

**REPORT DOCUMENTATION PAGE**

*Form Approved  
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.  
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 10-05-2019		<b>2. REPORT TYPE</b> Master's of Military Studies		<b>3. DATES COVERED (From - To)</b> SEP 2018 - APR 2019	
<b>4. TITLE AND SUBTITLE</b> Shifting Priority: The Case for Cyber Resilience and Techniques for Employment				<b>5a. CONTRACT NUMBER</b> N/A	
				<b>5b. GRANT NUMBER</b> N/A	
				<b>5c. PROGRAM ELEMENT NUMBER</b> N/A	
<b>6. AUTHOR(S)</b> Sealey II, Reginald, M., Major, USMC				<b>5d. PROJECT NUMBER</b> N/A	
				<b>5e. TASK NUMBER</b> N/A	
				<b>5f. WORK UNIT NUMBER</b> N/A	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b> N/A	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b>				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b> Jorge Benitez, Ph.D.	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b> N/A	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> Approved for public release, distribution unlimited.					
<b>13. SUPPLEMENTARY NOTES</b>					
<b>14. ABSTRACT</b> The future operating environment requires the Joint Force to sense and share information to locate and close with adversary formations under the threat of degraded networked communications. This scenario requires the elevation of resilience in USCYBERCOM's strategy with a focus on engineering, tailored defense, and deception together with trained personnel and repeatable processes that take greater priority over the development and implementation of offensive and defensive cyber weapons. This paper examines the reasons surrounding the shift in priority while exploring					
<b>15. SUBJECT TERMS</b> Cyber, Cyberspace, Cyber Resilience, Cyberspace Resilience, Cyberspace Deterrence					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	42	<b>19b. TELEPHONE NUMBER (Include area code)</b> (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: Shifting Priority: The Case for Cyber Resilience and Techniques for Employment**

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


**AUTHOR: Major Reginald Morris Sealey II, United States Marine Corps**

AY 2018-19

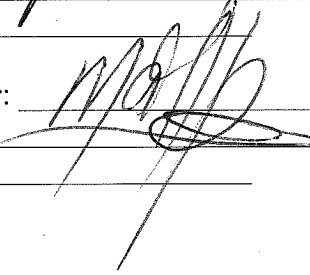
---

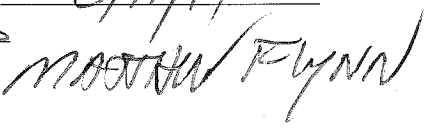
---

Mentor and Oral Defense Committee Member: Jorge Benitez, Ph.D.

Approved: 

Date: May 11, 2019

Oral Defense Committee Member:  5/11/19

Approved: 

Date: \_\_\_\_\_

## Executive Summary

**Title:** Shifting Priority: The Case for Cyber Resilience and Techniques for Employment

**Author:** Major Reginald Morris Sealey II, United States Marine Corps

**Thesis:** If the future operating environment requires the Joint Force to sense and share information to locate and close with adversary formations under the threat of degraded networked communications, then USCYBERCOM's strategy must elevate resilience with a focus on resilience through engineering, tailored defense, and deception together with trained personnel and repeatable processes that take greater priority than the development and implementation of offensive and defensive cyber weapons.

**Discussion:** The USCYBERCOM vision statement includes a three-pronged approach that embraces resiliency, defending, and contesting to achieve a more stable and secure cyberspace. However, USCYBERCOM is investing more of its funding towards the development of offensive cyberspace capability to create effects in support of Joint Force Commander objectives and defend forward through a strategy of persistent engagement. The persistent engagement strategy is more focused on nuclear deterrence theory, where the threat of punishment shapes decision making. This approach also unbalances USCYBERCOM's vision and neglects the less attractive parts like resilience. Shifting the priority to invest more in resilience can deter adversaries in cyberspace by imposing time and cost while enabling the Joint Force to rapidly project networks as a military instrument in support of kinetic operations. Resilience also supports operations in a degraded environment and offers options to make networks more secure, survivable, and available.

**Conclusion:** Shifting the priority to resilience enables the Joint Force to be better postured for the future operating environment but involves significant change to how communication officers employ networks in support of operations. Tailoring defenses, implementing deception techniques, solidifying processes, and investing in training allow the Joint Force to adapt and anticipate the trials to come while also preparing communication planners at all levels to assure the network or provide off ramps that facilitate C2 in future war.

## DISCLAIMER

THE OPINIONS AND CONCLUSIONS 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. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

*Table of Contents*

	Page
TITLE PAGE .....	i
EXECUTIVE SUMMARY .....	ii
DISCLAIMER .....	iii
TABLE OF CONTENTS.....	iv
PREFACE.....	v
REPORT DOCUMENTATION PAGE.....	vi
INTRODUCTION/PROBLEM .....	1
THE CURRENT US GOVERNMENT APPROACH TO CYBERSPACE.....	3
IMPROVING SECURITY AND STABILITY THROUGH RESILIENCE .....	7
RESILIENCE THROUGH ENGINEERING .....	7
RESILIENCE THROUGH TAILORED DEFENSE.....	13
RESILIENCE THROUGH DECEPTION .....	15
RESILIENCE THROUGH PEOPLE AND PROCESSES.....	18
CONCLUSION.....	20
ENDNOTES .....	22
BIBLIOGRAPHY.....	27

## *Preface*

In order to compete in the future operating environment, the Joint Force must be adaptive and agile. As it pertains to cyberspace, we must not assume that the network will be available when we need it during a near-peer conflict. Rather, we must assure its existence in support of military operations. That is my job as a communications officer: facilitate the Commander's ability to command & control, through the rapid projection of cyber capability. This paper rests on the thought that as cyber warriors, communicators, and signallers, we not only maneuver personnel and capability in defense of the network but we must also maneuver the network in defense of itself. For this reason, I took the position that resilience in cyberspace can deter and provide the necessary capability to outpace our adversaries. Three reasons motivated my interest in the topic. First, USCYBERCOM's approach seemed more offensive than defensive. Coming from Joint Force Headquarters Department of Defense Information Networks (JFHQ-DODIN), the organization charged with Command & Control in defense of the DODIN, I was naturally drawn towards operating in the defense and have come to believe that the defense is the stronger form of warfare in cyberspace. Second, I believe that resilience is a viable option to address the cyber deterrence dilemma. Finally, communication officers have a role to play in assuring networks in the future environment; however, there are critical shortfalls in the planning and employment of networks that may leave future formations isolated. With hope, this paper can inform strategy and trigger investment in new concepts. A special thanks to my family for supporting me throughout the year, my friends for encouragement and uplift, former and present JFHQ-DODIN colleagues, and my classmates, professors, and mentors for imparting the knowledge and wisdom necessary to prepare for the unknown.

## **INTRODUCTION/PROBLEM**

The 2018 United States Cyberspace Command (USCYBERCOM) vision statement describes, a three-pronged approach to cyber space that includes: “The sum of resiliency, defending, and contesting, not one in isolation, will lead to a more stable and secure cyberspace.”<sup>1</sup> However, there is a gap between the current vision and reality. Of the funding requested by USCYBERCOM in fiscal year 2019, the most expensive items trend towards offensive capabilities including joint tools and access platforms used for the employment of offensive cyberspace weapons on adversary targets.<sup>2</sup> USCYBERCOM has taken a more proactive cyberspace posture that includes preemption and a focus on the development of offensive cyber weapons.<sup>3</sup> Their strategic approach to counter and contest adversary gains, through persistent engagement, has consumed many of the top policy makers demanding capabilities to deter in cyberspace.<sup>4</sup> This is partially due to a historical understanding of nuclear deterrence by policy makers without a full appreciation for other forms, such as deterrence through denial and entanglement.<sup>5</sup> While policy makers focus more on the aggressive elements of USCYBERCOM’s strategy, the less attractive pieces are neglected.

General James Cartwright notes that, “We’ve got to talk about our offensive capabilities...to make them credible so that people know there’s a penalty [for attacking the United States].”<sup>6</sup> General Cartwright’s position on brandishing cyberspace capability or swaggering, is often referred to as the ‘Cartwright Conjecture’ and has moved the resiliency conversation to the backburner without giving it proper priority in assuring missions in future conflict.<sup>7</sup> Cyber is an effective offensive capability for strike operations however, it is also a powerful enabler spanning across all domains. The addition of plug and play services adds capability to warfighters that have the potential to increase lethality but, with more services,

there is also more risk. Whenever cyber power is primarily based on military disruption, regardless of the skill of the operators, the resilience part of cyber power is often neglected.<sup>8</sup>

The demand for availability of technology increases with technological advance. This increase in demand requires new techniques to increase availability while addressing confidentiality and integrity as factors of resilience. Even IBM Chief Technical Officer, Cindy Compant recognizes that, “Being resilient is more critical than ever”, specifically because US critical infrastructure is constantly at risk from cyber actors.<sup>9</sup> According to Compant, what keeps her up at night is not whether US critical infrastructure will be attacked, but how fast the US can respond and recover from such attacks.<sup>10</sup> While resilience has a critical role in business, the risks are even greater in military operations because lives may depend on the continuity of operations and survivability of communications networks. When networks are threatened, degraded, or even destroyed, US advantage erodes, and operations can suffer. Therefore, a focus on resiliency must not only be elevated in USCYBERCOM’s current operational approach, but it must also be made a Joint Force priority when planning for future war.

Risks to networks are increasing with the rapid proliferation of technology. These risks present themselves in several ways including; increased vulnerabilities, adversary sophistication, environmental risks affecting communication networks, and increased threat of physical destruction in the face of future conflict. These risks also come with increasing difficulty in defense. Therefore, the Joint Force must assume these risks will come to fruition while aiming to mitigate their impact in order to continue the mission. Resilience provides the Joint Force with an alternative to heavy investments in offensive cyberspace capability and has become the main focus in many successful cybersecurity strategies in the private sector. Resilience provides the capability to continue the mission when faced with such adversities however, increasing the



resilience posture is by no means easy. Effective resilience requires improvements to multiple different actions: engineering, tailored defense, deception, and personnel training and education. Improvements in all of these areas will better prepare the Joint Force for the future operating environment while providing more safety and security in cyberspace versus the current cyber-offensive-centric approach.

### **The Current US Government Approach to Cyberspace**

Preparation for future war requires a Joint Force capable of operating in a contested space and cyberspace environment. A key assumption that planners often take into account when planning cyberspace operations is that adversaries already have access. This access often includes placing well-hidden implants without tripping alarms. USCYBERCOM openly recognizes peer competitors in cyberspace and concludes that cyberspace superiority is under continual stress.<sup>11</sup> Former Cisco Chief Executive Officer, John Chambers stated that, “there are two types of companies: those that have been hacked and those who don’t know they have been hacked.”<sup>12</sup> Different from other domains, the Joint Force is in contact with adversaries in cyberspace constantly. For example, after talks with USCYBERCOM’s defensive operational headquarters, Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DODIN), Frank Konkel of Nextgov stated: “Every day, the Defense Department thwarts 36 million emails full of malware, viruses and phishing schemes from hackers, terrorists and foreign adversaries trying to gain unauthorized access to military systems.”<sup>13</sup> Cyber insecurity and information warfare attacks often fall in the gray zone, just below the threshold for kinetic response.<sup>14</sup> USCYBERCOM assumes that adversary behavior in cyberspace is intentionally set below the level of armed conflict.<sup>15</sup> This enables adversaries to execute campaigns to degrade US power while avoiding significant armed US reactions.<sup>16</sup> Therefore, peer competitors are

increasingly taking advantage of gray zone activities and escalating in cyberspace to achieve their ends without fear of escalation to armed conflict. Moore's Law further complicates the situation, which states, "the number of electronic components (transistors, resistors, capacitors) that could be squeezed onto integrated circuits would double every year for a decade."<sup>17</sup> Not only is the amount of computing power, devices, and cyberspace personas exponentially growing, but the attack surface, avenues of approach, and vulnerabilities of networks are also continuing to increase as a function of Moore's Law. In the case Moore's Law is disproven, technological increases may slow but will continue to increase with time.

The assumption that defenses are impenetrable or will effectively deter adversaries may be no more successful than the French construction of the Maginot Line prior to World War II.<sup>18</sup> Adversaries continue to make it their objective to find a way over, around, or through defenses to achieve their aims. Originally, the French envisioned the Maginot Line as a force multiplier (a device to enhance resilience) to free manpower for offensive operations so that the French could absorb blows and reallocate forces to counterattack.<sup>19</sup> Instead of prioritizing resilience, the French prioritized security and hunkered down behind the Maginot Line while failing to reallocate sufficient forces to defend gaps in the Ardennes.<sup>20</sup> Instead of relying on passive defense, the Germans won the Battle of France through surprise, mass, and intelligence. France's false assumptions and failure to anticipate also played a role, but it is important for the Joint Force to apply the original vision of the Maginot Line to cyberspace. Focus not on the capability to defend forward and strike preemptive blows or rely on an impenetrable defense, but the ability to absorb and move capability that supports the survivability of the system. Dictate the operational terrain and battlefield geography while forcing the adversary to engage on predetermined times. Seize the initiative and get ahead of adversary decision cycles. This is the

essence of resilience, and for it to be a top priority in the planning and implementation of networks, planners must understand it in terms of the complexities of the cyberspace domain.

In the cyberspace domain, resilience is about how much an organization can recover without losing the ability to execute the mission. This is no different from Rocky Balboa stating, “It’s about how hard you can get hit and keep moving forward.”<sup>21</sup> Although Joint Publication 3-12 Cyberspace Operations mentions cyber resilience as essential to planning, it does not define the term and there is no Department of Defense (DoD) definition available via joint doctrine.<sup>22</sup> The National Institute of Standards and Technology (NIST) in the Department of Commerce defines cyber resilience as, “the ability of an organization to continue to operate in a degraded Information Technology (IT) environment while maintaining operational capabilities and recovering to an effective operational posture in a time frame consistent with mission needs.”<sup>23</sup>

Although there is no definition of cyber resilience in joint publications, a US Army document provides a simple and effective definition: “resilience is the ability to recover from or easily adjust to misfortune or change.”<sup>24</sup> Resilience is different from risk. While risk is a product of threat, vulnerability, and consequence, resilience results from the minimization of the impact of threat actions and the facilitation of recovery.<sup>25</sup> There is also risk in the lack of resilience. The initiative is often ceded to the adversary when there is a lack of resilience. This is modeled in adversary behavior. Adversaries are more prone to escalate when there are perceived weaknesses in resiliency. On the contrary, adversaries tend to get deterred when the resiliency posture is strong. The failure to learn from historic examples, adapt to overwhelming attacks, and anticipate future threats will often lead down the pathway of misfortune.<sup>26</sup>

Therefore, to avoid failure, the Joint Force network must be constantly learning, adapting, and

anticipating, much like a maneuver unit, with an eye towards achieving resilience if availability is to be achieved in the future operating environment.

The future operating environment detailed in both the National Security and National Defense Strategies recognizes the challenges in both space and cyberspace when fighting to win against near-peer competitors. As the Joint Force prepares for the next war, it must consider the overreliance on command and control systems and networks that enable concepts like the Marine Operating Concept (MOC) to be realized. Realization of the MOC requires resiliency to decrease friction in the uncertain and complex future. Jesse Solman describes future battles as, “confusing and disorganized affairs more similar to the clashes of a predigital age.”<sup>27</sup> When the military shifts out of the competition space and potentially into kinetic operations, the communications infrastructure, networks, and systems that the Joint Force is currently accustomed to may not be present. For the Joint Force to overcome heavy losses to networked communications from space, cyberspace, and kinetic destruction, and still accomplish assigned missions, resilient networks that are distributed, survivable, diverse, and agile, need incorporation into current Joint Force actions. The implementation of new ways and means will shape policy and doctrine pertaining to actions in future war. Thus, a focus on resilience in support of military operations and in the face of surmountable losses will be required to be successful now and in the future. The gains in cyber offensive capability and improvements in defense are not discounted, but sadly, resiliency is more often spoken than practiced. If the future operating environment requires the Joint Force to sense and share information to locate and close with adversary formations under the threat of degraded networked communications, then resilience must be elevated in USCYBERCOM’s strategy, with a focus on gaining resilience through engineering, tailored defense, and deception together with trained personnel

and repeatable processes that take greater priority than the development and implementation of offensive and defensive cyber weapons.

### **Improving Security and Stability Through Resilience**

Prioritizing resiliency and elevating it in USCYBERCOM's current operational approach requires improvements in the following focus areas: acquisition of technology, network resilience planning that includes tailoring defense and deception, and training and education for the implementation of resilience across Joint Force networks. Like defense-in-depth, which aims to attrit an attacker while possessing the ability to strike a decisive blow, the above-mentioned focus areas provide a winning strategy that builds and acquires network resilient components, plans resilient networks, and trains personnel to further increase the resilience posture of the organization. Standing alone, these focus areas will serve to increase resilience but only to a limited degree. When integrated together and promulgated with messaging to the Joint Force, gains in resilience will exceed expectation. Ultimately, each focus area addresses the problem the Joint Force faces: the increasing threat to its networks in the future operating environment.

### **Resilience through Engineering**

Resilience through engineering involves the planning and engineering of networks while also considering the engineering of systems in development. The first tenet of Marine Corps's communications is flexibility and must be considered to increase resiliency. When planning the employment of networks, communications planners often design for speed and efficiency versus resiliency. Planning for the employment of 100% of resources is efficient in cost and resources ;however, if networks are 100% efficient, the slightest fault in a system can lead to catastrophic failure.<sup>28</sup> Therefore, networks focused on resiliency will be much different from those built with efficiency in mind.<sup>29</sup> Efficiency works well when operating in a fiscally constrained

environment that mandates certain acquisitions and procurements. For example, the Clinger-Cohen Act, US Code Title 40 directs that processes to maximize the value and manage the risks of IT acquisitions are in place while ensuring information systems are designed, developed, maintained, and used effectively.<sup>30</sup> The Clinger-Cohen act is often in contention with the Goldwater-Nichols Act that governs Joint Force operations. This is due to cyberspace becoming an operational domain in which the money saving focus of efficient acquisition of IT may not necessarily support the security priorities of military operations in cyberspace. In addition, the Chief Information Officer's (CIO) strategy may conflict with the operational commander responsible for cyber terrain. The inherent conflict between efficiency and resilience planning involves flexibility. Planning for flexibility often introduces excess capability and capacity to overcome faults and increase resilience; this often conflicts with efficiency because more systems are employed without necessarily being utilized.<sup>31</sup> Therefore, planners may have to shift the paradigm when it comes to IT acquisition and add more capacity and capability so that networks can absorb more when under attack.

In his work on cyber resilience, Colonel William Bryant concludes that, an imbalance that favors efficiency will hamper resiliency, and the Joint Force should do well to build less-efficient redundant systems if they want to achieve resiliency under attack.<sup>32</sup> Redundancy is also a tenet of Marine Corps's communications and provides Primary, Alternate, Contingency, and Emergency (PACE) capabilities to support command and control and assure networks. However, there are gains to planning for some efficiency. Efficiency enables the ease of management across a network and can help with security. For example, a homogeneous network with the same routers and switches, or servers and clients, gains efficiency and speed when implementing patches, running updates, or pushing configurations. Although this may help with

speed and management, the rapid deployment of multiple instances can increase risk by spreading malicious configurations consistent with one type of system. Having network elements that possess the same attributes creates a monoculture that can be efficient for management but risky when compromised images, patches, or updates are introduced in the system, which can compromise all systems in the monoculture.<sup>33</sup>

Consequently, a heterogeneous network made up of multiple different operating systems will add to the resilience posture.<sup>34</sup> Heterogeneity in systems reduces the potential damage of adversary exploitations and also guards against common system failures.<sup>35</sup> Heterogeneity decreases the probability that adversary capability will be effective against different systems by increasing the complexity of adversary planning.<sup>36</sup> Adversaries must plan to infiltrate multiple platforms, which requires more knowledge, training, and capability for adversaries to meet their aims. Cyber weapons such as exploits are often a one-and-done capability because after their use and subsequent discovery, defenses can be put into place to block attributes of that capability. The expenditure of more cyber capability from adversaries adds time and cost to their attacks and may deter some actors from attempting to infiltrate networks planned with diversity. Colonel William Bryant offers that diversity of systems, for example, mixing Windows and Linux systems will allow the network to overcome an attack associated with certain operating systems by maintaining capability within the degraded environment.<sup>37</sup> In the case when 50% of the network is Windows and 50% is Linux, if all Linux systems were compromised by a malicious software patch, those systems could be isolated or taken off line while the Windows systems continued to operate.<sup>38</sup> This means that although some functionality may be lost, if the network is properly planned, the organization will be able to absorb blows while continuing operations.

Another way to make systems more resilient through engineering is virtualization.<sup>39</sup> The National Institute of Standards and Technology (NIST) defines virtualization as, “the use of the abstraction layer to simulate computing hardware so that multiple operating systems can run on one computer.”<sup>40</sup> First, virtualization lessens the IT footprint without decreasing computing power and functionality. The smaller target is often the one harder to hit. Second, virtualization allows for less power and cooling, thus further decreasing the signature of units employing them. This is especially important for speed and tempo, as virtualization lightens the load of units deploying and maneuvering. Now that the Joint Force is leveraging cloud computing, it is feasible to assume degradation or denied access to the cloud environment in a conventional fight. Plus, cloud services and collaboration tools may be better served if employed locally for smaller tactical formations. The use of virtual machines provides localized services that can replicate with remote services. This enables local operations to continue uninhibited when connectivity is lost to the main cloud environment because the applications and tools are still available. Another positive to virtualization is that it enables the rapid deployment and management of specific operating system configurations.<sup>41</sup> This provides the ability to automate reconfigurations across multiple virtual machines in the case of a physical or logical fault.<sup>42</sup> This could be the reconfiguration of the network as is, or reconfiguration to a different network not known to a suspected attacker. This allows planners to create advantages in cyberspace by redefining cyber terrain on favorable terms not immediately known to the attacker. Although virtualization can create a monoculture, it does allow for the rapid reconstitution of networks in the event of loss and should be considered in resiliency planning. The rapid projection of services in an area enables units to quickly assume processes reliant on technology. Planners will have to weigh the



risk of monocultures and virtualization when planning architectures and assessing rapid recovery as a viable course of action to increase resiliency.

In addition to virtualization and diversity of network elements, the acquisition and procurement of systems designed for resilience must also be considered when increasing a resilience posture. The key issues affecting the engineering and development of resilient systems and their employment in the future involve unknown and uncertain environments, mobile and limited support structures, extreme conditions, adversaries operating within and outside of the area of hostilities, and changing natural and manmade environments.<sup>43</sup> To address these issues, the Joint Force must acquire systems that respond to new or changing conditions, exhibit predictable and graceful degradation outside their design performance envelope, while being sustainable, reconfigurable, and replaceable in a timely manner consistent with mission needs.<sup>44</sup>

The most important factor in engineering systems for resilience is getting the requirements right. Requirement management demands a focus on requirement analysis, tracking, and verification.<sup>45</sup> Requirement analysis requires that the procurer understands the requirements of the Service and Joint Force.<sup>46</sup> This is especially challenging when planning for future uncertain environments and must be anticipated based on military judgement. Requirement tracking involves analyzing design tradeoffs, like cost and time, with performance goals.<sup>47</sup> This is an important factor when time is fleeting and systems require resiliency as a performance metric to meet current demands. Finally, requirement verification calls for determining whether system design will meet specified requirements.<sup>48</sup> Joseph Fiksel's study on designing resilient sustainable systems suggests that systems should be designed for the environment in which they will be employed.<sup>49</sup> This is aimed specifically at the availability of components for repair, maintenance, and replacement. If the system will be deployed in the US,

it should be engineered to use US parts and labor as a factor of speed and availability. Wherever the next war may be, systems need to be engineered with an eye towards living off the land like Napoleon's armies while campaigning. If not, stockpiling forward logistics bases that are survivable enough to rapidly service requirements will be necessary. Fiksel's study also calls for the simplification of product architecture to reduce the number of distinct parts and assembly operations.<sup>50</sup> Simplifying product architecture ties back into repair, maintenance, and replacement. If a reduction is made in monopolized or proprietary components only available in specific markets, then availability increases thereby increasing the recoverability of equipment to attacks or malfunctions. Malfunctions in vulnerable systems can however be reasonably predicted.

To address technical malfunctions, the Joint Force must acquire systems that exhibit predictable and graceful degradation as a requirement.<sup>51</sup> If degradation and malfunction can be predicted, then planning can address issues prior to failure. This is comparable to a technical refresh, where a system has hit its end of life based on a simulated or calculated prediction of obsolescence. To aid in this process, the use of high-performance computing assets, together with modeling and simulation, can help replicate complex interactions.<sup>52</sup> This allows for predictions in system functionality, based on different environments associated with where the Joint Force will operate and to whom it will face.<sup>53</sup> Ultimately, these factors will drive acquisition decisions geared towards the design and engineering of resilient systems.<sup>54</sup> Acquiring systems that include built in resilience, together with the ability to model system malfunction, enables communication planners to increase the resilience posture of networks by not only components but also through predictions that enable agility.

## **Resilience through Tailored Defense**

USCYBERCOM aims to gain the strategic advantage by increasing resiliency, defending forward, and continuously engaging adversaries.<sup>55</sup> Since defending forward requires preemption and counterattack methods that reach across gray and red space to create effects on adversaries, they can often be perceived as escalatory.<sup>56</sup> The following defense methods supporting resilience are internal to the network enclaves supporting the Joint Force and are not overtly escalatory. These non-escalatory actions add to deterrence by persuading adversaries that their efforts will not achieve their planned outcomes while imposing time and cost for actions taken against friendly networks. Therefore, the mention of defense in this case is not necessarily congruent with USCYBERCOM defending forward through offensive capability, but focuses on internal defensive efforts to bolster the planning for resilient systems.

Tailoring defense to the mission and threat will also promote a resilient posture by massing resources at the critical point or as Clausewitz explains, the *Schwerpunkt*; that if attacked can quickly throw the system out of balance.<sup>57</sup> Complex networks have many different critical points that can produce failure, and if assigned priority of protection during network planning, can most certainly yield increases in resilience. Economy of force requires the efficient employment of resources. Holding true to this principle of war, only when beneficial, requires the Joint Force to analyze mission essential functions and gain a true understanding of its footprint in cyberspace. As Sun Tzu states, “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”<sup>58</sup> Often, networks are employed without proper documentation and correct tracking of change management. This makes it especially difficult when planning for recovery during and after an attack. Therefore, the network architecture, together with logical elements, and cyber personas, must be known, documented, and understood

not only for trouble-shooting of issues, but also defending against threats. This starts with an understanding of mission essential tasks and functions of the unit. Once the mission essential functions of the organization are understood, an analysis of the systems that enable those functions is required. The network dependencies of those systems also need to be analyzed for gaps in defenses. Identifying those systems, gaps in defenses, and vulnerabilities enables the Joint Force to prioritize protection efforts and increase resiliency. For example, mission critical systems will have a higher priority than systems that serve largely administrative functions. This does not imply that administrative functions are not important, but it does recognize that the loss of administrative systems will not degrade mission essential functions. Understanding the cyber terrain supporting operations increases the ability to tailor defenses in support of critical elements. This is a paradigm shift from the traditional static defense architecture that relies on the lines of traditional defense in depth. The traditional defense in depth model only accounts for major avenues of approach without recognizing these avenues may shift with time or shift priority depending on the adversary. Shifting or tailoring defense in time and space requires actively maneuvering capabilities to increase resiliency.

Anticipation and sensing are key elements that enable tailored defenses to be employed on the most vulnerable terrain supporting critical systems. The identification of systems, gaps in defenses, and associated vulnerabilities allows for the proper placement of sensors that can collect on sensitive areas. This is much like the employment of collection assets on Named Areas of Interest (NAIs). The Joint Force can monitor these areas for adversary activity while hardening vulnerabilities associated with network dependencies supporting critical functions. Information sharing plays a critical role by facilitating the exchange of strategic, operational, and tactical threat information so networks can anticipate and adapt to the changing environment.

The ability to harness situational awareness and intelligence allows planners to estimate where, when, how, and why attacks may occur. With this information, the Joint Force can outpace adversaries, maintain the advantage, and as bamboo does, “bend to minimize the effect of future wind gusts,” but not break.<sup>59</sup> Bending but not breaking through a changing tailored defense will also increase the resiliency posture of the Joint Force.

### **Resilience through Deception**

Resilience through deception requires communication planners to understand deception as it pertains to the employment of networks. Deception is the provision of misinformation that is believable enough to confuse an adversary’s situational awareness while influencing and misdirecting perceptions and decision-making.<sup>60</sup> For example, the Marine amphibious demonstration, supporting the “Left Hook” during the 1991 Gulf War, lured the Iraqi Republican Guard to plan defenses towards the coastal area.<sup>61</sup> This demonstration was enhanced by inviting the media to cover amphibious landing rehearsals in Oman.<sup>62</sup> These actions were able to persuade the Iraqis to focus on amphibious operations instead of avenues of approach to the West, where the coalition was massing an attack. Deception in cyberspace can be used much in the same way it is in the land domain. To support resilience, deception can impart an incorrect belief in the attacker which goes beyond static defenses and has the potential to distract from real networks, expose tactics, give false confidence, and impose cost and time that in the end is fruitless.<sup>63</sup>

Deception efforts can be described in two types: ambiguity-increasing and ambiguity-decreasing. Ambiguity-increasing aims to impose time and cost in adversary decision making by providing several options.<sup>64</sup> This is also important for deterrence because with increasing options there lies increasing complexity. The more complexity that adversaries have to get

through, the less likely they are to spend the time to go after hard targets versus softly defended targets. This can turn the cyber deterrence equation from offensive persistent engagement to one of resilience. Complexity in friendly networks can also add to the deterrence strategy of denial, verses one of punishment that is offensive minded. The second type of deception is ambiguity-decreasing. Ambiguity-decreasing is defined as, plays on the biases and preconceived notions of the adversary.<sup>65</sup> Information is provided to reinforce adversary beliefs to make the decision desired by friendly forces.<sup>66</sup> This type of deception enables friendly forces to collect on adversaries or exploit their decisions to gain a friendly advantage. There are several deception efforts that are advantages to network planners that include honeypots, decoys, and moving target techniques.

Honeypots sit outside of traditional networks and deceive potential adversaries by broadcasting attributes that are similar, but more attractive than that of the protected network.<sup>67</sup> When adversaries penetrate a honeypot, they expose themselves to be collected on. This allows adversary attributes to be exploited or defended against in the real network. There are two types of honeypot technology, low-fidelity and high-fidelity honey pots. Low-fidelity honeypot technologies contain little to no information, but look real from outside the network when adversaries use low cost enumeration/reconnaissance techniques like scanning tools.<sup>68</sup> High-fidelity honeypot technology includes detailed false network information and activity known as ‘pocket litter’, to waste adversary time with analysis.<sup>69</sup> This requires network planners to include planning and implementation of cyber misinformation campaigns that have previously been conducted at much higher levels and not taught at communication or cyber planner courses.

Decoys also add to deception by misleading adversaries to systems that look real but in turn, only log adversary activity and report breaches.<sup>70</sup> Decoys obfuscate true network topology

and provide adversaries with the challenge of distinguishing the real from the fake.<sup>71</sup> Friendly forces can take advantage of adversary tactics on decoy systems to attribute and learn capability and intent. These actions provide a more resilient posture by deceiving adversaries from critical elements of the system, but are manpower intensive and require planning, training, and education currently not in place. Lastly, decoys can aid in network heterogeneity by diversifying what looks to be different operating systems. This adds to the cost and experience needed by the attacker thus making it more difficult to reconnoiter, place implants, and attack critical systems.

Security is also a tenet of Marine Corps' communications. Transmission security masks and protects most radio and satellite communication systems. One technique commonly used in tactical communications is frequency hopping. Frequency hopping uses a range of frequencies to broadcast communications randomly via encrypted means. It enables users to cycle through different frequencies so the enemy cannot fixate its jamming efforts on one frequency with any success. This concept is useful when explaining moving target techniques because it includes rapid cycling through frequencies that make it hard for the enemy to create effects. Rapid cycling is used to constantly reset the system to a known good state in order to get rid of adversaries who have gained access and imbedded exploits.<sup>72</sup> Cycling can be timed or random depending on the planner. The same is true for binary scrambling which provides code diversity by morphing code with identical performance that is seamless to the user viewing the website but different to an attacker examining the code.<sup>73</sup>

Other techniques include the constant changing of Internet Protocol (IP) or IP hopping and changes to network identifiers or host names to counter adversaries from learning the environment.<sup>74</sup> Moving target techniques assume that traditional defense in depth concepts and cybersecurity practices are effective only against lower level hackers, but not for the advanced

persistent threats that most nation states can access.<sup>75</sup> Polyverse CEO Alex Gounares explains that, “the core issue in cybersecurity today is the static and homogenous nature of the systems we are using.”<sup>76</sup> These networks are similar to medieval castles with moats or fortresses with built up bastions and ramparts. The problem with castles and fortresses is that they don’t pick up and move. Therefore, adversaries have time to learn capabilities and weakness and carefully plot attacks. This holds true for some of the Joint Force networks. Adversaries have time to learn these static networks because they seldom change.<sup>77</sup> Moving target techniques make networks dynamic, which lessens the time adversaries have to understand the environment.<sup>78</sup> The more confused adversaries are about Joint Force networks, the better the Joint Force can absorb their attempts. This ability to absorb adversary attempts will increase the resiliency posture of the Joint Force.

### **Resilience Through People and Processes**

Just as networks are a center of gravity for Joint Force employment, so are the people conducting and supporting Joint Force operations. Developing people and processes will also lead to a more resilient force that can overcome degraded communication environments in future war. Through the examination of training and process development, both communication planners and operators can identify the conditions that call for a shift in and out of scenarios that challenge both communications networks and the wills of operators seeking to accomplish a mission. Focusing on the person and the process, enables the Joint Force to recognize and address vulnerabilities that can shatter cohesion when friction is introduced and ultimately develop contingency plans to continue operations.

The first element of a command and control system are the people who acquire information, make decisions, act, and provide feedback into the system for further action.<sup>79</sup>



Increasing resilience in people, requires the development of their capacity to conduct these tasks in a contested environment. This requires training and education which necessitates institutions that support Joint Force operations in a degraded environment while also addressing future war concepts. Focusing on educating and training personnel will most certainly yield gains in resiliency. While education provides the ability to prepare for the unknown, training allows preparation for the known. This phrase is often spouted at many Professional Military Education (PME) courses and continues to hold true. The Joint Force is not necessarily dealing with the unknown, but rather what is in the realm of the possible considering the technology available. Currently, Joint Force education offered in Joint Professional Military Education (JPME) Phase I provides an increasing focus on what future war may look like against a near peer competitor. However, most Joint Force training courses have not yet begun to implement tactics and techniques needed in future war. This is mostly because concepts involving the anticipation of the future are nascent and need further development to realize the tactics, techniques, and procedures necessarily for execution. For example, the Joint Force Staff College oversees the Joint Command, Control, Communications, and Computers Planners Course (JC4PC) at the Army Cyber Center of Excellence in Fort Gordon, GA. This course focuses on the planning of communications supporting the Joint Force. While the course includes planning for the employment of radio, satellite, telephone, and computer systems, and gives basic information about cyberspace, it does not address planning techniques, other than cybersecurity and redundancy planning, to ensure resiliency in a degraded environment. This gap can be mitigated through the inclusion of new techniques in the curriculum. At the very least, the inclusion of these techniques will provide more tools in the communication planner toolset to assist in the planning, installation, operation, and maintenance of networks in future scenarios.

It is important to remember that people are the decisive factor in cyber resilience, just as they are in conventional armed conflicts. Training communication planners is essential to resilience because it allows for the detailed planning and protection of networks supporting the warfighter. However, training the staff to operate in a degraded environment is also equally important. This requires staff processes to include worst case scenarios as it pertains to communications availability. This may require the rapid shift from reliance on big bandwidth data networks to radio communications or even messenger. This will require staffs to become efficient in the basics of radio communications to accomplish staff functions. This includes passing graphics and location information over limited data circuits traversing radio networks. The staff must possess the ability to quickly transition to high availability of networks to low availability or even create new ways of passing information that fit the current situation. Issuing mission type orders and allowing decision making to be pushed down to the point of friction allows the Joint Force to continue operations when communications with higher and adjacent units may not be possible. This requires trust and the ability of subordinate commanders to operate inside of commander's intent. If units and staff processes can flex with the communication mediums available, then the organization increases its resilience posture.

## **Conclusion**

In conclusion, the future operating environment requires more priority on the resilience of systems, networks, and people for the Joint Force to be successful in future war. This position is contrary to USCYBERCOM's approach that invests mostly in offensive cyber weapons to create effects and defend forward of friendly networks. Focusing on resilience acknowledges that near-peer adversaries possess emerging technologies capable of causing significant degradations that will challenge Joint Force C2 and requires communications planners to possess the capability to

plan and implement networks much different from traditional communications employment. Resilience adds to current deterrence effort by imposing time and cost on the adversary without being overtly escalatory. Tailoring defenses, implementing deception techniques, solidifying processes, and investing in training allows the Joint Force to adapt and anticipate the trials to come while also preparing communication planners at all levels to assure the network or provide off ramps that facilitate C2 in future war.

## End Notes

---

<sup>1</sup> Richard J. Harknett, “United States Cyber Command’s New Vision: What It Entails and Why It Matter,” *Law Warfare, Cybersecurity and Deterrence*, March 2018, 2, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>

<sup>2</sup> Mark Pomerleau, “What the budget request explains about Cyber Command’s goals,” *Fifth Domain*, February 2018, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>

<sup>3</sup> Michael P. Fischerkeller, Richard J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation,” Army Cyber Institute, West Point, November 2018, 1, [https://www.ida.org/idamedia/Corporate/Files/Publications/IDA\\_Documents/ITSD/2018/D-9076.pdf](https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/ITSD/2018/D-9076.pdf)

<sup>4</sup> Ibid.

<sup>5</sup> Joseph S. Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security, Vol 41, No 3*, Winter, 2017, 45, [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266); Angus King, “In Armed Services Hearing, King Questions Top Cyber Command Official on National Doctrine of Deterrence in Cyberspace,” February 27, 2018, 2:20.

<https://www.king.senate.gov/newsroom/press-releases/in-armed-services-hearing-king-questions-top-cyber-command-official-on-national-doctrine-of-deterrence-in-cyberspace>

<sup>6</sup> Jason Healey, “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities.” Brookings Institution Press, June 2015, 173.

<sup>7</sup> Ibid.

<sup>8</sup> Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (University of Georgia Press, 2011), 310.

<sup>9</sup> Cindy Compart, “From Cyber Defense to Cyber Resilience: Charting a new course,” Cyber Security Symposium event, San Jose, CA September 2018, 2:09, <https://www.youtube.com/watch?v=NrFK27Z5yU0&t=889s>

<sup>10</sup> Ibid.

<sup>11</sup> Richard J. Harknett, “United States Cyber Command’s New Vision: What It Entails and Why It Matter,” *Law Warfare, Cybersecurity and Deterrence*, March 2018, 2, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>

<sup>12</sup> US Army Research Laboratory, *Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153* (NATO, April 2018), 11, <https://www.arl.army.mil/arlreports/2018/ARL-SR-0396.pdf>

<sup>13</sup> Frank Konkel, “And you thought your inbox was dangerous.” *Nextgov*, January 11, 2018, <https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/>

<sup>14</sup> Frank G. Hoffman, “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War,” (The Heritage Foundation, 2016), 30, [https://s3.amazonaws.com/ims-2016/PDF/2016\\_Index\\_of\\_US\\_Military\\_Strength\\_ESSAYS\\_HOFFMAN.pdf](https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_HOFFMAN.pdf)

---

<sup>15</sup> Richard J. Harknett, “United States Cyber Command’s New Vision: What It Entails and Why It Matter,” *Law Warfare, Cybersecurity and Deterrence*, March 2018, 2, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>

<sup>16</sup> Ibid.

<sup>17</sup> Robert J. Samuelson, “The Power of Moore’ Law,” *The Washington Post*, April 2015, [https://www.washingtonpost.com/opinions/the-power-of-moores-law/2015/04/19/f1806c98-e6b6-11e4-9a6a-c1ab95a0600b\\_story.html?utm\\_term=.f07a4bd6d055](https://www.washingtonpost.com/opinions/the-power-of-moores-law/2015/04/19/f1806c98-e6b6-11e4-9a6a-c1ab95a0600b_story.html?utm_term=.f07a4bd6d055)

<sup>18</sup> Ray A. Rothrock, “Digital Network Resilience: Surprising Lessons from the Maginot Line,” *The Cyber Defense Review*, Vol. 2, No. 3, FALL 2017, 35, [https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience\\_Rothrock.pdf?ver=2018-07-31-093725-860](https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience_Rothrock.pdf?ver=2018-07-31-093725-860)

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

<sup>21</sup> Sylvester Stallone, “Rocky Balboa the Movie,” Metro-Goldwyn-Mayer, Columbia Pictures, Revolution Studios, Chartoff/Winkler Productions, 2006.

<sup>22</sup> Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations*, The Pentagon, Arlington, VA, June 8, 2018, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf?ver=2018-07-16-134954-150](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150)

<sup>23</sup> Ron Ross, *Building Cyber Resilient Systems: A National and Economic Security Imperative* (National Institute of Standards and Technology), Power Point Presentation, <https://csrc.nist.gov/CSRC/media/Presentations/building-cyber-resilient-systems/images-media/Building-Cyber-Resiliency-MITRE-20180508.pdf>

<sup>24</sup> US Army Research Laboratory, *Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153* (NATO, April 2018), 1, <https://www.arl.army.mil/arlreports/2018/ARL-SR-0396.pdf>

<sup>25</sup> Ibid, 2.

<sup>26</sup> Elliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War*. (New York: The Free Press, 1990).

<sup>27</sup> Jesse Sloman, “The future of war (25): You better be ready to fight like it’s a pre-electronic age,” *Foreign Policy, Best Defense*, April, 2014, <https://foreignpolicy.com/2014/04/18/the-future-of-war-25-you-better-be-ready-to-fight-like-its-a-pre-electronic-age/>

<sup>28</sup> William D. Bryant, “Resiliency in Future Cyber Combat,” *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, 90, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>

<sup>29</sup> Ibid.

<sup>30</sup> Clinger Cohen Act of 1996, 40 U.S.C. (1996), <https://business.defense.gov/Portals/57/Documents/Federal%20Acquisition%20Reform%20Act%20of%201996%20Clinger-Cohen%20Act.pdf>

<sup>31</sup> William D. Bryant, “Resiliency in Future Cyber Combat,” *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, 91, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>

<sup>32</sup> Ibid, 90.

<sup>33</sup> Panayotis A. Yannakogeorgos and John P. Geis II, “The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce,” (Maxwell Air Force Base, Alabama: Air University Press 2016), 34,

---

[https://media.defense.gov/2017/Apr/07/2001728472/-1/-](https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B_0143_YANNAKOGORGOS_GEIS_HUMAN_CYBER_CONFLICT.PDF)

[1/0/B\\_0143\\_YANNAKOGORGOS\\_GEIS\\_HUMAN\\_CYBER\\_CONFLICT.PDF](https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B_0143_YANNAKOGORGOS_GEIS_HUMAN_CYBER_CONFLICT.PDF)

<sup>34</sup> William D. Bryant, “Resiliency in Future Cyber Combat,” *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, 90, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>

<sup>35</sup> National Institute of Standards and Technology, *Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, U.S. Department of Commerce, April 2013, F-204,

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>

<sup>36</sup> Ibid, F-204.

<sup>37</sup> William D. Bryant, “Resiliency in Future Cyber Combat,” *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, 90, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>

<sup>38</sup> Ibid, 92.

<sup>39</sup> Panayotis A. Yannakogeorgos and John P. Geis II, “The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce,” (Maxwell Air Force Base, Alabama: Air University Press 2016), 34,

[https://media.defense.gov/2017/Apr/07/2001728472/-1/-](https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B_0143_YANNAKOGORGOS_GEIS_HUMAN_CYBER_CONFLICT.PDF)

[1/0/B\\_0143\\_YANNAKOGORGOS\\_GEIS\\_HUMAN\\_CYBER\\_CONFLICT.PDF](https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B_0143_YANNAKOGORGOS_GEIS_HUMAN_CYBER_CONFLICT.PDF)

<sup>40</sup> National Institute of Standards and Technology, *Special Publication 800-44 Version 2: Guidelines on Securing Public Web Servers*, U.S. Department of Commerce, September 2007, B-2, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf>

<sup>41</sup> Ibid.

<sup>42</sup> Ibid.

<sup>43</sup> Sim R. Goerger, Azad M. Madni, and Owen J. Eslinger, *Engineered Resilient Systems: A DoD Perspective* (The Authors, 2014), 649,

<https://www.sciencedirect.com/science/article/pii/S1877050914001665>

<sup>44</sup> Ibid, 781.

<sup>45</sup> Joseph Fiksel, “Designing Resilient, Sustainable Systems,” *Environmental Science & Technology*, Vol. 37, No 23, American Chemical Society, (2003): 5335,

<https://www.sciencedirect.com/science/article/pii/S1877050914001665>

<sup>46</sup> Ibid.

<sup>47</sup> Ibid.

<sup>48</sup> Ibid.

<sup>49</sup> Ibid, 5334.

<sup>50</sup> Ibid.

<sup>51</sup> Ibid.

<sup>52</sup> Ibid.

<sup>53</sup> Ibid.

<sup>54</sup> Ibid.

<sup>55</sup> United States Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” (April 2018), 4,

<https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>

<sup>56</sup> JP 3-12 Defines the following terms as: “The term ‘blue cyberspace’ denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. The term ‘red cyberspace’ refers to those portions of cyberspace owned or controlled by an adversary or enemy. All cyberspace that does not meet the description of either ‘blue’ or

‘red’ is referred to as ‘gray’ cyberspace.” Joint Chiefs of Staff, *Joint Publication 3-12 Cyberspace Operations*, The Pentagon, Arlington, VA, June 8, 2018, I-5, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf?ver=2018-07-16-134954-150](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150)

<sup>57</sup> It is important to note that Antulio J. Echevarria’s use of Schwerpunkt was from the original version of *On War, Vom Kriege*. He then examined the concept of center of gravity through elementary physics which deals with balance and equilibrium. Carl Von Clausewitz, *Vom Kriege*, 19<sup>th</sup> ed., (Regensburg: Pustet, 1991), p.810, Carl Von Clausewitz, *On War*, edited by Michael Howard and Peter Paret. Princeton, N.J. Princeton University Press (1976), Antulio J. Echevarria II, “Clausewitz’s Center of Gravity Its Not What We Thought,” *Naval War College Review*, Winter 2003, Vol.LVI, No. 1 <http://www.au.af.mil/au/awc/awcgate/navy/art4-w03.htm> , Milan Vego, “Clausewitz’s SCHWERPUNKT: Mistranslated from German-Misunderstood in English,” [https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview\\_20070228\\_art014.pdf](https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20070228_art014.pdf)

<sup>58</sup> Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (Oxford University Press 1963).

<sup>59</sup> William D. Bryant, “Resiliency in Future Cyber Combat,” *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, 89, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>

<sup>60</sup> KJ Ferguson-Walter, DS LaFon and TB Shade, “Friend or Faux: Deception for Cyber Defense,” *Journal of Information Warfare*, Vol. 16, No.2 (Peregrine Technical Solutions, Spring 2017), 29.

<sup>61</sup> Wyatt Olson, “‘Left hook’ deception hastened Gulf War’s end,” *Stars and Stripes*, January, 2016, <https://www.stripes.com/news/special-reports/the-gulf-war-25-year-anniversary/deception>

<sup>62</sup> Ibid.

<sup>63</sup> KJ Ferguson-Walter, DS LaFon and TB Shade, “Friend or Faux: Deception for Cyber Defense,” *Journal of Information Warfare*, Vol. 16, No.2 (Peregrine Technical Solutions, Spring 2017), 29.

<sup>64</sup> This document states the definition of Ambiguity-increasing: “Ambiguity-increasing deception provides the enemy with multiple plausible friendly COAs. Ambiguity-increasing deception is designed to generate confusion and cause mental conflict in the enemy decision maker.” Department of the Army, *Field Manual 3-13.4 Army Support to Military Deception* (Feb 2019), 1-7. <https://fas.org/irp/doddir/army/fm3-13-4.pdf>

<sup>65</sup> This document states the definition of Ambiguity-decreasing: “Ambiguity-decreasing deceptions manipulate and exploit an enemy decision maker’s pre-existing beliefs and bias through the intentional display of observables that reinforce and convince that decision maker that such pre-held beliefs are true.”

Ibid, 1-8.

<sup>66</sup> Ibid.

<sup>67</sup> John Leyden, “To Russia with Love? Georgia snaps ‘cyber-spy’ with his own cam: Govt puts pics on internet – not much else they can do,” *The Register: Security*, Oct 2012, [https://www.theregister.co.uk/2012/10/31/georgia\\_russia\\_counter\\_intelligence/](https://www.theregister.co.uk/2012/10/31/georgia_russia_counter_intelligence/) ; Ted Cruz, “In Cuba, Obama Will Legitimize the Corrupt and Ignore the Oppressed.” *Politico Magazine*, March 2016, <https://www.politico.com/magazine/story/2016/03/russia-cyber-war-fred-kaplan-book-213746>

<sup>68</sup> KJ Ferguson-Walter, DS LaFon and TB Shade, “Friend or Faux: Deception for Cyber Defense,” *Journal of Information Warfare*, Vol. 16, No.2 (Peregrine Technical Solutions, Spring 2017), 30.

---

<sup>69</sup> Ibid.

<sup>70</sup> Ibid.

<sup>71</sup> Ibid.

<sup>72</sup> Kiley Williams, *Moving Target Defense Webinar*, Cover6 Solutions, October 2017, <https://www.youtube.com/watch?v=D9V0qiPQ8Lo>

<sup>73</sup> Ibid.

<sup>74</sup> Andrew Mellinger, *SEI Podcast Series: Conversations in Software Engineering*, December 9, 2016, [https://www.youtube.com/watch?v=Dq\\_eZITL0Is](https://www.youtube.com/watch?v=Dq_eZITL0Is)

<sup>75</sup> Kiley Williams, *Moving Target Defense Webinar*, Cover6 Solutions, October 2017, <https://www.youtube.com/watch?v=D9V0qiPQ8Lo>

<sup>76</sup> Ibid.

<sup>77</sup> Andrew Mellinger, *SEI Podcast Series: Conversations in Software Engineering*, December 9, 2016, [https://www.youtube.com/watch?v=Dq\\_eZITL0Is](https://www.youtube.com/watch?v=Dq_eZITL0Is)

<sup>78</sup> Ibid.

<sup>79</sup> Joint Chiefs of Staff, *Joint Publication 6-0 Joint Communications System*, The Pentagon, Arlington, VA, June 10, 2015, vii, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6\\_0.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf)



## Bibliography

- Bryant, William D. "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly*, Vol. 9, No. 4, Winter 2015, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1003656.pdf>
- Burger, Brian. "BFT, C2PC, VTC, and SharePoint are Down!," *Marine Corps Gazette*, Vol 101, Issue 8, August, 2017, <https://search-proquest-com.lomc.idm.oclc.org/docview/2025652679?accountid=14746>
- Canter, Christopher R. "The Enemy's most Dangerous Course of Action." *Marine Corps Gazette*, Vol 102, Issue 4, April, 2018, <https://search-proquest-com.lomc.idm.oclc.org/docview/2026328239?accountid=14746>
- Clausewitz, Carl Von., Michael Howard, and Peter Paret. *On War*, (N.J. Princeton University Press, 1976)
- Clausewitz, Carl Von, *Vom Kriege*, 19<sup>th</sup> ed., (Regensburg: Pustet, 1991)
- Clinger Cohen Act of 1996, 40 U.S.C. (1996), <https://business.defense.gov/Portals/57/Documents/Federal%20Acquisition%20Reform%20Act%20of%201996%20Clinger-Cohen%20Act.pdf>
- Cohen, Elliot A., John Gooch, *Military Misfortunes: The Anatomy of Failure in War*. (New York: The Free Press, 1990).
- Conklin, William Arthur, Dan Shoemaker, and Anne Kohnke. "Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture," *Academic Conferences International Limited*, 2017, <https://search-proquest-com.lomc.idm.oclc.org/docview/1897660614?accountid=14746>
- Compart, Cindy. "From Cyber Defense to Cyber Resilience: Charting a new course," Cyber Security Symposium event, San Jose, CA September 2018, <https://www.youtube.com/watch?v=NrFK27Z5yU0&t=889s>
- Cruz, Ted. "In Cuba, Obama Will Legitimize the Corrupt and Ignore the Oppressed." *Politico Magazine*, March 2016, <https://www.politico.com/magazine/story/2016/03/russia-cyber-war-fred-kaplan-book-213746>
- Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, (Athens: University of Georgia Press, 2011).
- Department of the Army, *Field Manual 3-13.4 Army Support to Military Deception* (Feb 2019), 1-7. <https://fas.org/irp/doddir/army/fm3-13-4.pdf>
- Echevarria II, Antulio J. "Clausewitz's Center of Gravity Its Not What We Thought." *Naval War*

- College Review*, Winter 2003, Vol.LVI, No. 1  
<http://www.au.af.mil/au/awc/awcgate/navy/art4-w03.htm>
- Esper, Michael, H. “Defensive Culmination: A useful piece of theory?,” *School of Advanced Military Studies*. April, 1997, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a240405.pdf>
- Fiksel, Joseph. “Designing Resilient, Sustainable Systems,” *Environmental Science & Technology*, Vol. 37, No 23, American Chemical Society, (2003),  
<https://www.sciencedirect.com/science/article/pii/S1877050914001665>
- Fischerkeller, Michael P. and Richard J. Harknett. “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation,” Army Cyber Institute, West Point, November 2018,  
[https://www.ida.org/idamedia/Corporate/Files/Publications/IDA\\_Documents/ITSD/2018/D-9076.pdf](https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/ITSD/2018/D-9076.pdf)
- Ferguson-Walter, KJ, DS LaFon and TB Shade, “Friend or Faux: Deception for Cyber Defense,” *Journal of Information Warfare*, Vol. 16, No.2 (Peregrine Technical Solutions, Spring 2017),
- Goerger, Sim R., Azad M. Madni, and Owen J. Eslinger, *Engineered Resilient Systems: A DoD Perspective* (The Authors, 2014),  
<https://www.sciencedirect.com/science/article/pii/S1877050914001665>
- Harknett, Richard J. “United States Cyber Command’s New Vision: What It Entails and Why It Matter,” *Law Warfare, Cybersecurity and Deterrence*, March 2018,  
<https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>
- Healey, Jason. “The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities.” Brookings Institution Press, June 2015.
- Hoffman, Frank G. “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War,” (The Heritage Foundation, 2016), 30,  
[https://s3.amazonaws.com/ims-2016/PDF/2016\\_Index\\_of\\_US\\_Military\\_Strength\\_ESSAYS\\_HOFFMAN.pdf](https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_HOFFMAN.pdf)
- King, Angus. “In Armed Services Hearing, King Questions Top Cyber Command Official on National Doctrine of Deterrence in Cyberspace,” February 27, 2018,  
<https://www.king.senate.gov/newsroom/press-releases/in-armed-services-hearing-king-questions-top-cyber-command-official-on-national-doctrine-of-deterrence-in-cyberspace>
- Konkel, Frank. “And you thought your inbox was dangerous.” *Nextgov*, January 11, 2018,  
<https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/>

- Johnston, Robert S. "Next-Gen Warfare." *Marine Corps Gazette Vol 97, Issue 5*, May, 2013, <https://search-proquest-com.lomc.idm.oclc.org/docview/1372737801?accountid=14746>
- Joint Chiefs of Staff. *Joint Publication 3-12 Cyberspace Operations*, The Pentagon, Arlington, VA, June 8, 2018, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf?ver=2018-07-16-134954-150](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150)
- Joint Chiefs of Staff, *Joint Publication 6-0 Joint Communications System*, The Pentagon, Arlington, VA, June 10, 2015, vii, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6\\_0.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf)
- Leyden, John. "To Russia with Love? Georgia snaps 'cyber-spy' with his own cam: Govt puts pics on internet – not much else they can do," *The Register: Security*, Oct 2012, [https://www.theregister.co.uk/2012/10/31/georgia\\_russia\\_counter\\_intelligence/](https://www.theregister.co.uk/2012/10/31/georgia_russia_counter_intelligence/)
- Mellinger, Andrew *SEI Podcast Series: Conversations in Software Engineering*, December 9, 2016, [https://www.youtube.com/watch?v=Dq\\_eZITL0Is](https://www.youtube.com/watch?v=Dq_eZITL0Is)
- NewsRx. "Resilient Systems; New Ponemon Institute Study Reveals that Improving Cyber Resilience is Critical for Prevailing Against Rising Cyber Threats," *Journal of Engineering*, October 05, <https://search-proquest-com.lomc.idm.oclc.org/docview/1718140489?accountid=14746>
- National Institute of Standards and Technology, *Special Publication 800-44 Version 2: Guidelines on Securing Public Web Servers*, U.S. Department of Commerce, September 2007, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf>
- National Institute of Standards and Technology, *Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal information Systems and Organizations*, U.S. Department of Commerce, April 2013, <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>
- Nye, Joseph, S. Jr. "Deterrence and Dissuasion in Cyberspace," *International Security, Vol 41, No 3*, Winter, 2017, [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266)
- Olson, Wyatt. "'Left hook' deception hastened Gulf War's end," *Stars and Stripes*, January, 2016, <https://www.stripes.com/news/special-reports/the-gulf-war-25-year-anniversary/deception>
- Ormrod, David and Benjamin Turnbull. "Cyber Resilience as an Information Operations Action to Assure the Mission," *Academic Conferences International Limited, 06*, June, 2018, <https://search-proquest-com.lomc.idm.oclc.org/docview/2077000320?accountid=14746>
- Pomerleau, Mark. "What the budget request explains about Cyber Command's goals," *Fifth*

*Domain*, February 2018, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>

Ross, Ron. *Building Cyber Resilient Systems: A National and Economic Security Imperative* (National Institute of Standards and Technology), Power Point Presentation, <https://csrc.nist.gov/CSRC/media/Presentations/building-cyber-resilient-systems/images-media/Building-Cyber-Resiliency-MITRE-20180508.pdf>

Rothrock, Ray A. "Digital Network Resilience: Surprising Lessons from the Maginot Line," *The Cyber Defense Review*, Vol. 2, No. 3, FALL 2017, 35, [https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience\\_Rothrock.pdf?ver=2018-07-31-093725-860](https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Digital%20Network%20Resilience_Rothrock.pdf?ver=2018-07-31-093725-860)

Samuelson, Robert J. "The Power of Moore' Law," *The Washington Post*, April 2015, [https://www.washingtonpost.com/opinions/the-power-of-moores-law/2015/04/19/f1806c98-e6b6-11e4-9a6a-c1ab95a0600b\\_story.html?utm\\_term=.f07a4bd6d055](https://www.washingtonpost.com/opinions/the-power-of-moores-law/2015/04/19/f1806c98-e6b6-11e4-9a6a-c1ab95a0600b_story.html?utm_term=.f07a4bd6d055)

Shockey, Jason R. "Combat Readiness through Cyber Resilience," *Marine Corps Gazette Vol 99, Issue 9*, September, 2015, <https://search-proquest-com.lomc.idm.oclc.org/docview/1713499390?accountid=14746>

Sloman, Jesse. "The future of war (25): You better be ready to fight like it's a pre-electronic age," *Foreign Policy, Best Defense*, April, 2014, <https://foreignpolicy.com/2014/04/18/the-future-of-war-25-you-better-be-ready-to-fight-like-its-a-pre-electronic-age/>

Stallone, Sylvester. "Rocky Balboa the Movie," Metro-Goldwyn-Mayer, Columbia Pictures, Revolution Studios, Chartoff/Winkler Productions, 2006.

Stokes, Paul L. "Closing the MAGTF C2/Cyber Gap," *Marine Corps Gazette, Vol 102, Issue 4*, April, 2018, <https://search-proquest-com.lomc.idm.oclc.org/docview/2026327921?accountid=14746>

Stokes, Paul L. "The Will to Communicate," *Marine Corps Gazette Vol 100, Issue 9*, September, 2016, <https://search-proquest-com.lomc.idm.oclc.org/docview/1815404132?accountid=14746>

Tzu, Sun. *The Art of War*, trans. Samuel B. Griffith (Oxford University Press 1963).

United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (April 2018), <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>

US Army Research Laboratory, *Approaches to Enhancing Cyber Resilience: Report of the North*

*Atlantic Treaty Organization (NATO) Workshop IST-153* (NATO, April 2018),  
<https://www.arl.army.mil/arlreports/2018/ARL-SR-0396.pdf>

Williams, Kiley. *Moving Target Defense Webinar*, Cover6 Solutions, October 2017,  
<https://www.youtube.com/watch?v=D9V0qiPQ8Lo>

Yannakogeorgos, Panayotis A. and John P. Geis II, “The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce,” (Maxwell Air Force Base, Alabama: Air University Press 2016),  
[https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B\\_0143\\_YANNAKOGEOGOS\\_GEIS\\_HUMAN\\_CYBER\\_CONFLICT.PDF](https://media.defense.gov/2017/Apr/07/2001728472/-1/-1/0/B_0143_YANNAKOGEOGOS_GEIS_HUMAN_CYBER_CONFLICT.PDF)

Vego, Milan. “Clausewitz’s SCHWERPUNKT: Mistranslated from German – Misunderstood in English.” *Military Review* (January-February 2007)  
[https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview\\_20070228\\_art014.pdf](https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20070228_art014.pdf)