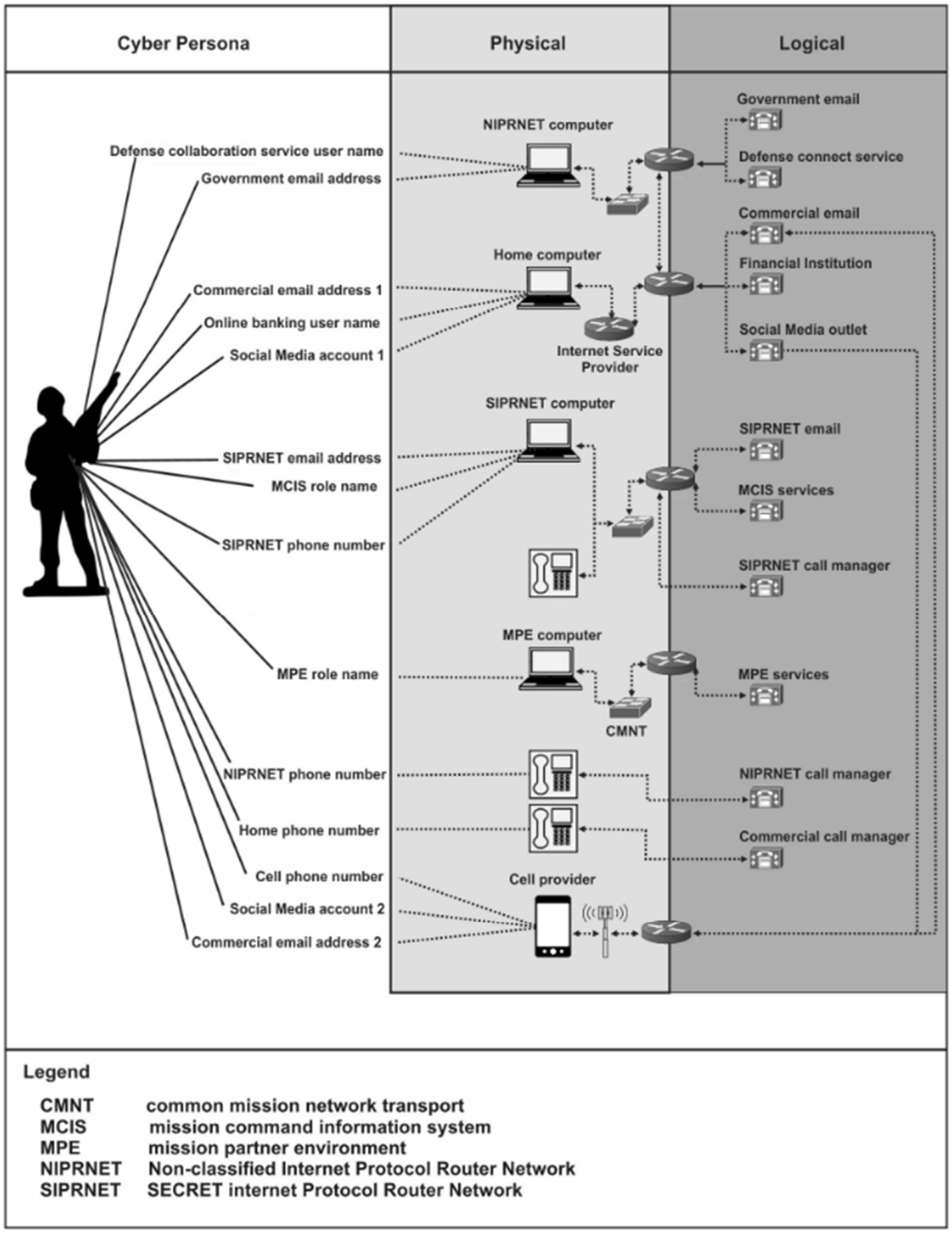

Fig. 2 Relationships among the cyberspace network layers (image reprinted from Army Field Manual 3-12)[5]

3 Results and Discussion

3.1 Definitions

Definitions are important to the advancement of any area of study. The definitions used in Army doctrine and throughout the DoD pertaining to this topic area may lack some of the precision required to formulate a common and thorough understanding. Therefore, the following definitions are offered as starting points for this research area, subject to change as the research progresses (note: critical differentiations are italicized):

- **Cyberspace Advantage** - *Any degree of advantage* in cyberspace *that may permit* the secure, reliable conduct of friendly cyberspace and non-cyberspace operations (i.e., land, air, maritime, and space operations) at a given time and scope.
- **Cyberspace Windows of Advantage (CWoA)** - *Contextually finite periods of time* in which friendly forces have cyberspace advantage.
- **Cyberspace Superiority** - *A degree of advantage* in cyberspace *that permits* the secure, reliable conduct of friendly cyberspace and non-cyberspace operations (i.e., land, air, maritime, and space operations) at a given time and scope *without prohibitive interference*.
- **Cyberspace Windows of Superiority (CWoS)** - *Contextually finite periods of time* in which friendly forces have cyberspace superiority.
- **Cyberspace Supremacy** - *A degree of advantage* in cyberspace *that permits* the secure, reliable conduct of friendly cyberspace and non-cyberspace operations (i.e., land, air, maritime, and space operations) at a given time and scope *without the possibility of interference*.
- **Cyberspace Windows of Supremacy** - *Contextually finite periods of time* in which friendly forces have cyberspace supremacy.
- **Cyberspace Disadvantage** - *Any degree of disadvantage* in cyberspace *that may impact* the secure, reliable conduct of friendly cyberspace and non-cyberspace operations (i.e., land, air, maritime, and space operations) at a given time and scope *upon exploitation*.
- **Cyberspace Windows of Disadvantage** - *Contextually finite periods of time* in which friendly forces have cyberspace disadvantage.
- **Cyberspace Windows of Opportunity** - Any opportunistically relevant CWoA other than an advantage specifically created for the situation at hand.

The notable difference between these definitions and the definition of cyberspace superiority offered in Joint Publication (JP) 3-12 is that these terms relate to multiple levels of advantage and are defined from a friendly force viewpoint. This allows us to be more precise about the level of advantage or disadvantage. These terms also relate to each other on an advantage spectrum, as summarized in Fig. 3. At this time, we have not further categorized the disadvantage portion of the spectrum. Vulnerability is not used as a synonym for disadvantage because a cyberspace vulnerability is not necessarily required for a cyberspace disadvantage to exist.

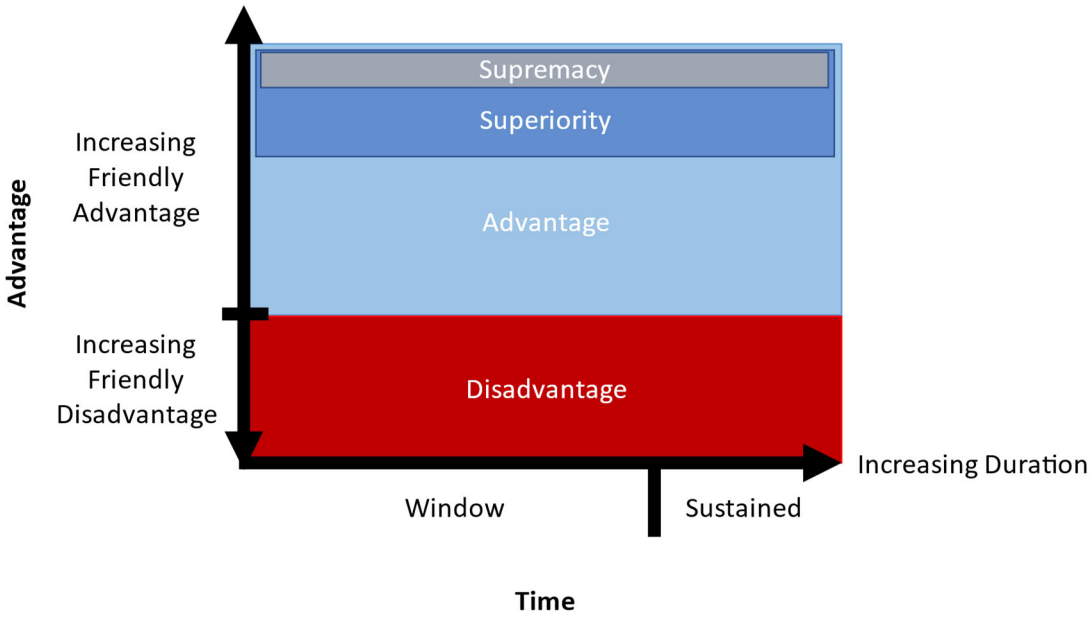

Fig. 3 Terms in relation to advantage spectrum and time

An advantage in cyberspace can be differentiated into a window of time or a sustained period, based on a time context. Relevant time contexts might be at the strategic, operational, or tactical levels of warfare, which tend to be long-term, medium-term, and short-term timeframes, respectively. For example, if a tactical-level cyberspace operation is expected to last 24 h, an advantage that lasts less than 24 h would be considered a window in this context, and an advantage that lasts for the entire operation, or longer, would be considered sustained.

3.2 Desired Capabilities

To maximize periods of cyberspace advantage and their benefit, the Army requires the ability to identify, predict, and create CWoA while minimizing periods of disadvantage. To achieve these capabilities, we must establish a conceptual, theoretical, and analytical framework with which to understand and explore the concept, ideally in a uniform manner across both tactical and enterprise networks.

Figure 4 demonstrates the anticipated window of advantage utilization cycle in the planning and execution of an operation or its individual missions. Details on identifying, predicting, and creating CWoA are provided in Sections 3.2.1 through 3.2.3.

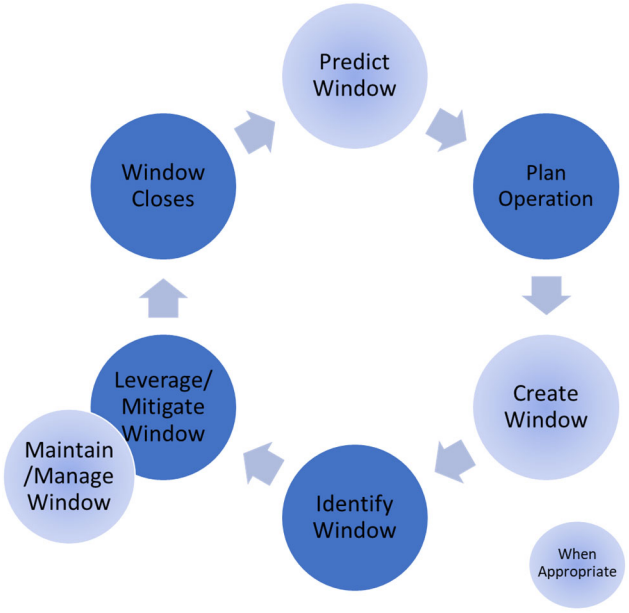

Fig. 4 Window of advantage utilization cycle

3.2.1 Identify

Our ability to identify a CWoA is fundamental to its use. This involves determining the information and methods necessary to understand when a CWoA presents itself. The ultimate goal is to be able to successfully leverage CWoA in military operations. To accomplish this, we must be able to understand when a CWoA exists, the scope of the CWoA in the cyber domain, and how long the CWoA is expected to last. Questions relevant to this research area include:

- What knowledge products, or information items, are required to recognize a CWoA, identify its scope, and estimate its duration?
- At what rate does the usefulness or accuracy of this information decay?

- What are the relevant operational inputs needed to determine the required scope of the CWoA in support of a mission?
- What are innovative techniques for sensors and measurements required for determining the existence, scope, and duration of the CWoA?

3.2.2 Predict

The ability to predict a CWoA would be a powerful cyberspace operations planning capability. By understanding when future opportunities for CWoA exist, mission resources can be more efficiently assigned and missions can be more thoroughly planned and coordinated, whether through deliberate planning cycles or continuous and integrated planning. Similar to identifying a CWoA, the critical elements of predicting a CWoA include understanding when and for how long a CWoA might be present as well as its scope within cyberspace. Additional elements may include confidence levels of the predictions or even the ability to conditionally predict a CWoA, meaning a CWoA could exist at some time in the future if additional conditions are met. This research area includes identification of the information, information sources, and the communications and computational methods required to make predictions about the corporality of a CWoA in terms of its virtual, physical, and temporal aspects. Questions relevant to this area include:

- What current and historical information is required to make predictions about future CWoA?
- How can we estimate the accuracy of these predictions?
- Can we identify methodologies for conditionally predicting CWoA?
- Can we identify and solve any unique aspects of predicting the scope and duration of a CWoA not covered under research done under "Identifying CWoA"?
- Can we identify innovative and resource-efficient methodologies for obtaining required information and processing it for predictions in a relevant time scale for Army use?

3.2.3 Create

An ideal capability would be the ability to create a CWoA with the desired scope and length of time to align with operational or mission needs. The key to achieving this is a thorough understanding of operational/mission needs and being able to align those needs with actionable steps within the cyberspace domain, which can ensure friendly use of the necessary cyberspace resources despite adversary actions to the contrary. It is also important to be able to identify second- and third-order

effects of any friendly actions aimed at creating a CWoA. Questions relevant to this research area include:

- What actionable steps within cyberspace can be used to shape cyberspace in such a way as to create a CWoA?
- Regarding these actions:
    - What is the expected impact of the action?
    - What is the expected scope of the action's impact, and can the impact be controlled?
    - How can we predict and quantify the second- and third-order effects of the action in terms of impact and duration?
    - Can the action be identified and nullified by an adversary?
    - How long is the action's impact expected to last?

3.3 Example Use Case

The following is an example use case for understanding the potential impact of harnessing CWoA. Specifically, it demonstrates how CWoA can be applied to a Defensive Cyberspace Operation (DCO) (depicted in the middle of Fig. 5). Other valid use cases include all types of cyberspace operations as well as operations in other domains that are enabled through cyberspace.

Consider, for example, the case of an advanced persistent threat within the Army's Non-classified Internet Protocol Router Network (NIPRNET) e-mail cloud infrastructure. Once discovered, a DCO mission is planned and executed to ultimately eliminate the intrusion. This scenario can occur if a CWoS is created through stealthy migration of the compromised virtual machine assets into a sandbox infrastructure where the adversary can be observed without posing additional threats to the Army enterprise. Once the migration is complete and the CWoS is verified, cyber misrepresentation techniques are used to coax the adversary into revealing their tactics, techniques, and procedures while the cyberspace protection team (CPT) observes from their privileged hypervisor position and automatically generates signatures. These signatures are then utilized in ongoing Department of Defense Information Network (DODIN) operations to identify additional intrusion activity and restore the cloud infrastructure.

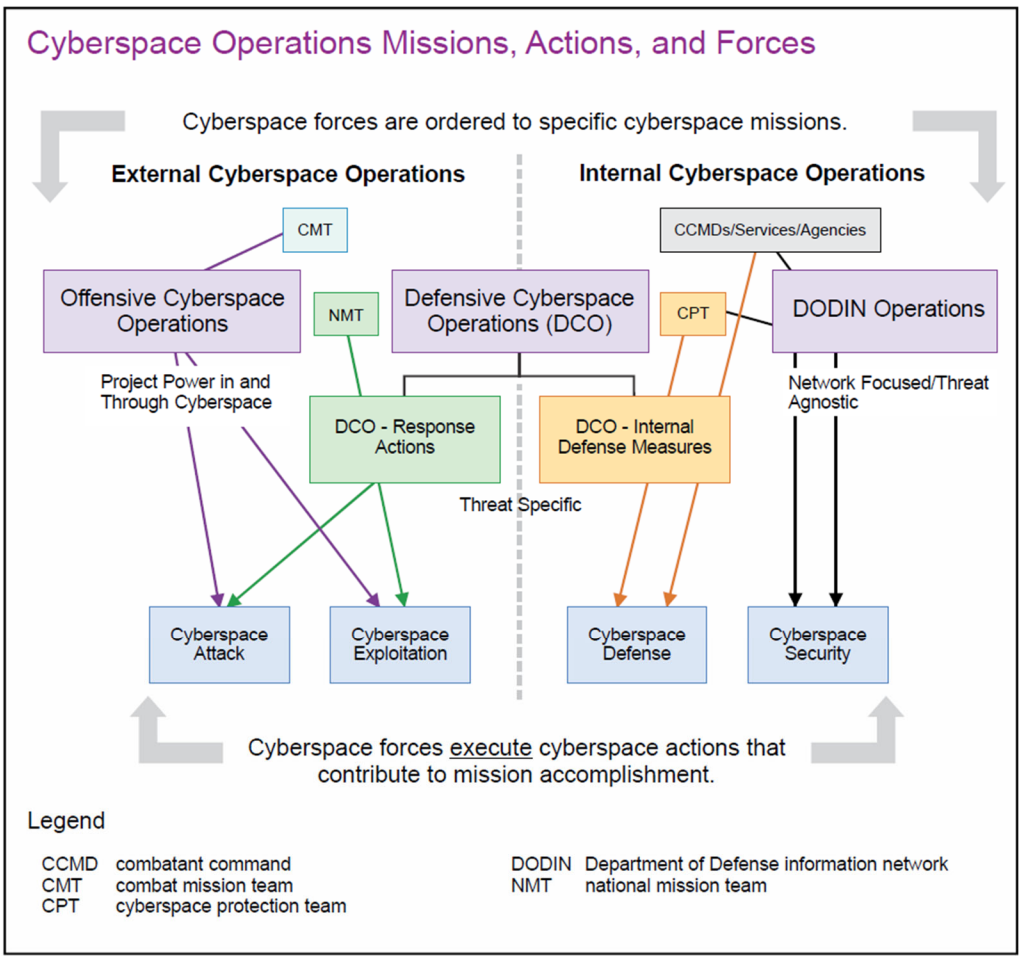

Fig. 5 Cyberspace operations missions, actions, and forces (image reprinted from Joint Publication 3-12)[1]

During the sandboxed observation of the adversary, it is recognized that this intrusion is linked to previous attack campaigns and that additional DCO-Response Actions are needed to prevent future intrusions. The adversary's command and control (C2) systems are port scanned and fingerprinted as part of cyberspace exploitation actions by a National Mission Team (NMT) in preparation for future cyberspace attack actions. It is determined that the software used by the adversary's C2 systems undergoes regular vulnerability patching on a monthly cycle that lags the patch availability by 3 days. Assuming these software vulnerabilities can be reverse engineered from the patches and weaponized within 1 day, there is a predicted CWoA for 2 days every month coinciding with the software patching cycle. This prediction is made with some measurable confidence level informed by relevant data points understood to be valid for certain timeframes. This information can be used to plan future NMT cyberspace attack actions aimed at creating denial effects against the adversary's ability to carry out future intrusions.

Meanwhile, the CPT uncovers an evasion technique used by the adversary to bypass the Army's machine learning-based intrusion detection system during exfiltration activities. This information is then utilized as part of future DODIN operations to use additional adversarial machine learning defense techniques during identified or predicted cyberspace windows of disadvantage (e.g., unusually high bandwidth on critical network segments), with a reasonable understanding of the second- and third-order effects of such increases to the defense posture.

This simplified hypothetical example is meant to provide additional context on how research into CWoA can benefit Army operations and missions. For an example of how all-domain windows of advantage can be utilized in multidomain operations, see the article by Skates.[6]

4 Conclusion

This report covers the interim progress toward defining a conceptual framework for cyberspace advantage and related CWoA. It presents proposed definitions, conceptual graphics, desired future capabilities, and an example use case for solidifying a common understanding of this topic area. This work, once finalized and combined with a theoretical and analytical framework, could aid in the scientific advancement toward and use of CWoA capabilities in multidomain operations.

5 References

1. Joint Chiefs of Staff. Cyberspace operations. Joint Chiefs of Staff (US); 19 2022 Dec 19. Joint Publication No.: JP 3-12 [accessed 2023 July 12]. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

2. Clark, DD. Characterizing cyberspace: past, present and future. Massachusetts Institute of Technology; 2010.

3. Headquarters, Department of the Army. Operations. Headquarters, Department of the Army; 2022 Oct. Field Manual No.: FM 3-0 [accessed 2023 July 12] https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1025593.

4. Army Training and Doctrine Command. The U.S. Army in multi-domain operations 2028. Army Training and Doctrine Command (US); 2018 Nov 27. Pamphlet No.: 525-3-1 [accessed 2023 July 12] https://adminpubs.tradoc.army.mil/pamphlets.html.

5. Headquarters, Department of the Army. Cyberspace operations and electromagnetic warfare. Headquarters, Department of the Army; 2021 Aug. Field Manual No.: FM 3-12 [accessed 2023 July 12] https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713.

6. Skates JL. Multi-domain operations at division and below. Army University Press; 2021 Feb [accessed 2023 July 12] https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Skates-Multi-Domain-Ops/.

Appendix. Existing Definitions and Term Uses

Advantage

- Information Advantage
    - An information advantage is the operational benefit derived when friendly forces understand and exploit the informational considerations of the operational environment to achieve information objectives while denying the threat's ability to do the same. (FM 3-0, Oct. 2022[1])

Dominance

- Decision Dominance (FM 3-0, Oct. 2022[1])
    - A desired state in which a force generates decisions, counters threat information warfare capabilities, strengthens friendly morale and will, and affects threat decision making more effectively than the opponent.
    - Decision dominance requires developing a variety of information advantages relative to that of the threat and then exploiting those advantages to achieve objectives. Commanders employ relevant military capabilities from all warfighting functions to create and exploit decision dominance.
    - Because threat forces adapt, and situations evolve, decision dominance is relative and transitory.
    - Decision dominance is aspirational, situationally dependent, and always relative to an opponent.
    - Adversaries and enemies pursue their own relative advantages, typically in asymmetric ways, while continually attempting to achieve decision dominance over friendly forces. Because threat forces adapt, and situations evolve, decision dominance is relative and transitory. Commanders therefore continuously make assessments to determine which forms of relative advantage are most important to pursue over time.
- Information Dominance
    - The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and

[1] Headquarters, Department of the Army. Operations. Washington (DC): Headquarters, Department of the Army; 2022 October. Field Manual No.: FM 3-0.

maximize warfighting effects. (Air Force Information Dominance Vision[2])

- America's Navy defines Information Dominance as the operational advantage gained from fully integrating our information functions, capabilities and resources to optimize decision making and maximizing warfighting effects. In other words, information dominance means maximizing America's Navy's operational employment of cyber, cryptologic and space forces working hand-in-hand with its intelligence, meteorological and oceanographic experts (US Navy Information Dominance Corps Brochure[3])

Superiority

- Air Superiority
  - That degree of control of the air by one force that permits the conduct of its operations at a given time and place without prohibitive interference from air and missile threats. (DoD Dictionary of Military and Associated Terms, May 2023[4])
  - That degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force. (NATO terminology database, retrieved 13 Jun 2023[5])
  - Air superiority is a condition on the spectrum of air control, which ranges from adversary air supremacy, to air parity, to friendly air supremacy. The air superiority condition is achieved when friendly operations are able to proceed without prohibitive interference from opposing forces. (Air Superiority 2030 Flight Plan[6])
- Cyberspace Superiority

[2] Office of the Chief Information Officer, Department of the Air Force. Air Force Information Dominance Vision. Department of the Air Force; 2015 January. https://www.safcn.af.mil/Portals/64/documents/AFD-150112-026.pdf?ver=2016-07-
[3] Department of the Navy. Information Dominance Corps. Department of the Navy; 2018 February. https://www.navy.com/sites/default/files/2018-03/0210-IDC-brochure.pdf.
[4] Department of Defense. DoD Dictionary of Military and Associated Terms. 2023 May.
[5] NATO terminology database [accessed 13 Jun 2023]. https://nso.nato.int/natoterm/Web.mvc.
[6] Team EC. Air superiority 2030 flight plan. US Air Force, Washington DC. 2016 May.

- The 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 Dictionary of Military and Associated Terms, May 2023[7])

- Electromagnetic Spectrum Superiority
  - That degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same. (DoD Dictionary of Military and Associated Terms, May 2023[6])
- Information Superiority
  - The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations. (DoD Dictionary of Military and Associated Terms, May 2023[6])
- Space Superiority
  - The degree of control in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from terrestrial or space-based threats. (DoD Dictionary of Military and Associated Terms, May 2023[6])
  - The concept of space superiority hinges on the idea of preventing prohibitive interference to space capabilities from adversary forces. Prohibitive interference would prevent space capabilities from creating desired effects. Space supremacy prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or will have little or no effect on operations. Space superiority provides sufficient freedom of action to create desired effects. (Air Force Doctrine Publication 3-14 Updated: 25 January 2021[6])

[7] Curtis E. Lemay Center for Doctrine Development and Education. Space Situational Awareness. 2021 January. Air Force Doctrine Publication No.: AFDP 3-14 Counterspace Operations.

- Window of Superiority
    - Converging capabilities in time and space in selected domains and environments to enable commanders to gain localized control or physical, virtual, and/or cognitive influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations. (Proposed in TRADOC Pamphlet 525-3-1, 27 Nov 2018[8])

Supremacy

- Air Supremacy
    - That degree of control of the air wherein the opposing force is incapable of effective interference within the operational area using air and missile threats. (DoD Dictionary of Military and Associated Terms, May 2023[6])
    - That degree of air superiority wherein the opposing air force is incapable of effective interference. (NATO terminology database, retrieved 13 Jun 2023[7])
- Maritime Supremacy
    - That degree of maritime superiority wherein an opposing force is incapable of effective interference. (DoD Dictionary of Military and Associated Terms, May 2023[6])

[8] TRADOC. The U.S. Army in Multi-Domain Operations 2028. 2018 December. TRADOC Pamphlet No.: TP 525-3-1.

List of Symbols, Abbreviations, and Acronyms

ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
C2	command and control
CPT	cyberspace protection team
CWoA	cyberspace windows of advantage
CWoS	cyberspace windows of superiority
DCO	defensive cyberspace operation
DoD	Department of Defense
DODIN	DoD Information Network
FM	field manual
JP	joint publication
NATO	North Atlantic Treaty Organization
NIPRNET	Non-classified Internet Protocol Router Network
NMT	National Mission Team
SIPRNET	Secret Internet Protocol Router Network

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLB CI TECH LIB
1 (PDF)	DEVCOM ARL FCDD RLA ND S RAIO