# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 04/26/2018 | Master's of Military Studies | SEP 2017 - APR 2018 |

**4. TITLE AND SUBTITLE**
Cyber Sand Tables: Representing the Cyber Integrated Battlefield to Decision Makers

**5a. CONTRACT NUMBER**
N/A

**5b. GRANT NUMBER**
N/A

**5c. PROGRAM ELEMENT NUMBER**
N/A

**6. AUTHOR(S)**
Huber, Derek J., Major, USAF

**5d. PROJECT NUMBER**
N/A

**5e. TASK NUMBER**
N/A

**5f. WORK UNIT NUMBER**
N/A

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

**8. PERFORMING ORGANIZATION REPORT NUMBER**
N/A

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**
Dr. Richard DiNardo

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
N/A

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
Approved for public release, distribution unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**
In order to support the delegation of cyberspace effects, the US military will need to develop cyberspace capabilities at the operational and tactical levels in order to maintain US superiority within all war fighting domains. Future conflicts will demand a more flexible and capable US military that can operate in an anti-access area denial environment while still maintaining the weapon system capabilities that are employed through cyberspace. The local battlefield commander will require the authority to prosecute cyberspace targets in the physical and cyber domains. To support these commanders, accurate depictions of cyberspace, which can fuse these domains into a realistic depiction, will be a requirement.

**15. SUBJECT TERMS**
Tactical Cyber, Operational Graphics, Cyberspace Operations, Cyberspace Effects, Anti-Access Area Denial (A2AD)

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | USMC Command and Staff College |
| | | | | | 19b. TELEPHONE NUMBER *(Include area code)* |
| Unclass | Unclass | Unclass | UU | 42 | (703) 784-3330 (Admin Office) |

*United States Marine Corps*
*Command and Staff College*
*Marine Corps University*
*2076 South Street*
*Marine Corps Combat Development Command*
*Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

---

**TITLE:**
CYBER SANDTABLES:
REPRESENTING THE CYBER INTEGRATED
BATTLEFIELD TO DECISION MAKERS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

**AUTHOR:**
MAJOR DEREK J. HUBER
UNITED STATES AIR FORCE

AY 2017-18

---

Mentor and Oral Defense Committee Member: Richard DiNardo
Approved: Richard D. DiNardo
Date: 2 April 2018

Oral Defense Committee Member: [illegible]
Approved: [illegible]
Date: 2 April 2018

H. R. RAWLINGS
02 APR 18

EXECUTIVE SUMMARY

**Title:** Cyber Sand Tables: Representing the Cyber Integrated Battlefield to Decision Makers

**Author:** Major Derek Huber, United States Air Force

**Thesis:** The US military is still deciding how to fully implement cyberspace operations across all levels of warfare, and decision makers need an effective representation of cyberspace operations at the tactical and operational level in order to integrate cyberspace operations into existing concept of operations.

**Discussion:** The commitment to generating effects in cyberspace has grown rapidly since the Department of Defense declared cyberspace as an operational domain. The willingness to implement cyberspace effects is stymied by the lack of authority and understanding by most conventional commanders and decision makers. In order to support the delegation of cyberspace effects, the US military will need to develop cyberspace capabilities at the operational and tactical levels in order to maintain US superiority across all military operations. The DOD needs to further develop processes and procedures to increase current and future leaders' awareness of cyberspace effects and capabilities because future military operations will require combined arms across all domains including cyberspace.

**Conclusion:** Future conflicts will demand a more flexible and capable US military that can operate in an anti-access area denial environment while still maintaining the weapon system capabilities that are employed through cyberspace. The local battlefield commander will require the authority to prosecute cyberspace targets in the physical and cyber domains. To support these commanders, accurate depictions of cyberspace, which can fuse these domains into a realistic depiction, will be a requirement.

DISCLAIMER

THE OPINIONS AND CONLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFRENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

## *LIST OF ILLUSTRATIONS*



## *LIST OF TABLES*

## *Table of Contents*

Page

## *PREFACE*

First and foremost, I must thank my family for their support throughout my education endeavors. Their willingness to put up with hours of research and study has allowed me to complete this paper, and I would not have been able to complete it without their encouragement.

I also need to thank Doctor DiNardo and Doctor Flynn for their guidance and advice throughout my time at the Marine Corps University's Command and Staff College. I am also very appreciative of the assistance I have received from my faculty advisors and fellow students as they have provided influential viewpoints to aid in my learning.

Cyberspace is an emerging warfighting domain and will continue to present challenges to the US military as new capabilities are added to the nation's armory. Hopefully my small contribution to the community will contribute to a better understanding of cyberspace operations and subsequently future employment at the operational and tactical levels.

*"If you read enough biography and history, you learn how people have dealt successfully or unsuccessfully with similar situations or patterns in the past."*
**Secretary of Defense James Mattis, 2017[1]**

## INTRODUCTION

War was declared between two global superpowers, and one of the first actions taken was an operation to isolate the new enemy's ability to communicate with the rest of the globe. This denial of service (DoS) attack achieved a second order effect by corralling the enemy into the precarious position of conducting command and control across an insecure communications medium. The reliable and trustworthy communications established during peacetime were no longer available to the enemy, and the superpower enjoyed a major strategic advantage because it impacted the enemy's ability to communicate. This scenario may sound like modern 21st century warfare, but in fact it is a summary of the opening operations conducted by the United Kingdom against Germany at the outset of World War I. The British realized the importance of limiting Germany's communications and were able to force the Germans to utilize insecure wireless telegraphy by deploying the cable ship *Telconia* to cut five German telegraphic cables within forty-eight hours of the declaration of war between the two countries. Author Peter Matthews highlights the importance of Britain's actions when he stated, "Cutting Germany's cable communications fundamentally changed the signals intelligence battleground."[2] The Germans to a lesser degree also understood the importance of global communications and conducted operations of their own to sever the United Kingdom's communications.[3] Does history foreshadow today's modern battlefield where cyberspace is the new medium that the United States military can utilize to influence an enemy's ability to conduct war and has it changed the battlefield to require US military planners to effectively plan for cyberspace effects within an operation?

Almost a century later, the Eastern European countries of Estonia and Georgia would be subjected to attacks against their communications infrastructure that "affected the nation's information flow to the outside world."[4] These attacks on Estonia and Georgia's communications would be deemed by some military professionals as revolutionary, but the effect achieved was very similar to the effects achieved by the belligerents in World War I when global communications were disrupted to gain a strategic advantage. The major difference between these events was the communication disruption for Estonia and Georgia was conducted through the cyber domain instead of the physical domain. Robert A. Miller and Daniel T. Kuehl claim that, "…the world witnessed what may have been the first major cyber-based assault on a nation-state."[5] The entity(s) that attacked Estonia and Georgia's communications infrastructure were able to achieve these effects without having to destroy or disrupt any physical communications infrastructure. These actions conducted in the cyber domain foreshadowed to the international community and especially the United States what future conflicts in cyberspace may look like.

The United States military is at the precipice of a new era of warfare and military operations. The cyberspace domain is fueling this new era and has drastically changed the modern battlefield within which American forces are being asked to operate. Cyberspace has blurred the lines between conventional military targets and the civilian institutions and populations that build, manage, and work within the cyber domain. It has direct and indirect relationships with all other domains that the military operates in, but current decision makers and planners cannot comprehend these relationships quickly or effectively with the existing representations of the cyber domain. Just like all other domains, cyberspace has its own distinct characteristics available to commanders or decision makers to exploit as they plan for and conduct defensive and offensive operations. Unfortunately, since there is not a clear

representation of the cyber integrated battlefield available to decision makers, there has been reluctance to employ cyber capabilities either on their own or in conjunction with traditional military operations. This paper attempts to provide a framework that can be used to represent the cyber integrated battlefield, comprised of cyber components and capabilities, available to current military decision makers within their area of responsibility. The U.S. Department of Defense (DOD) needs to further develop processes and procedures to increase current and future leaders' awareness of cyberspace effects and capabilities because future military operations will require combined arms across all domains including cyberspace.

The international and private sector cyber professionals have recognized the need for accurate modeling of the cyber domain so that businesses and governments can make effective decisions when trying to determine how to maintain and defend their assets that exist in cyberspace. Cyberspace is the only current domain that requires private organizations, in modern peaceful countries, to maintain defensive postures that are at least as capable as the most hardened military defenses. In fact, the cutting edge of cyberspace development of both defensive and offensive capabilities does not necessarily reside with the militaries of the world but instead is found in the private sector. This paper will analyze some of the existing methodologies and techniques used by current cyber professionals and identify existing frameworks or models that can assist in developing a model that is applicable for military operations and planning. An effective and fully realized representation of cyberspace operations (CO) to decision makers will require contributions and input from the cyber community and also the current military operations communities. This paper does not attempt to achieve consensus from these two communities and instead focuses on analysis of the current methods and

proposing modifications that may be adapted by military planners, at the combatant command (CCMD) level and below, to meet evolving threats facilitated through the cyber domain.

**Background**

Cyberspace and the cyber domain were officially codified within the US military's doctrine when *Joint Publication 3-12 Cyberspace Operations* (JP 3-12) was published on February 5th, 2013. This doctrinal publication allowed the DOD to consolidate all cyber doctrine into one document and define key terms that help decision makers and planners understand the domain.[6] The thirty years prior to the publication of JP 3-12 was filled with contention as professionals at all levels debated if cyberspace should be considered a separate domain. Since the cyber domain has rapidly changed the future of warfare, the United States is in the process of developing tactics, techniques, and procedures (TTPs) to operate in a cyber integrated battlefield. The DOD published its latest cyber strategy in April of 2015 to identify the strategic goals and objectives that it was pursuing over the next five years. In it the DOD highlights three primary missions in cyberspace: "to defend its [DOD] own networks, systems, and information;" "defend United States and its interests against cyber attacks of significant consequence;" and "provide integrated cyber capabilities to support military operations and contingency plans."[7] These three primary missions in cyberspace are very similar to the DOD primary missions within each of the physical domains just with the verbiage changed to reflect the corresponding domain. The DOD has provided the Joint Force the fundamental construct and guidance when conducting cyber operations in support of these three primary missions within JP 3-12. Both of these publications require planners and decision makers to attain an increased awareness of COs and how they integrate with the other domains to achieve the desired effects.

*"Mankind is endowing virtually every space with battlefield significance. All that is needed is the ability to launch an attack in a certain place, using certain means, in order to achieve a certain goal. Thus, the battlefield is omnipresent."*

**People's Liberation Army Colonels Qiao Liang and Wang Ziangsui, 1999[8]**

## UNDERSTANDING CYBERSPACE'S ROLE IN WARFARE

Assistant Secretary of Defense for Homeland Defense and Global Security, Kenneth P. Rapuano, on October 19th, 2017, appeared before the Senate Armed Services Committee and stated that, "DoD's role in cyberspace goes beyond adversary-focused operations and includes identifying and mitigating our own vulnerabilities. DoD recognizes its own reliance on cyber-enabled critical infrastructure to conduct its core missions."[9] This statement and the direction given to the DOD within JP 3-12 outline the key cyber terrain that the DOD is charged with defending. Only on rare occasions would the DOD be asked to conduct defensive cyber operations (DCO) for US networks and communications that are not part of the Department of Defense information networks (DODIN). It is imperative that decision makers fully grasp the makeup of cyberspace in order to not only defend the DODIN but to also be able to conduct COs against an adversary's networks. According to the JP 3-12, "cyberspace can be described in terms of three layers: physical, logical network, and cyber-persona"[10] (see Figure 1).

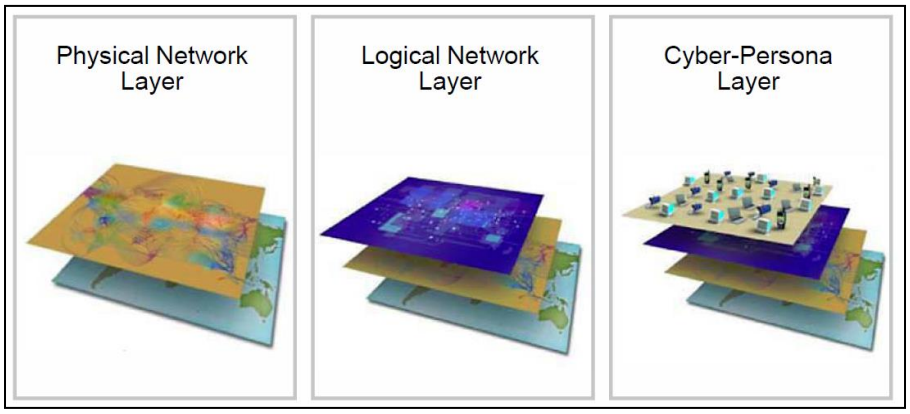



**Figure 1 – The Three Layers of Cyberspace**

***Source:*** **JP 3-12 (R) Cyberspace Operations, February 5, 2013, I-2-I-4.**

The cyber layers are unique because cyberspace still relies on the physical world, but it is the only domain that is not limited by time and space. An adversary operating in cyberspace can now achieve effects against an opposing force without physically mobilizing conventional forces, and these effects can be realized instantaneously. Cyber terrain is also unique because it evolves and changes drastically in a very short period of time. Users and devices will connect and disconnect from the network, which alters the environment in a matter of seconds. Cyber law experts, Gary Brown and Kurt Sanger, highlight the unique issues facing cyber planners, "the fact that the changes are rapid, constant and to some extent unpredictable makes cyber planning a different proposition than planning in the kinetic realms."[11] The drastic changes in cyberspace could be analogous to drastic change in weather in the physical world that disrupts the battlefield because of flash floods, hurricanes, tornadoes, or other such natural phenomena. However, the difference is that cyberspace changes much faster than the physical world, and a change in cyberspace can impact the entire domain whereas severe weather geographically separated from the area of operations (AO) may have little to no impact on a specific battlefield.[12]

Cyberspace is unique, but just like all of the physical domains there is key terrain that can either be used to exploit an enemy's weaknesses or a vital point to defend and hold to avoid any adverse effects against friendly forces. There are differing opinions on what cyber terrain exactly is and also where it even resides. In April 2017, Erick McCroskey and Charles Mock claim in the Joint Forces Quarterly that the "logical layer is where cyber terrain exists, and the primary cyberspace terrain feature is the network."[13] This narrow view of cyber terrain residing only at the logical layer is not held by others or the DOD. JP 3-12R alludes to key cyber terrain being primarily in the physical layer when it states, "key terrain involves network links and nodes that are essential to a particular friendly or adversary capability."[14] By limiting cyber terrain to a

single layer, both approaches will underestimate the value of targeting and defending cyber terrain across all three layers of cyberspace. In order for planners and decision makers to identify key cyber terrain, the physical domain needs to be evaluated for key terrain that can have effects in cyberspace. It's imperative that COs become integrated across all operations and combined with all combat arms of the US military especially since near peer competitors in cyberspace may become future adversaries.

**Cyber's Role in Anti-Access Area Denial Theaters**

The United States military's dependence on cyberspace is unmatched in the modern era. Author and prior White House cabinet member, Richard A. Clarke, paints a stark picture of the United States' current cyberspace posture when he claims, "…because of its [United States] inability thus far to create national cyber defenses, the United States is currently far more vulnerable to cyber war … cyber war puts America at a disadvantage right now… as long as our economic and military systems are so obviously vulnerable to cyber war, they will tempt opponents to attack in a period of tensions."[15] US global influence and power is diminished significantly because of the US military's reliance on cyberspace and weak defensive capabilities to defend against a significant cyber attack. Cyberpower must be pushed down to the lowest level as a goal of some potential US adversaries is to sever reach-back capability to higher echelons. If cyberpower is primarily centralized at USCYBERCOM then US forces are susceptible to cyber attacks without adequate cyberspace defense and attack capabilities.

An Anti-Access Area Denial (A2AD) theater of war would be catastrophic against a US Joint Task Force (JTF) that does not have significant defensive and offensive cyber forces forward deployed. The lack of forward deployed cyber forces allows enemy forces to isolate JTF units through cyber effects in order to launch successive kinetic attacks. It does appear that senior military decision makers are beginning to understand the cyber shortcomings of forward

deployed units and are making changes in their force structure to incorporate cyberpower at the tactical edge. Technology editor for *Defense One*, Patrick Tucker, stated in February 2017 that, "the service [US Army] has been experimenting with different concepts of operations for the cyber units that will be on the front lines of tomorrow's fights."[16] This first iteration of forward deployed cyber forces appear to be the combat mission teams and combat support teams aligned to the CCMDs, but these forces are still under the operational control of USCYBERCOM.[17] This inhibits planning efforts and command of these forces by the operational commander since they must request permission of USCYBERCOM to employ the cyberspace effects needed by the CCMD. In order for true operational success these forces must be aligned as tactical cyber forces imbedded in the CCMDs and JTFs.

Another key cyberspace aspect that military leaders need to focus energy and resources on in an A2AD Theater is the development of robust cyberspace primary, alternate, contingency, and emergency (PACE) plans. A generalized example of a PACE plan is shown in Table 1. The primary focus of all military branches on the Global War on Terror in relatively low-tech countries and insurgent hotspots has instigated a gradual deterioration of US military capabilities and expertise needed to combat a near-peer competitor.[18] The PACE plan was a mainstay throughout the Cold War and detailed the communications channels that would be used in descending order if the enemy were to disrupt or degrade the primary communication channel. Many units still utilize a PACE plan when planning and conducting an operation, but the planners rarely account for cyberspace vulnerabilities in the communication mediums selected. These vulnerabilities must be identified and accounted for so that robust PACE plans can be used to withstand enemy cyber attacks. Table 1 provides an example of a potential PACE plan with cyberspace and Information Environment vulnerabilities listed for each communication method.

**Table 1: Cyber and Communications PACE Plan Example**

| PRECENDENCE | TECHNOLOGY/MEDIUM | VULNERABILITIES OR LIMITING FACTORS |
|---|---|---|
| PRIMARY: | Secure Internet Protocol Router Network (SIPRNet) E-mail & Voice Over IP | Satellite frequency jamming; Terrestrial network exploited |
| ALTERNATE: | Ultra High Frequency (UHF) or Very High Frequency (VHF) a.k.a. Tactical Satellite (TACSAT) Voice | Satellite frequency jamming; Man in the Middle |
| CONTINGENCY: | High Frequency (HF) | Low bandwidth |
| EMERGENCY: | Commercial Cell phones | Man in the Middle; Jamming; Unencrypted voice & data |

## Close Cyber Support (CCS) and Tactical Cyber

A comparison can be made between airpower and its evolution within the history of warfare and the potential effects cyberpower will have on future warfare. Airpower at the end of World War I was able to impact almost every aspect of the two traditional physical domains: land and sea. Ground and maritime forces were no longer able to mask their movements and were very susceptible to attack from the air. The British in the Palestinian campaign against the Ottoman Empire highlighted the tremendous benefits of airpower when used as close air support (CAS) against ground forces that were ill prepared for this new era of warfare. At Wadi el Far'a on 21 September 1918, the British were able to destroy much of the Turkish Seventh Army through attacks from the air.[19] A famous British military officer, Thomas Edward Lawrence more commonly known as Lawrence of Arabia, described the destruction caused by British airpower, "It was the RAF [Royal Air Force] which had converted the Turkish retreat into a rout, which had abolished their telephone and telegraph connections, had blocked their lorry columns, scattered their infantry units."[20] The ability of airpower to permanently change warfare was discovered in its infancy, but unfortunately senior decision makers of the era, most notably during the Interwar Period, fixated on one aspect of airpower, strategic bombing. Strategic bombing definitely had a place in airpower doctrine, but the CAS lessons learned by the British in World War I were abandoned by the RAF and most other belligerents as it was believed that

airpower was solely a strategic-level weapon. It appears that cyberpower is currently following a similar path as airpower in its infancy and is viewed primarily as a strategic-level asset.

Cyberpower can greatly impact all of the traditional physical domains, analogous to airpower, because most modern military technology is reliant on cyberspace. In order to offset these cyber weaknesses within US systems, the US military must develop and extend cyberpower down to the tactical level so that commanders can employ close cyber support (CCS) in the same way CAS was and is used to support friendly forces in close proximity to hostile targets. There are some analysts that have advocated for tactical cyber or CCS capabilities to be developed to support a military force in the field. The Rand Corporation commissioned a report in 2017 to build a case for tactical cyber support to Corps and below within the US Army and Marine Corps. The case was made that Army units will be asked to fight in areas of operations that are full of enemy and neutral cyberspace technologies and data. The commanders on the ground will need the capability to respond quickly in this "dynamic, information-rich environment." The report also explains the benefits of not only tactical level DCOs, but also focuses on tactical level offensive cyberspace operations (OCO) because battlefield commanders will have cyberspace targets of opportunities that strategic-level cyber units will not be privy too. The report analyzes three case studies and then provides recommendations on how to implement tactical cyber support. It even offers a simple flowchart (see Figure 2) to determine what operations would justify tactical cyberpower.[21] This report is a useful resource for current decision makers to utilize as they develop authorities and relationships that will ultimately allow for tactical cyber to become a fully realized capability inherent in all the services.

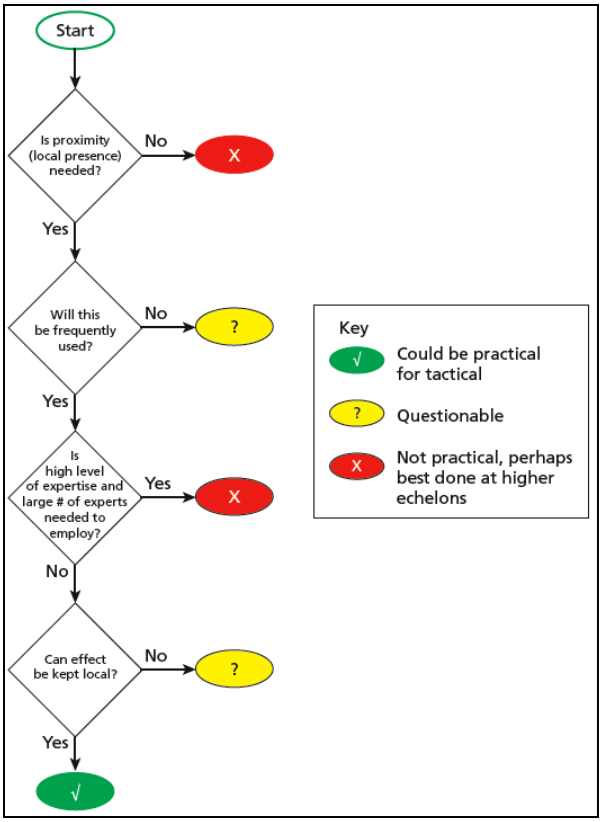



**Figure 2 - Flowchart to Assess Practical Tactical Offensive Cyber Capability**

***Source:*** **Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND, 2017).**

Many of the same arguments and justifications utilized within the Rand report can be used to highlight the need for CCS capabilities. A paper was released in conjunction with the 18th International Command and Control Research and Technology Symposium (ICCRTS) that described a very high-level approach to applying CAS principles to CCS, or as they called it Close Cyber Security Support (CCSS).[22] CCS, similar to CAS in the air domain, would fill the gap between strategic-level cyber capabilities and tactical cyber once it is fully entrenched in small fighting units. Cyber force apportionment and allocation for CCS would occur at the operational level just as CAS does and could bring to bear cyber capabilities more potent than those that will reside at the tactical level. This level of integration would require robust planning for combined arms that included CCS "to exploit tactical opportunities in the offense or

defense."[23] CCS could be used to provide fires to deny, degrade, disrupt, destroy, or manipulate enemy forces within cyberspace in preparation for follow-on military operations.[24] A CCS unit would reside within each Combatant Command (CCMD) much in the same way the Cyberspace Support Element (CSE) is currently organized under the CCMDs. The current organizational structure and support between United States Cyber Command (USCYBERCOM) and the CCMDs is shown in Figure 3. The CSE is currently organized to provide reach back to USCYBERCOM from the CCMDs and also direct support to the CCMDs.[25] The CSE could evolve into a fully operational CCS that has the authority to integrate the CCMDs allocated cyberpower into a cyberspace integrated Concept of Operations (CONOPS).

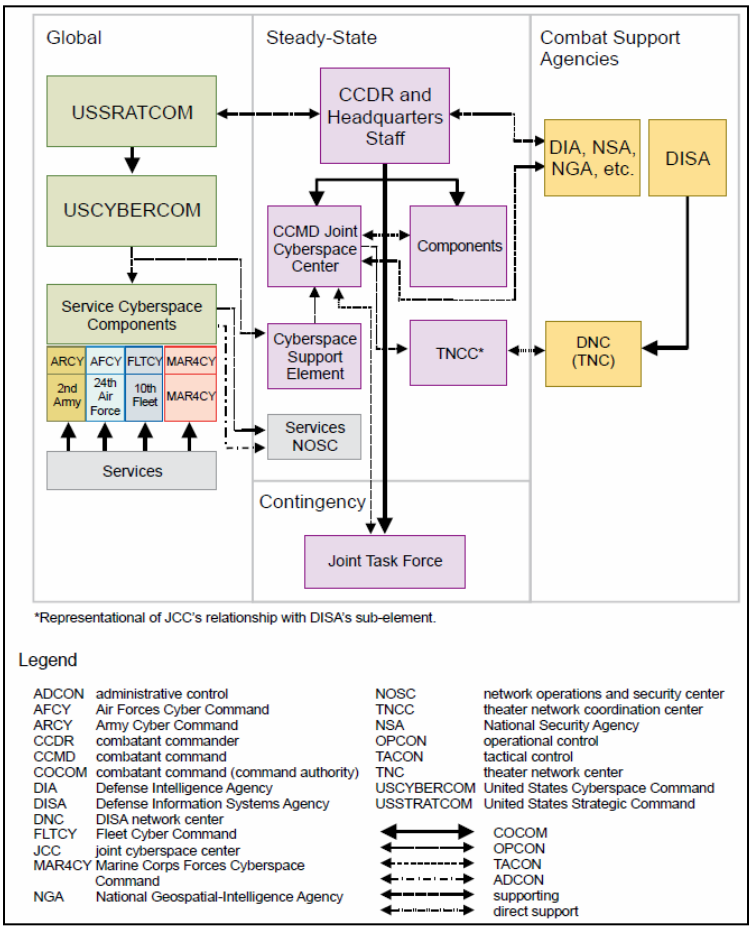



**Figure 3 - Cyberspace Command and Control Organizational Construct**

***Source*: US Department of Defense, *Cyberspace Operations*, IV-8.**

Major General Brett T. Williams, USCYBERCOM Director of Operations (J3) in 2014, proposed that a key element for success with CO is to designate a joint force cyberspace component commander (JFCCC) that is on the same level as the other domain functional component commanders. This concept ties in perfectly with CCS and tactical cyber initiatives discussed in this paper. The JFCCC would direct DCO and OCO for the cyberspace forces allocated to the CCMD and their corresponding JTFs. However, he acknowledges that his recommendation for the JFCCC follows closely along the U.S. Special Operations Command (USSOCOM) force structure because the cyber forces assigned to the CCMD would still be controlled by USCYBERCOM. In July 2017, Gen Raymond A. Thomas III, commander of USSOCOM, was very supportive of empowering commanders with the authority to conduct CO. He states, "It essentially boils down to trusting the commander and the team to do the right thing."[26] COs may have finally overcome the strategic-level only weapon mantra, and with continued senior leadership support at the CCMD level and higher, cyber planners will be able to start planning tactical COs.

**Defining Cyber Area of Interest and Area of Influence**

Since COs are conducted almost exclusively by USCYBERCOM, there has not been a need to define a Cyber Area of Interest (AOI) or Area of Influence for operational or tactical-level units. Instead USCYBERCOM works out the de-confliction and authorities needed to conduct OCO in support of a JTF or CCMD. As the push for the authority to conduct COs at the tactical units increases, the requirement to have a clearly defined operational environment (OE) will become a necessity. JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, defines the OE, "[it] encompasses all characteristics, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission."[27] This translates to cyberspace as planners and intelligence personnel take into account

the cyberspace effects that can be levied against friendly and adversary units. McCroskey and Mock distill cyberspace OE down to "networks as the cyberspace equivalent to areas of operations in the physical domain."[28] However, this definition may be too narrow and allows for cyberspace blind spots when a planner is attempting to clearly define the OE. Electronic signatures, domestic and international law and policy, and cyberspace technology not part of a network, i.e. stand-alone computers, may be overlooked as weaknesses that require defense by friendly forces, or a potential seam to exploit within the adversary's cyber defense. Ultimately, JP 3-12 states CO planners will face unique challenges as they will need to understand the physical and logical characteristics of friendly and adversary networks and the governing laws and policies in regards to CO for their OE.[29]

According to JP 2-01.3, an area of influence is "a geographical area wherein a commander is directly capable of influencing operations," but if COs are restricted to physical geography then a commander's cyber area of influence would primarily reside in defensive operations and limited offensive operations. Instead a cyber area of influence should be aligned with not only physical geography but also the authorities that have been delegated to a commander to operate against logical networks and cyber personas. Allowing a tactical commander to defend his forces at the logical and cyber persona layers has never been controversial, but the same commander has not had the same autonomy to respond to an attack (DCO Response Action) or conduct OCO against enemy forces even within their geographical area of operation. As tactical commanders gain this authority to target and attack enemy forces they will have to coordinate their actions with USCYBERCOM and other government agencies because COs can have unintended second order effects in cyberspace.[30] Commanders will have

to take an active approach to ensure their cyber area of influence does not unintentionally expand because of unintended second order effects.

A cyber area of interest (AOI) encompasses the area of influence, but it is not restricted by geographical or political boundaries. Unlike the conventional area of influence definition in JP 2-01.3, a cyber AOI is in line with the traditional doctrine definition of AOI. In fact, the information environment is highlighted as a key reason why there should not be a set boundary when planning an AOI for an operation, "many of these factors [cyberspace] transcend the traditional concept of physical boundaries and have worldwide implications and relevance."[31] A well developed cyber AOI will identify cyber actors outside of the commander's area of influence that are motivated to conduct cyber attacks against their forces. The key will be for a planner to ensure that a cyber AOI can overlay or integrate seamlessly with a traditional AOI graphical representation so that a commander can evaluate all of the domains to identify where future threats or targets may reside. Matthew Stern, prior commander for the US Army Computer Emergency Response Team, offers his opinion on cyberspace OE, "cyber defenders today must employ this mindset [knowledge of cyberspace vulnerabilities] and employ tools that provide the understanding of their areas of operation, influence, and interest."[32] Once cyber planners can develop accurate tactical cyber areas of influence and cyber AOIs then the next task will be to represent the OE in concert with traditional combined arms.

*"One picture is worth ten thousand words."*
**Publicist Frederick Barnard, 1921**[33]

## REPRESENTING CYBERSPACE IN COMBINED ARMS

Major General Williams provided a guide to Joint Force Commanders (JFC) on CO and stressed that, "relying on tactical actions from any single domain to be dominant is a pitfall that we have mostly learned to avoid, and we should not have to relearn the lesson as we integrate cyberspace operations into joint planning."[34] Following Williams' guidance and the lessons learned almost a century ago, when the air domain was believed to be the single domain capable of dominating an adversary, will ensure that cyberspace effects are integrated thoroughly with all other domains when conducting combined arms. JP 3-12 also stresses the importance of integrating all domains when planning for an operation, "while cyberspace operations can produce stand-alone tactical, operational, and strategic effects and achieve objectives, they must be integrated with the employment of the JFC's other capabilities to create synergistic effects in support of the JFC's plan."[35] Similar to how the air domain was first integrated into operational planning; the cyber domain requires decision makers and planners to understand that cyberspace has unique characteristics that must be accounted for in planning operations.

One tried and true way to help planners and decision makers understand a battle space is to represent the battle space visually. Senior leaders are advancing the need for representation of the cyber domain. Major General Patricia Frost, US Army Director of Cyber, stated this requirement in 2017, "The commander has [to have] a complete visualization of the domain [cyber]. That's really important."[36] This has proven to be easier said than done for the cyber domain because the three different layers that make up cyberspace do not lend themselves to traditional visual representations. Military planners and decision makers have grown accustomed to the graphical representations offered for the physical domain, and it makes sense to model

cyber representations off already existing products like the event template from JP 2-01.3 (see Figure 4).

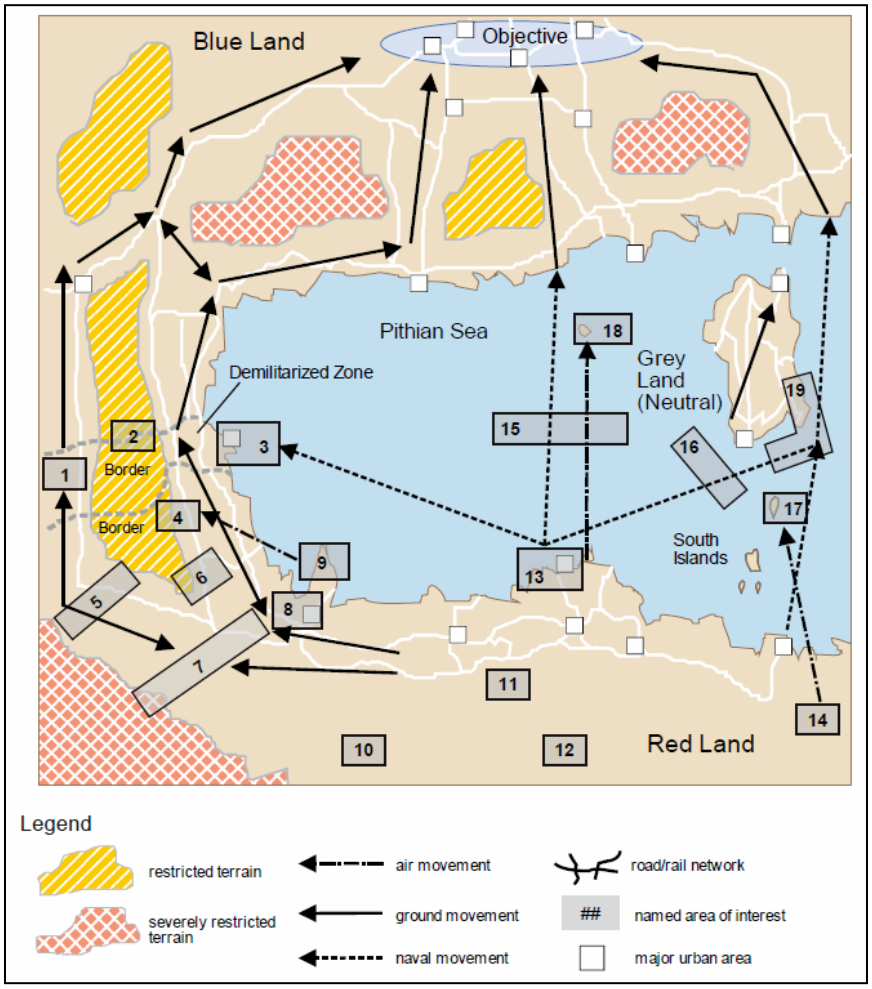



**Figure 4 - Event Template**

***Source:*** **US Department of Defense, Joint Intelligence Preparation of the Operational Environment, V-12.**

Cyber professionals and industry partners are starting to answer the call for visual representations of the cyber domain. McCroskey and Mock have provided the community with cyber symbols to be used when representing COs in the logical and persona layers of cyberspace. They utilize the same methodology outlined in MIL-STD-2525 DOD Common Interface, Warfighting Symbology, to create cyber symbols that represent cyberspace components, and they have adapted many of the traditional operational graphics to be used for actions conducted in cyberspace. Their approach allows decision makers and planners already familiar with the

traditional symbols and graphics to intuitively identify what the symbols and graphics mean in the cyber domain (see Appendix B an abbreviated version of their adapted graphics). They also utilize these symbols and graphics to depict a notional cyberspace battle, see Figure 5, but it is lacking the integration with the physical domains as it is focused on the logical layer of cyberspace.[37]

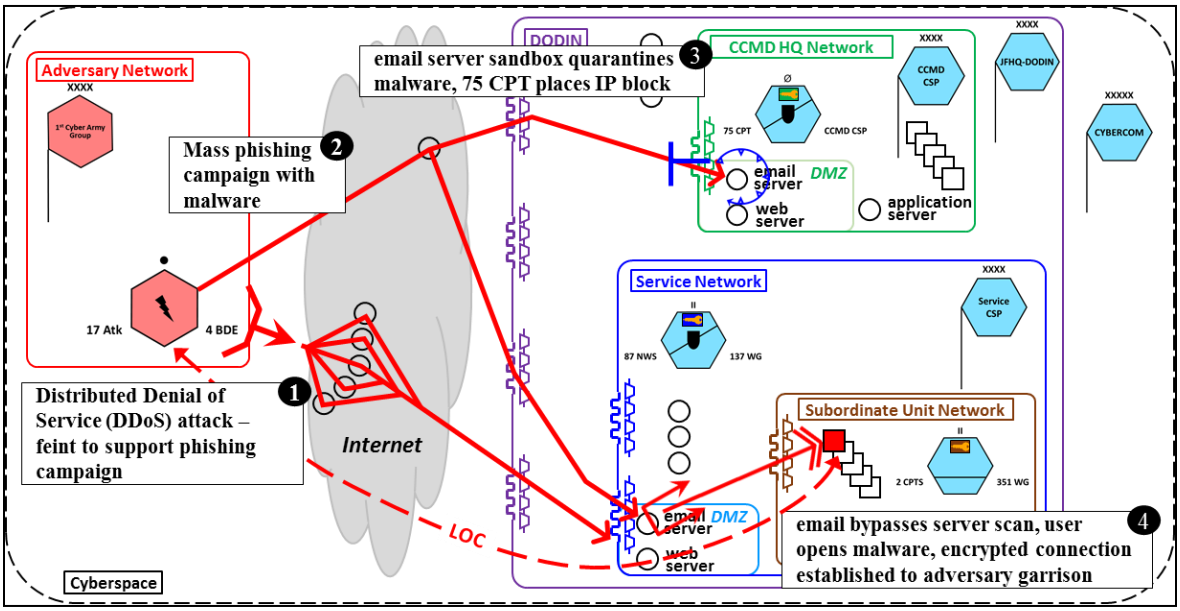



**Figure 5 - Notional Cyberspace Battle**

***Source:*** **McCroskey and Mock. "Operational Graphics for Cyberspace."** ***Joint Force Quarterly,*** **48.**

McCroskey and Mock advanced the work towards a realization of cyberspace visualization, but additional refinements are still needed to be useful representations for planners and decision makers beyond cyberspace only operations. Their model can be used by planners to war game potential courses of action (COA) and to illustrate flaws in the logical networks a unit is attempting to defend or attack, but it cannot provide real-time reporting and visualization to a decision maker once the conflict has begun. Commanders at the operational and tactical level need cyberspace operational graphics integrated into an automated common operating platform (COP). Automation will allow for real-time analysis of COs and their effects on the battle space, and the Defense Advanced Research Projects Agency (DARPA) has developed a COP called

PlanX that is geared to "facilitate planning, monitoring, rehearsal, analysis and execution" of COs.[38] PlanX is built to be a one-stop shop for COs and provides a "multi-dimensional view of the Cyber Terrain at the tactical, operational, and strategic levels," which is linked to the Military Decision Making Process (MDMP).[39] Since DARPA was the mastermind behind the creation of the Internet, it is fitting that DARPA would develop an automated platform that enhances the DOD's ability to conduct COs. PlanX also appears to solve some of the concerns senior leaders have about COs being conducted at the tactical level. PlanX is a modular platform, and it functions as a baseline system that permits cyberspace operators to mix and match cyber tools and weapons to the specific cyberspace effects and authorities delegated down to an operational or tactical commander. Ideally planners would utilize the tactical cyber flowchart (see Figure 2) to analyze which cyber weapons or effects should be added to a PlanX configuration for a specified offensive operation at the tactical level. PlanX can evolve to become a tremendous asset to cyberspace personnel as it allows for the complexity of cyberspace to be graphed out and parsed down into digestible chunks.

**Integrating Cyber Operational Graphics across Warfighting Domains**

The cyber community has advanced other methodologies that are not covered in this paper, which endeavor to provide a simple product that decision makers can understand and execute from. As evidenced by the work that was highlighted in this paper, the initiative to visually represent cyberspace for leadership is beginning to show positive results. It is beneficial to combine some of these efforts to create a robust cyberspace visualization tool that also integrates kinetic operations into one platform or graphic, similar to a merger of Figure 4 and Figure 5. The North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defence (sic) Centre (sic) Of Excellence (CCD COE) has been advocating for a cyber common operating picture (CCOP) that would merge the physical and cyber domains. One of CCD COE's

publications in 2013 identified that “a primary challenge will be how they [cyber planners] seamlessly fuse the physical domain with cyberspace for planning and execution of combined arms operations.”[40] The method described in this paper draws a correlation to how the DOD integrated airpower into combined arms with the challenge of integrating the cyber domain into modern day combined arms. Cyberspace much like airspace is a domain that can encompass the entire battlefield but still has physical assets, such as server farms, satellite terminals, networking components, personal computers, and cell phones. These physical assets can be pinpointed to a specific point in the land or maritime domains, which is analogous to airfields and aircraft carriers in the air domain. The actual cyberspace effects of OCO or DCO are not realized in the physical domain, which also requires a representation of the logical layer.

The first step in creating a cyberspace graphical representation is to develop a cyberspace integrated AOI and area of influence graphic, and again, the DOD already has a methodology in place that can be easily adapted for cyberspace. Chapter II of JP 2-01.3 covers the development of combined obstacle overlays and identifies that key elements of the physical world can be represented as layers, which can be added or removed to highlight key aspects of the OE (see Figure 6). It even discusses the steps to create a robust combined obstacle overlay for the electromagnetic spectrum and the information environment, both of which cyberspace is reliant upon (see Figure 7).

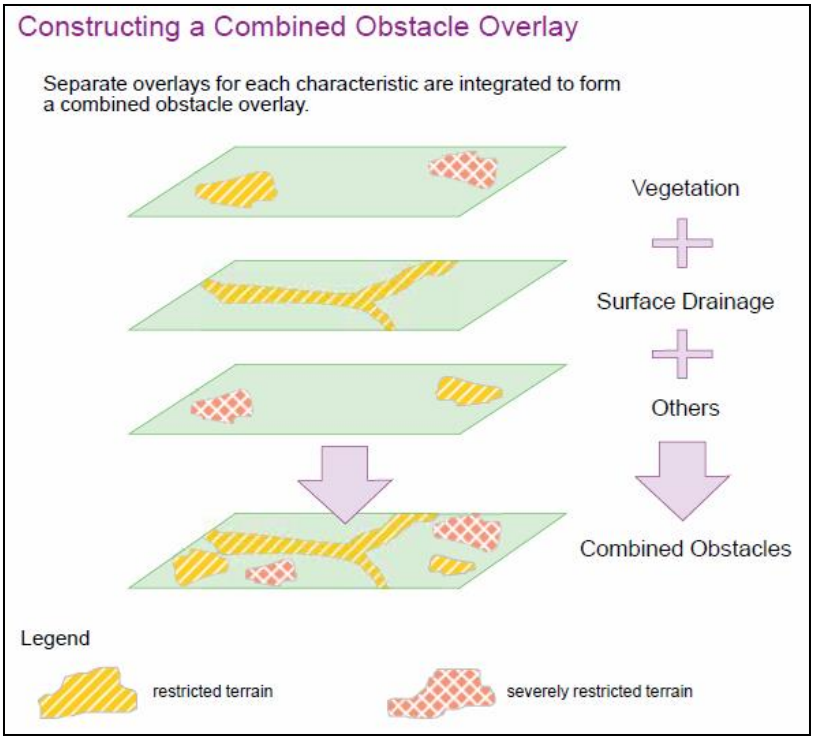



**Figure 6 - Constructing a Combined Obstacle Overlay**

***Source*: US Department of Defense, Joint Intelligence Preparation of the Operational Environment, III-5.**

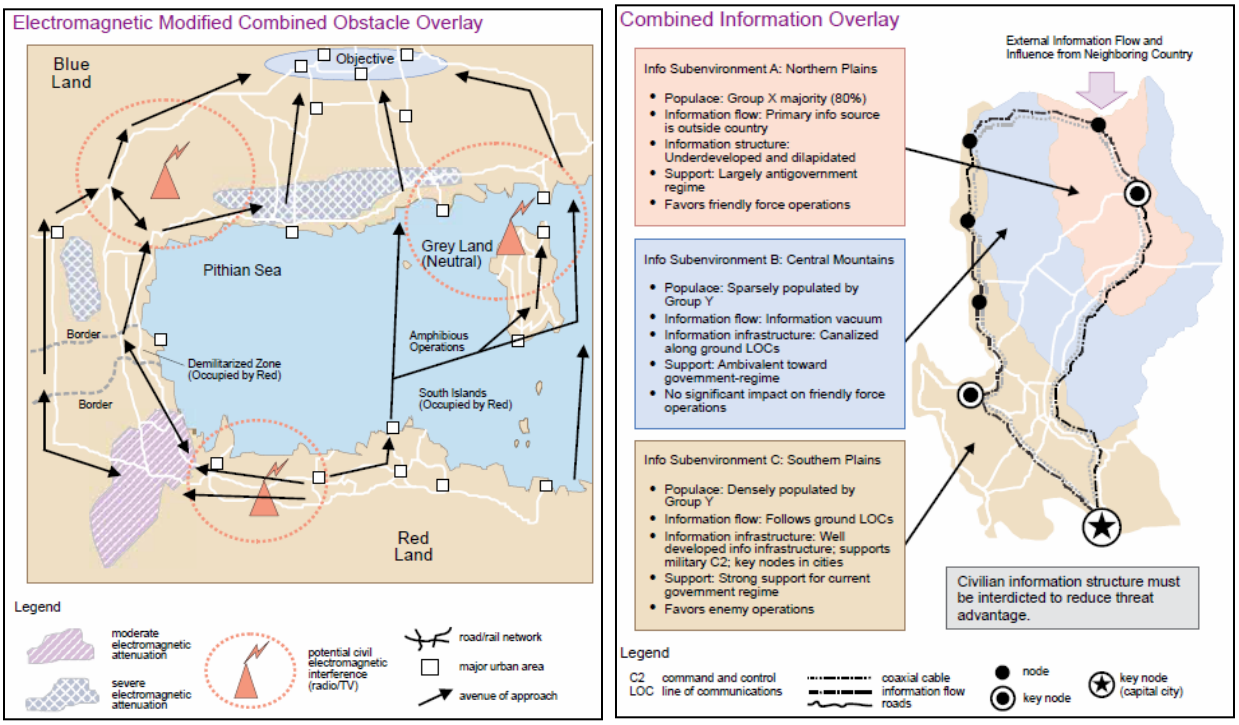



**Figure 7 - Electromagnetic Modified Combined Obstacle & Combined Information Overlay**

**Source: US Department of Defense, Joint Intelligence Preparation of the Operational Environment, III-28.**

Figure 8 illustrates a basic notional build for a cyber AOI and area of influence utilizing the obstacle overlay method from JP 2-01.3. The entire graphic depicts cyberspace and conventional elements in the physical world with a depiction of cyberspace elements in the logical and persona layers. It is important that a commander or decision maker can see the pertinent cyberspace elements within all cyberspace layers in an AOI or area of influence graphic without having to try and decipher how the physical world relates to the logical and persona layer. The physical layer would be built with the same terrain characteristics as any standard conventional combined obstacle overlay, and friendly and adversary conventional units could be added. The symbol for each friendly unit is encircled by a cyberspace graphic depicting its cyber network defense. Each adversary unit symbol is encircled by a cyberspace graphic depicting a network utilized by the unit and the authority level required to conduct OCO against it. The adversary units are represented in both the physical and logical areas of the graphic since the physical location of an adversary may be outside the physical bounds of an operation's area of influence. The adversary depictions would be based on intelligence reporting that indicates the cyber targets and networks that are present in the physical, logical, and persona layers. Just as with the physical domains, intelligence reporting will be instrumental in developing graphics and overlays for any tactical use of COs. As with any graphical representation, all possible elements are not depicted and only the most pertinent to the mission objectives or any combination of most likely and most dangerous COAs for the adversary. In the scenario depicted in Figure 8, the friendly forces (blue) objective is to secure a key chemical weapons storage facility. They may encounter cyberspace actors within their physical area of influence, and also cyberspace actors that reside outside the physical area of influence of the JTF. The primary goal is to ensure the

seizure or destruction of the chemical weapons and the freedom of movement for friendly land and air units.

Figure 8 utilizes the symbols from the electromagnetic and information overlays from JP 2-01.3 because these overlays portray key cyber terrain elements in the physical domain. The conventional military unit symbols were pulled from the US Marine Corps University's Briefing Graphics file, which was created from the DOD publications: MIL-STD-2525B, Field Manual (FM) 101-5-1/Marine Corps Reference Publication (MCRP) 5-12A Operational Terms and Graphics, and MCRP 5-12D Organization of the Marine Corps Forces.[41]

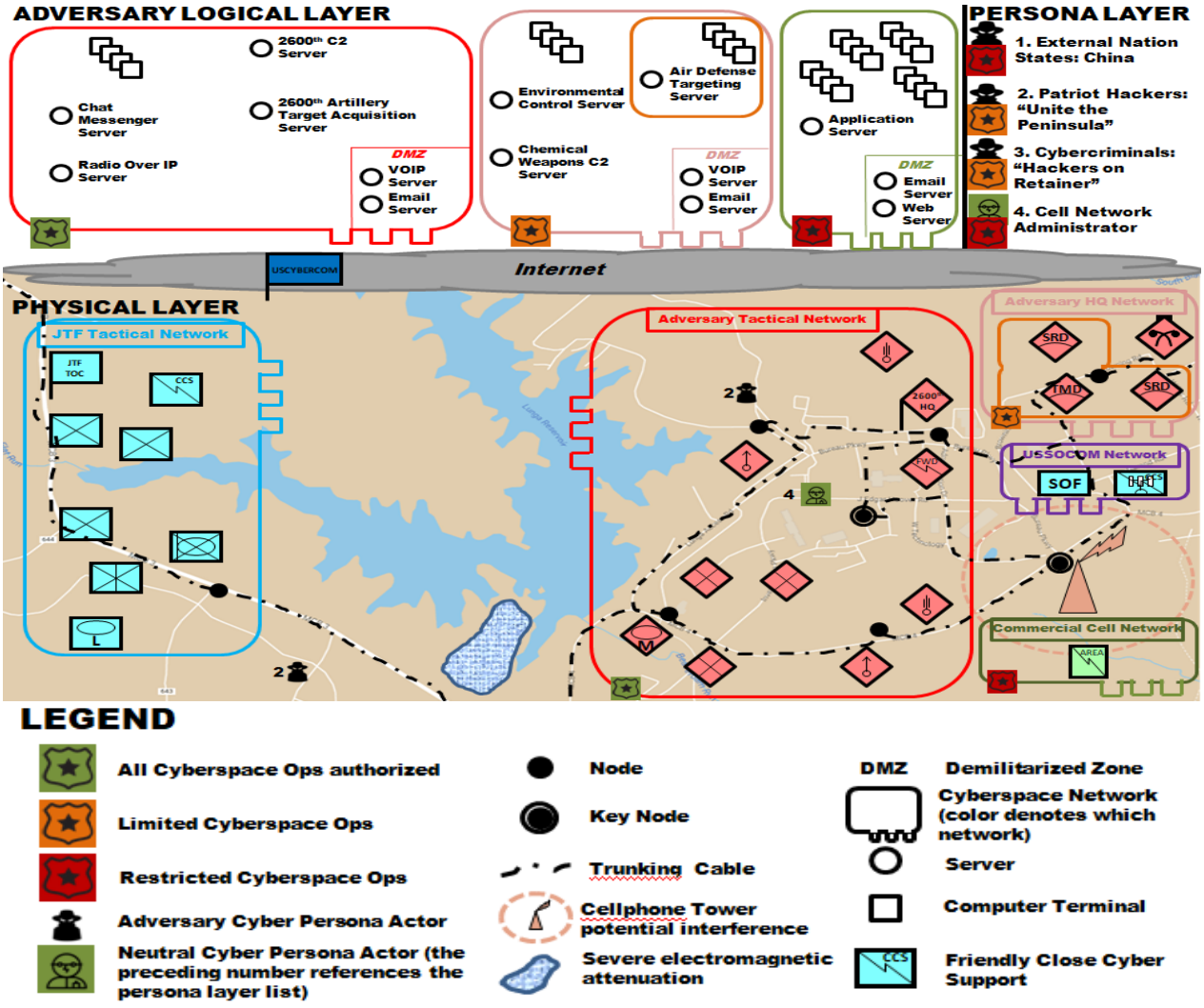



**Figure 8 - Notional Cyberspace Battlefield with all three layers depicted**

The other icons were developed for this paper to indicate to the decision maker the level of authority that is required to engage the adversary or neutral network and to identify the cyber actors at the physical and persona layers. The sheriff badge was selected as the symbol to denote authority since it is universally known as a symbol of authority. The badge was then filled in with a corresponding color to denote where the authority lies to conduct CO on that network or persona (see Figure 9). Green indicates that the commander responsible for the cyber area of influence, JTF commander in this scenario, depicted in the overlay can implement any COs against that target. Orange indicates that the JTF commander can only implement a select few COs and has to request support from higher headquarters. Red indicates that the JTF commander is restricted from conducting any COs against the network or persona and must be cognizant of any collateral damage that may impact these networks or personas.

**Figure 9 – Notional CO Authority Icons (Green = All, Orange = Limited, Red = Restricted)**

The icon selected for the adversary cyber persona actors have some universal recognition as the traditional cyber hacker is commonly referred to as a "black hat." The other icon is a generic symbol representing a neutral cyber persona actor and has a green background to reinforce the actor's neutrality (see Figure 10). The icons could be substituted for actual images of the individuals controlling the cyber personas if the intelligence section is able to provide this level of detail. Lastly, these icons are used in both the physical and persona layers in the graphic with the use in the physical layer to denote a known physical location for a specific actor and the persona layer to list the most significant cyber actors for a specific cyber AOI.


**Figure 10 - Notional Cyber Persona Actor Icons (Adversary, Neutral, and example image)**

In addition to the new icons, an already existing symbol, forward communications, was changed to denote the recommendation expressed in this paper to authorize COs to be executed at the operational and tactical level. The only change to the existing symbol was to change the text modifier to read CCS instead of FWD (see Figure 11). This informs the JTF commander of the presence of a fully operational CCS unit attached to his JTF. The actual composition and capabilities of a typical CCS unit is outside the scope of this paper, and for this scenario it is assumed that the CCS unit can conduct all required COs in an A2AD environment.

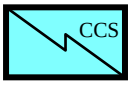



**Figure 11 - CCS symbol**

Lastly, USCYBERCOM was represented with a Headquarters symbol with the text modifier as USCYBERCOM and was placed in the Internet cloud region of the graphic. The cloud represents the bridge between the logical and physical layers depicted in the graphic. This cloud could be changed to a specific communication network if the COs will be executed on a network not connected to the Internet, such as a power plant or utility network a.k.a. a Supervisory Control and Data Acquisition (SCADA) network. Since USCYBERCOM resides physically outside of the area of influence, the best way to represent it was to place it within the Internet cloud. The JTF commander would not be concerned with a logical layer representation of USCYBERCOM's network because the commander is only concerned with the OCO effects that USCYBERCOM can levy against the adversary networks. Also there is no logical or persona layer representation of any friendly communication network because in this scenario the JTF commander was more concerned with COs against the adversary than the defense of friendly networks. As with any planning tool, this graphic can be tailored to meet the priorities of the commander to focus on OCO, DCO, or a combination of both. This prioritization would be based heavily on intelligence reporting of friendly network vulnerabilities within cyberspace.

In order to showcase the additional benefits of representing all three cyberspace layers, a notional battle in cyberspace is represented in Figure 12. The action taken by both forces utilize the actions developed by Mock and McCroskey, see Appendix B, and also utilizes a textbox description for each action taken with the corresponding number to indicate the order of battle. Each action is color coordinated to match which cyberspace entity is conducting the operation. Some of the major benefits of presenting COs in this manner are that the commander can visualize the conventional forces and the physical effects that can be achieved by some of the COs, see actions #2 and 8. This graphic also illustrates to the commander the importance of adhering to correct authorities to conduct COs. In this scenario, the JTF commander only has the authority to execute COs against the 'Adversary Tactical Network' and thus requests additional support from USCYBERCOM to conduct actions against the 'Adversary HQ Network' and the cyber persona 'patriot hackers.'

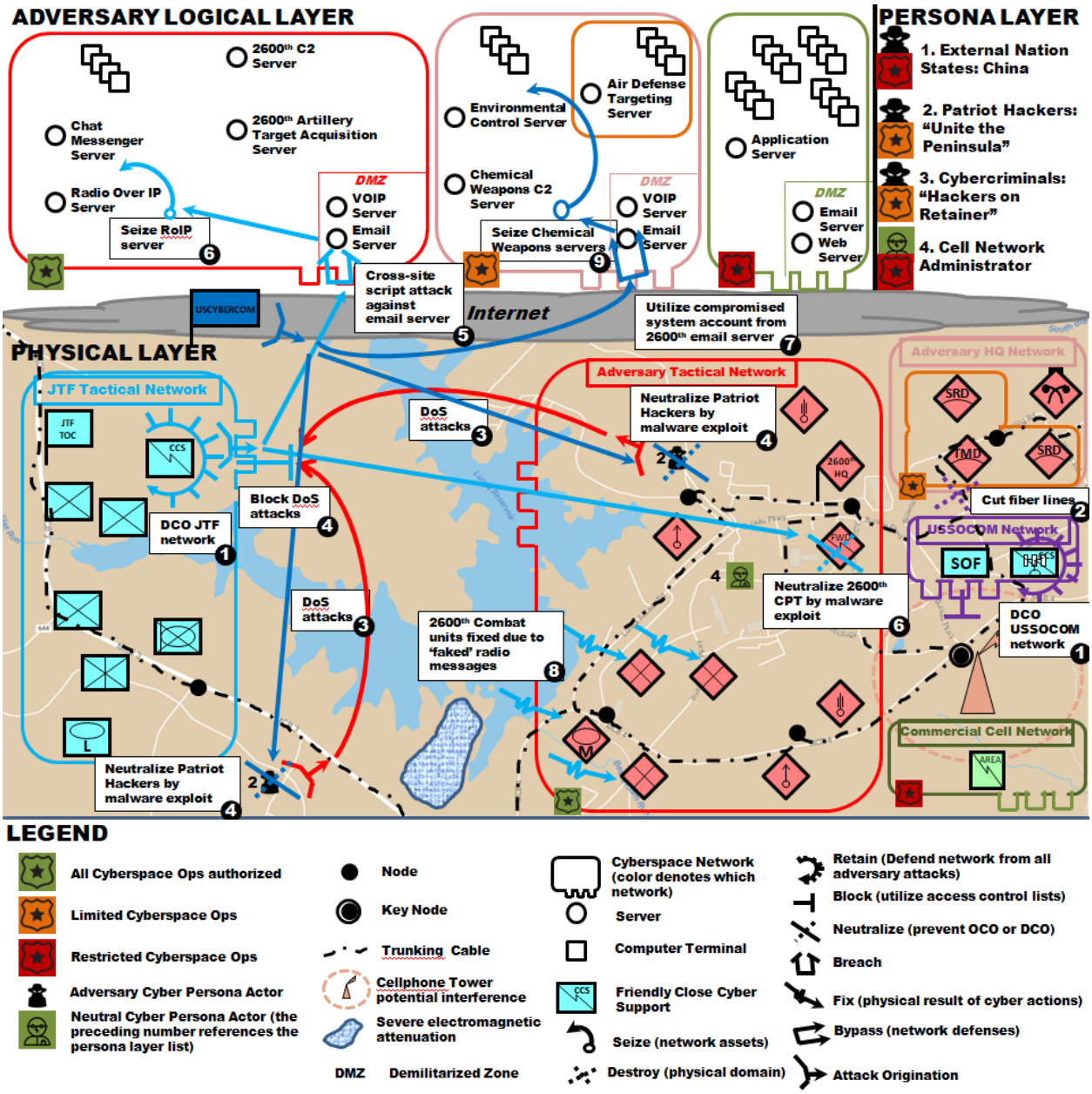



**Figure 12 - Notional Cyberspace Battlefield with CO and physical operations depicted across all three layers**

*Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.*
**Sun Tzu**[42]

## CONCLUSION

The US military has to prepare for conflict in an A2AD environment, and the reliance on cyberspace for most weapon systems and command and control systems requires the authority to conduct CO at the tactical level. This shift from strategic level employment of CO to operational and tactical level employment will become a standard in the same way CAS has become for troops on the ground. Once the battlefield commander is given the authority to conduct COs, the commander will benefit greatly from an accurate depiction of cyberspace across all three layers.

The graphic representation presented in this paper integrated previous efforts to represent cyberspace into a combined arms graphic that represented conventional forces and cyberspace forces along with their effects. This combined graphic allows the commander to identify where COs can be conducted and how their employment will impact the conventional forces. Commanders will be more likely to employ CO if they can visualize the relationship to their conventional forces and the CO effects levied against enemy forces.

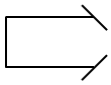
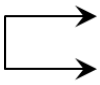
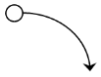
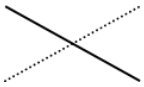
The most ideal graphical representation of cyberspace with conventional forces would include a human-machine automation system, such as PlanX, that could provide a commander with real-time updates to the battlefield. The existing graphical representations including the one proposed in this paper is only beneficial in the planning and post execution phases of an operation. The effects in cyberspace occur so quickly that there has to be an automated system to track COs during the execution phase. The ability to track CO effects in real time will remove much of the stigma preventing CO employment and the US military will need to develop this capability.

JP 3-12 clearly states what commanders and planners need to understand in regards to cyberspace, “while many elements of cyberspace can be mapped geographically in the physical domains, a full understanding of an adversary’s posture and capabilities in cyberspace involves understanding the underlying network infrastructure, a clear understanding of what friendly forces or capabilities might be targeted and how, and an understanding of applicable domestic, foreign, and international laws and policy.”[43] The cyber community will continue to develop and refine existing processes and systems to provide a clear and simple representation of cyberspace. Commanders and planners do not need to understand every minute detail of the cyberspace domain, but once CO authority is delegated down they will need the ability to understand the cyber AOI and area of influence for their OE.

**APPENDIX A: ACRONYMS**

| | |
|---|---|
| A2AD | Anti-Access Area Denial |
| AOI | Area of Interest |
| CAS | Close Air Support |
| CCD COE | Cooperative Cyber Defence Centre Of Excellence |
| CCMD | Combatant Command |
| CCS | Close Cyber Support |
| CCSS | Close Cyber Security Support |
| CO | Cyberspace Operations |
| COA | Course of Action |
| CONOP | Concepts of Operations |
| COP | Common Operating Platform |
| DARPA | Defense Advanced Research Projects Agency |
| DCO | Defensive Cyberspace Operations |
| DoS | Denial of Service |
| DOD | Department of Defense |
| ICCRTS | International Command & Control Research & Technology Symposium |
| JFCCC | Joint Force Cyberspace Component Commander |
| JP | Joint Publication |
| JTF | Joint Task Force |
| MDMP | Military Decision Making Process |
| NATO | North Atlantic Treaty Organization |
| OE | Operational Environment |
| PACE | Primary, Alternate, Contingency, Emergency |
| RAF | Royal Air Force |
| SCADA | Supervisory Control and Data Acquisition |
| TTP | Tactics, Techniques, and Procedures |
| USCYBERCOM | United States Cyber Command |
| USSOCOM | United States Special Operations Command |

## APPENDIX B: ABBREVIATED CYBERSPACE TACTICAL TASK GRAPHICS[44]

| Tactical Task | Operational Graphic | Doctrinal Description[1] | Potential Use in Describing Cyberspace Operations |
|---|---|---|---|
| Attack by fire |  | The use of direct fires, supported by indirect fires, to engage an enemy force without closing with the enemy to destroy, suppress, fix, or deceive that enemy. | Overt actions where an origination (or interim relay) point can be determined, such as Distributed Denial of Service attacks, broad intrusive scans, where these actions create the intended effect on the target. |
| Breach |  | Break through or establish a passage through an enemy defense, obstacle, minefield, or fortification. | Non-credential-based access (e.g., penetration through a firewall, using an exploit or hacking tradecraft). |
| Bypass |  | Maneuver around an obstacle, position, or enemy force to maintain the momentum of the operation while deliberately avoiding combat with an enemy force. | Credential-based access (use captured credentials for login). |
| Retain |  | Ensure that a terrain feature controlled by a friendly force remains free of enemy occupation or use. | Defense of a network device or domain to prevent any adversary access. |
| Seize |  | Take possession of a designated area by using overwhelming force. | Gain control of a device, network, data, or credentials. In cyberspace, two opposing forces *may* have simultaneous control of any or all of these assets. |
| Block |  | Deny the enemy access to an area or prevents the enemy's advance in a direction or along an avenue of approach.<br><br>Also an obstacle effect that integrates fire planning and obstacle efforts to stop an attacker along a specific avenue of approach or prevent the attacking force from passing through an engagement area. | Use or modification of blacklists, whitelists, access control lists, routing policies, credentials (username-password pairs, or machine-issued), or filters on firewalls, DNS servers, domain controllers, web servers, email servers, or others to prohibit or terminate access based on specific criteria. |
| Neutralize |  | Render enemy personnel or materiel incapable of interfering with a particular operation. | Any action taken against another cyberspace *unit* that prevents it from using its offensive or defensive capabilities (e.g., interrupt the sensor feeds from a target domain to the responsible cyber defense unit). |

1As described and depicted in various DOD sources, including: MIL-STD-2525D, Joint Military Symbology, 10 June 2014; FM-102/MCRP 5-12A, Operational Terms and Graphics, 2 February 2010 (incorporating Change 1); FM 3-90-1, Offense and Defense, Volume 1, March 2013; FM 3-90-2, Reconnaissance, Security and Tactical Enabling Tasks, Volume 2, March 2013.

**NOTES**

[1]Gary Brown and Kurt Sanger, "Mattis Faces a Challenge in Equipping US to Engage in Cyberwarfare," *The Hill* (February 6, 2017): http://thehill.com/blogs/pundits-blog/defense/318009-mattis-faces-a-challenge-in-equipping-us-to-engage-in-cyberwarfare.

[2]Peter Matthews, *SIGINT: The Secret History of Signals Intelligence 1914-45* (Stroud, UK: The History Press, 2013), 23.

[3]Ibid., 22-23.

[4]Eneken Tikk, Kadri Kaska, and Lils Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010), 25.

[5]Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the "First Battle" in 21st-century War," *Defense Horizons* 68 (September 2009): 3.

[6]Jared Serbu, "DOD Declassifies its Long-Awaited Joint Doctrine for Cyberspace Operations," *Federal News Radio* (October 27, 2014): https://federalnewsradio.com/defense/2014/10/dod-declassifies-its-long-awaited-joint-doctrine-for-cyberspace-operations/.

[7]US Department of Defense, *The DOD Cyber Strategy*, (Washington, DC, April 2015), 3, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf.

[8]Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 43, http://www.c4i.org/unrestricted.pdf.

[9]*Roles and Responsibilities for Defending the Nation from Cyber Attack: Hearing before the Senate Armed Services Committee*, 115th Cong., 10 (2017) (statement of Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense & Global Security).

[10] US Department of Defense, *Cyberspace Operations*, JP 3-12 (R) (Washington, DC: Headquarters Chairman of the Joint Chiefs of Staff, February 5, 2013), I-2-I-4.
[11]Brown and Sanger, "Mattis Faces a Challenge." Gary Brown served as senior legal counsel for USCYBERCOM and Kurt Sanger is a judge advocate in the US Marine Corps as of February 2017.

[12]Mark Reith, Seeley Pentecost, Daniel Celebucki, and Robert Kaufman, "Operationalizing Cyber: Recommendations for Future Research," *International Conference on Cyber Warfare and Security;* (Reading: 295-XVI Academic Conferences International Limited, 2017), 195-297.

[13]McCroskey, Erick D., and Charles A. Mock. "Operational Graphics for Cyberspace." *Joint Force Quarterly* 85, no. 2 (April 2017): 44.

[14]US Department of Defense, *Cyberspace Operations*, II-10.

[15] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collings Publishers, 2010), 155-157.
[16]Patrick Tucker, "For the US Army, 'Cyber War' is Quickly Becoming Just 'War'," *Defense One*, February 9, 2017, http://www.defenseone.com/technology/2017/02/us-army-cyber-war-quickly-becoming-just-war/135314/.

[17]Mark Pomerleau, "Here's How DOD Organizes its Cyber Warriors," *Fifthdomain.com*, July 25, 2017, https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/.

[18]Wesley Morgan, "U.S. Army Unprepared to Deal with Russia in Europe," *Politico.com*, September 2, 2017, https://www.politico.com/story/2017/09/02/army-study-173rd-airborne-brigade-europe-russia-242273.

[19]Williamson Murray and Allan R. Millet, ed., *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1996), 152.

[20]Royal Air Force Museum, "British Military Aviation in 1918," *Royal Air Force Museum*, accessed December 20, 2017, https://www.rafmuseum.org.uk/research/history-of-aviation-timeline/interactive-aviation-timeline/british-military-aviation/1918.aspx.

[21] Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND, 2017).

[22]Michele Turi, Agatino Mursia, Giuseppe Giannandrea, and Agostino G. Bruzzone, "Cyber Security: CCSS – Close Cyber Security Support: An Accessible Way to Protect Critical Information in a Tactical Environment," *Command and Control Research and Technology Symposium* (June 2013): http://www.hsdl.org/?abstract&did=754691.

[23] US Department of Defense, *Close Air Support*, JP 3-09.3 (Washington, DC: Headquarters Chairman of the Joint Chiefs of Staff, November 25, 2014), I-1 – I-3 and US Department of Defense, *Cyberspace Operations*, II-5.

[24]Ibid.

[25]US Department of Defense, *Cyberspace Operations*, IV-7.

[26]David Vergun, "Commanders Need Latitude to Employ Offensive Cyber, Says GEN Thomas," *Army News Service*, December 12, 2017, https://www.army.mil/article/198071/commanders_need_latitude_to_employ_offensive_cyber_says_gen_thomas.

[27]US Department of Defense, *Joint Intelligence Preparation of the Operational Environment*, JP 2-01. 3 (Washington, DC: Headquarters US Joint Chiefs of Staff, May 21, 2014), II-5.

[28] McCroskey and Mock, "Operational Graphics for Cyberspace," 44.

[29]US Department of Defense, *Cyberspace Operations*, IV-1 – IV-2.

[30]US Department of Defense, *Cyberspace Operations*, IV-9.

[31]US Department of Defense, *Joint Intelligence Preparation of the Operational Environment*, II-6.

[32]Matthew Stern, "Applying Military Doctrine to Cyberspace: Areas of Operation, Influence and Interest," *Security Week*, September 2012, http://www.securityweek.com/applying-military-doctrine-cyberspace-areas-operation-influence-and-interest.

[33]"The History of a Picture's Worth," accessed January 11, 2018, http://www2.cs.uregina.ca/~hepting/research/web/words/history.html#21ad.

[34]Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73, no. 2 (April 2014): 13.

[35]US Department of Defense, *Cyberspace Operations*, I-1.

[36]Tucker, "For the US Army, 'Cyber War' is Quickly Becoming Just 'War'."

[37]Erick D. McCroskey, and Charles A. Mock. "Operational Graphics for Cyberspace." *Joint Force Quarterly* 85, no. 2 (April 2017): 42-49.

[38]Information Innovation Office, "PlanX Technical Overview DRAFT IV," (working paper, Defense Advanced Research Projects Agency, 2017), 5.

[39]Information Innovation Office, "PlanX Technical Overview DRAFT IV," 13.

[40]Gregory Conti, John Nelson, and David Raymond, *Towards a Cyber Common Operating Picture.* 5th International Conference on Cyber Conflict, (Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre Of Excellence, 2013), 8, https://ccdcoe.org/cycon/2013/proceedings/d1r2s4_conti.pdf.

[41]William L. Simpson, *Briefing Graphics & Unit Symbols* (Marine Corps University, Quantico, VA, December 1, 2015), PowerPoint presentation.

[42]Sun Tzu, "Sun Tzu Quotes," *Brainy Quote,* accessed January 18, 2018, https://www.brainyquote.com/quotes/sun_tzu_387509.

[43]US Department of Defense, *Cyberspace Operations*, IV-1.

[44]Erick D. McCroskey, and Charles A. Mock. “Operational Graphics for Cyberspace.” *Joint Force Quarterly* 85, no. 2 (April 2017): 46-47.

**BIBLIOGRAPHY**


Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham, MA: Syngress, 2011.

Bodeau, Deborah, Richard Graubart, and William Heinbockel. *Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to be Stated and Evaluated with Greater Rigor and Utility.* Mitre Technical Report MTR130433. Bedford, MA: Mitre Corporation, November 2013. https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf.

Brown, Gary, and Kurt Sanger. "Mattis Faces a Challenge in Equipping US to Engage in Cyberwarfare." *The Hill* (February 6, 2017): http://thehill.com/blogs/pundits-blog/defense/318009-mattis-faces-a-challenge-in-equipping-us-to-engage-in-cyberwarfare.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II.* New York: The Free Press, 2000.

Budiansky, Stephen. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union.* New York: Alfred A. Knopf, 2016.

Bushman, John, Jack Dillon, Michal Padden, and Frank Pound. "X Marks the Spot." US Army Releases, February 27, 2017. https://www.army.mil/article/183310/x_marks_the_spot.

Carr, Jeffrey. *Inside Cyber Warfare.* Sebastopol, CA: O'Reilly Media, Inc., 2012.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collings Publishers, 2010.

Conti, Gregory, John Nelson, and David Raymond. *Towards a Cyber Common Operating Picture.* 5th International Conference on Cyber Conflict. Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre Of Excellence, 2013. https://ccdcoe.org/cycon/2013/proceedings/d1r2s4_conti.pdf.

Duus, Rikke and Mike Cooray. "Information Overload is Killing Our Ability to Make Decisions." *Business Insider,* July 15, 2015. http://www.businessinsider.com/information-overload-is-killing-our-ability-to-make-decisions-2015-7.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling.* Carlisle Barracks, PA: U.S. Army War College Press, 2013.

Harris, Shane. *@War: The Rise of the Military-Internet Complex.* New York: Houghton Mifflin Harcourt Publishing Company, 2014.

Headquarters Chairman of the Joint Chiefs of Staff. *Cyberspace Operations.* JP 3-12 (R). Washington, DC: Headquarters Chairman of the Joint Chiefs of Staff, February 5, 2013.

Information Innovation Office. "PlanX Technical Overview DRAFT IV." Working Paper. Defense Advanced Research Projects Agency, 2017.

Lewin, Ronald. *The American Magic: Codes, Ciphers and the Defeat of Japan.* New York: Farrar Straus Giroux, 1982.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999. http://www.c4i.org/unrestricted.pdf.

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy* 8, no. 2 (Fall 2012): 325-340.

Lopez, C Todd. "Key to Cyber Success: Operators Must Learn Land Operations Language." US Army Releases, November 10, 2015. https://www.army.mil/article/158462/key_to_cyber_success_operators_must_learn_land_operations_language.

Matthews, Peter. *SIGINT: The Secret History of Signals Intelligence 1914-45.* Stroud, UK: The History Press, 2013.

McCroskey, Erick D., and Charles A. Mock. "Operational Graphics for Cyberspace." *Joint Force Quarterly* 85, no. 2 (April 2017): 42-49.

Miller, Robert A., and Daniel T. Kuehl. "Cyberspace and the "First Battle" in 21st-century War." *Defense Horizons* 68 (September 2009): 1-6.

Murray, Williamson, and Allan R. Millet, ed. *Military Innovation in the Interwar Period.* New York: Cambridge University Press, 1996.

National Research Council of the National Academies. *Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making.* Washington, D.C.: The National Academies Press, 2013.

Porche III, Isaac R., Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below.* Santa Monica, CA: RAND, 2017.

Reith, Mark, Seeley Pentecost, Daniel Celebucki, and Robert Kaufman. "Operationalizing Cyber: Recommendations for Future Research." *International Conference on Cyber Warfare and Security;* Reading: 295-XVI Academic Conferences International Limited, 2017.

Riley, Shawn. “Cyber Terrain: A Model for Increased Understanding of Cyber Activity.” *Centre for Strategic Cyberspace and Security Science.* London, UK, August 20, 2016. http://cscss.org/CS/2016/08/20/cyber-terrain-a-model-for-increased-understanding-of-cyber-activity/.

Robinson, Ryan. “Understanding Digital and Cyber Topography is Critical to Successful Military Operations.” *Signal* (July 2015): 40-43.

Serbu, Jared. “DOD Declassifies its Long-Awaited Joint Doctrine for Cyberspace Operations.” *Federal News Radio* (October 27, 2014): https://federalnewsradio.com/defense/2014/10/dod-declassifies-its-long-awaited-joint-doctrine-for-cyberspace-operations/.

Simpson, William L. *Briefing Graphics & Unit Symbols.* PowerPoint presentation. Marine Corps University, Quantico, VA, December 1, 2015.

Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press, 2014.

Stern, Matthew. “Applying Military Doctrine to Cyberspace: Areas of Operation, Influence and Interest.” *Security Week*, September 2012. http://www.securityweek.com/applying-military-doctrine-cyberspace-areas-operation-influence-and-interest.

Tikk, Eneken, Kadri Kaska, and Lils Vihul. *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010.

Tucker, Pat. “For the US Army, ‘Cyber War’ is Quickly Becoming Just ‘War’.” *Defense One* (February 9, 2017): http://www.defenseone.com/technology/2017/02/us-army-cyber-war-quickly-becoming-just-war/135314/.

Turi, Michele, Agatino Mursia, Giuseppe Giannandrea, and Agostino G. Bruzzone. “Cyber Security: CCSS – Close Cyber Security Support: An Accessible Way to Protect Critical Information in a Tactical Environment.” *Command and Control Research and Technology Symposium* (June 2013): http://www.hsdl.org/?abstract&did=754691.

US Department of Defense. *Close Air Support.* JP 3-09.3. Washington, DC: Headquarters Chairman of the Joint Chiefs of Staff, November 25, 2014.

US Department of Defense. *Cyberspace Operations.* JP 3-12 (R). Washington, DC: Headquarters US Joint Chiefs of Staff, February 5, 2013.

US Department of Defense. *Joint Intelligence Preparation of the Operational Environment.* JP 2-01. 3. Washington, DC: Headquarters US Joint Chiefs of Staff, May 21, 2014.

US Department of Defense. *The DOD Cyber Strategy.* Washington, DC, April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf.

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly* 73, no. 2 (April 2014): 12-19.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Waltham, MA: Syngress, 2013.