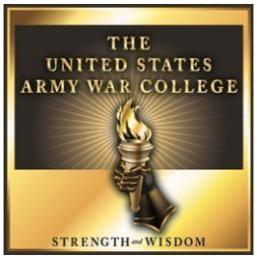
Strategy Research Project

Cyberspace Employment Challenges Comparison to the Machine Gun

by

Lieutenant Colonel Damon K. Burrows
United States Marine Corps

Under the Direction of:
Professor Howard Taylor



United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Cyberspace Employment Challenges Comparison to the Machine Gun

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Damon K. Burrows
United States Marine Corps

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Howard Taylor

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 5768

14. ABSTRACT
The machine gun (MG) changed the character of warfare. Nevertheless, its acceptance and role in combat were not always obvious. Barriers such as social acceptance, obedience to strategies of past wars, and challenges with conceptualizing the future environment hindered the United States' (U.S.) organizational and doctrinal changes for nearly fifty years after its initial employment in the American Civil War. The Battle of the Somme awakened the U.S. to the full strategic significance of this weapon and catalyze military reform. To foster a more deliberate and forward-thinking approach for conceptualizing warfighting in cyberspace, this research analyzes the lessons and similarities from the MG that are consequential to understanding, employing, and ultimately developing cyber warfare strategies, theories, and doctrine. The vantage of history offers an in-depth analysis on the missed opportunities and vulnerabilities from the MG's technology disruption without subjecting cyber warfare to the same bromidic and dangerous approach of waiting for a crisis to discover tectonic shifts in the character of warfare. This research reveals that drawing upon past MG gun lessons serves as a vignette for asking the right questions, avoiding the same pitfalls, and for effectively conceptualizing and developing a cyber warfare strategy.

15. SUBJECT TERMS
Strategy, Policy, Vision, Doctrine, Theorist

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	34	

Cyberspace Employment Challenges Comparison to the Machine Gun

(5768 words)

Abstract

The machine gun (MG) changed the character of warfare. Nevertheless, its acceptance and role in combat were not always obvious. Barriers such as social acceptance, obedience to strategies of past wars, and challenges with conceptualizing the future environment hindered the United States' (U.S.) organizational and doctrinal changes for nearly fifty years after its initial employment in the American Civil War. The Battle of the Somme awakened the U.S. to the full strategic significance of this weapon and catalyze military reform. To foster a more deliberate and forward-thinking approach for conceptualizing warfighting in cyberspace, this research analyzes the lessons and similarities from the MG that are consequential to understanding, employing, and ultimately developing cyber warfare strategies, theories, and doctrine. The vantage of history offers an in-depth analysis on the missed opportunities and vulnerabilities from the MG's technology disruption without subjecting cyber warfare to the same bromidic and dangerous approach of waiting for a crisis to discover tectonic shifts in the character of warfare. This research reveals that drawing upon past MG gun lessons serves as a vignette for asking the right questions, avoiding the same pitfalls, and for effectively conceptualizing and developing a cyber warfare strategy.

Cyberspace Employment Challenges Comparison to the Machine Gun

> The need to fight quickly led man to invent appropriate devices to gain advantages in combat, and these brought about great changes in the forms of fighting.
>
> —Carl von Clausewitz [1]

The machine gun (MG) "drastically altered" the character of warfare.[2] Nevertheless, its acceptance and role in combat were not always obvious. From its initial employment in the American Civil War to World War I (WWI), it took nearly fifty years of trial, error, and carnage for the United States (U.S.) and its allies to awaken to the full strategic significance of this weapon. Although a highly anticipated technology before its inception, barriers with social acceptance, obedience to strategies of past wars, and challenges with conceptualizing the future environment inhibited employing the MG to its full potential. Though numerous clues and opportunities existed to envision the MG's strategic significance, the U.S. Army still found itself "caught with its methods and thinking in transition between the nineteenth and twentieth centuries" and "unprepared for machine warfare in 1917."[3] Instead of a proactive approach propelled by leadership, strategic vision, and organizational reform, it was unthinkable violence that catalyzed the U.S.'s organizational and doctrinal changes for the MG.[4] This was not the first instance where overcoming bureaucratic inertia demanded a crisis to bring about needed military reform, nor would it be the last.[5]

To foster a more deliberate and forward-thinking approach for conceptualizing warfighting in cyberspace, this research analyzes the lessons and similarities from the MG that are consequential to understanding, employing, and ultimately developing cyber warfare strategies, theories, and doctrine. The vantage of history allows an in-depth analysis on the missed opportunities to respond adequately to the MG's

disruptive potential. This presents cyber warfare strategists with compelling parallels to avoid the perilously bromidic approach of reacting to changes in the character of warfare as a consequence of crisis. This research reveals that drawing upon past MG lessons serves as a vignette for asking the right questions, avoiding the same pitfalls, and for effectively conceptualizing and developing a cyber warfare strategy that will "conform to the spirit" of the future strategic environment.[6] Commonalities between the MG and cyber warfare include a lack of relevant theory for understanding and analyzing their strategic and disruptive significance; distractions from performance attributes and tools; and conceptual, social, and cultural barriers that each foster defensive-centric biases and obedience to strategies of past wars. This research also resolves that delays in recognizing cyberspace's warfighting advantages is perpetuating several cyber-specific challenges. First, distractions from various cyber taxonomies such as cyber norms, laws concerning cyber-crimes, data protection, and response actions are confounding cyber warfare strategy development efforts. Additionally, there is cognitive dissonance between current strategy and Joint operating concepts as to whether cyberspace is exclusively a domain, a combined-arm, or both. Finally, the Department of Defense's (DOD) role in protecting the homeland from cyberattacks of significant consequence is expanding the military's domestic sphere of influence, while conversely the wartime authorities required by Combatant Commanders (CCDRs) for conducting cyberspace operations remain closely controlled by civilian authorities. This ensuing civil-military relationship imbalance sets the foundation for friction in distinguishing between political and military matters during wartime.[7]

Defining the Scope

For this research, MG observations begin in the mid-1860s following the discovery of the Bessemer process and mechanical reloading.[8] For cyberspace, observations are focused on military considerations for offensive and defensive cyber warfare. By spotlighting cyber warfare, this permits exploration of unique strategic considerations that are separate and distinct from the more prevalent efforts to develop "appropriate and proportional response[s]" for other cyber taxonomies such as cyber-crimes, cyber-espionage, and cyber-terrorism.[9] While many cyber taxonomies are important to DOD, combined they introduce a litany of snares and distractions when attempting to concentrate on the strategy considerations necessary for Geographic Combatant Commands (GCCs) to leverage cyberspace during future wars.[10]

The Origins

Prior to its inception, the MG was envisioned as a means to rapidly "spew out vast numbers of bullets" in hopes of producing "significantly superior firepower."[11] Ingenious attempts, propelled by vision and purpose, eventually led to the long-awaited manifestation of a reliable automatic weapon and mechanized killing.[12] Despite having its wartime intention understood, fifty years passed before MG strategic employment concepts and force structure reform began to complement its offensive and defensive potential for mass-effects.[13] In contrast, cyberspace's wartime purpose emerged gradually over time, taking nearly fifty-years to become recognized as a warfighting domain.[14]

Unlike the MG which began as a vision for gaining "advantages in combat," a large portion of the cyberspace domain traces back to the Internet which began as a tool for sharing information.[15] In the mid-1960s, the Advance Research Projects Agency

(ARPA) conducted a packet-switching experiment to share information and resources between computer-science research departments.[16] By October 1969, the first computer message was sent over ARPA Network (ARPANET) bringing about the age in which any computer could “communicate freely” with any other computer.[17] Twenty years after the project’s launch, ARPANET split to form a military-specific network called MILNET to establish protected nodes for securing communications amongst installations, but continued to function principally for communications and information sharing. [18] The prevalence of DOD networks grew rapidly from 1983 to present, accompanied by steep advancements in tools and applications aimed at automating the Joint Warfighting Functions and enhancing Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance C4ISR systems.[19]

Cyberspace Domain

Unlike the easily studied and mastered mechanical properties and fundamentals of a MG, cyberspace’s complexity accelerated as an adaptive system with no foreseeable state of equilibrium. Immeasurable considerations emerged over a “variety of disciplinary perspectives” that complicated critical and creative thinking necessary to envision the future environment and develop a corresponding strategy aligned with military end states.[20] Although limited operations focused on cyberspace existed throughout the 1990s, it took another quarter century after splitting off MILNET to consolidate these disparate efforts and attempt to address cyberspace’s growing complexity by establishing U.S. Cyberspace Command (USCYBERCOM). While creating USCYBERCOM helps orchestrate all the cyberspace disciplines under one roof, the decision to subordinate it under the U.S. Strategic Command (USSTRATCOM) instead of establishing a new Functional Combatant Command (FCC) hinders the

commander's ability to perform global synchronization and prioritization as specified for FCCs in the Guidance for Employment of the Force (GEF).[21] As a result, this fractional reform effort further delayed the ability to conceptualize the future cyberspace environment and communicate a vision as is evident with President Obama's Cyber-Security Coordinator proclaiming that the U.S. was still struggling to define, let alone grasp, the concept of cyber warfare a full year after USCYBERCOM's activation.[22] In addition to challenges with command relationships and conceptualizing cyber warfare, there were also protracted delays with USCYBERCOM gaining operational control over the Cyber Mission Force Teams.[23] Initial operational capability (IOC) for these teams was not achieved until 2016, and their full operational capability (FOC) is not projected until later in 2018 due to defense management frictions associated with assimilating USCYBERCOM into the Joint Force.[24]

In 2010, the National Security Strategy (NSS) became the first strategy document to articulate concerns about cyberspace describing it as "one of the most serious national security, public safety, and economic challenges we face as a nation."[25] This breakthrough acknowledgement was a concerted attempt to manage national cyberspace implications, but it remained void of having a fundamental understanding of cyber warfare.[26] Former director of the Central Intelligence Agency, General Michael Hayden, captures this dilemma in his statement, "'rarely has something been so important and so talked about with less and less clarity and less and less understanding.'"[27] As a result, the 2010 NSS failed to adequately define either the strategic environment or cyber warfare and fell short in providing essential bridging guidance needed by the Secretary of Defense (SECDEF) and Chairman of the Joint

Chiefs of Staff (CJCS) to meet their U.S. Code Title 10 obligations. Without this guidance, the SECDEF and CJCS are unable to develop a prioritized strategy framework to counter cyber warfare threats, establish cyber warfare objectives and policies, provide strategic direction on the "the use and employment of military force," or conduct meaningful risk assessments within their respective National Defense Strategy (NDS) and National Military Strategy (NMS).[28]

By 2011, the DOD begins defining "cyberspace as an operational domain" and by 2017 the National Defense Authorization Act (NDAA) elevated USCYBERCOM to the status of a Functional Combatant Command.[29] These more recent national strategic-level publications demonstrate that DOD continues to organize and develop its cyberspace strategy but remains insufficient for developing a cyber warfare strategy or warfighting doctrine. Gaps in the current vision and strategy also raise concerns as to whether a cyber warfare strategy can be developed in sufficient time to avert a similar catalytic event as the MG.

Resembling Paradoxes

Despite the anticipation of automatic weapons, their arrival brought forth "no real value on the conventional battlefield" due to limited integration efforts until the Great War.[30] For the U.S., the MG was a "military non-starter" despite numerous trials and combat examples that reasoned otherwise.[31] Extensive trials to evaluate the merits of the MG between 1866 and 1870 arrived at the same general conclusion regarding its "superiority and great value" across a variety of military roles, and some even projected it would be "extensively employed in future wars by all civilized nations."[32] The MG and cyberspace share a perplexing paradox in that military leaders marveled at their

capabilities but fell short of appreciating “the extent to which they might be used on the battlefield."[33]

During the American Civil War, the Union employed the first repeating guns under the command of Col. John W. Geary who defensively engaged a charging Confederate Cavalry Squadron at 800 yards in Middleburg, Virginia. According to eyewitness accounts, this squadron was “cut up, and forced to retire by the hand-powered machine guns."[34] Less than a month later, Col Geary “shipped the guns back to Washington” reporting that the guns had proven “'inefficient, and unsafe to the operators.'"[35] Despite achieving precise long-range mass-effects, the significance of the MG as a technology disrupter against cavalry was overlooked. Assessing how the discernable effects of shattering an advancing cavalry squadron were so easily dismissed becomes an important strategic consideration as to whether similar barriers exist today that could contribute to overlooked cyber warfare effects.[36]

The Franco-Prussian War also provides examples where the significance of the French MGs (mitrailleuse) were overlooked. At the battle of Gravelotte, the French “mitrailleuse were placed on advantageous ground” and delivered “fearfully destructive fire” on the Germans.[37] At Mars la Tour, the 38th Prussian Infantry Brigade was forced to retreat into the valley due to French interlocking mitrailleuses’ fires before being nearly annihilated by the advancing mitrailleuses in a counterattack.[38] Despite numerous accounts of effective MG employment, the Franco-Prussian War became an “argument against the use of machine guns,” largely as a result of the German victors dismissing the merits of the mitrailleuse in their historical accounts.[39] Whether similar risks and present day cyberspace assumptions generate similar biases that preclude

the U.S. from decentralizing cyber warfare approaches is not yet apparent or may be unavailable due to classification.

Strategic Awakening

The devastating mass effects of WWI catalyzed the development of MG doctrine and organizational reform for defensive and offensive employment. On July 1, 1916, at the gut-rending Battle of the Somme, “three thousand men of 103 Brigade (Tyneside Irish), Thirty-Fourth Division suffered a 98% casualty rate.[40] The men left their trenches walked down the open slopes of the Avoca Valley" toward the German defensive line "a mile away."[41] German crews, sheltered “in deep dugouts,” had unknowingly survived the preparatory artillery barrage and lay in wait to employ well-emplaced interlocking fires to “cut down the ranks of the Irishmen as if they were wheat. When the 103 Brigade reached the front-line trench, two of its four battalions were gone."[42] A mere fifty survivors would remain after finally reaching the German trench line to move to the brigade objective.[43] These massive casualties reveal “the risks involved with employing units that are neither aligned nor sufficient for the mission” and bring to mind risks within cyber warfare in two alarming ways. First, there is the question as to whether the mass-effect potential of cyber warfare attack could ever deliver an equally devastating 98% effectiveness against a Joint or friendly force; and second is the more likely overconfidence in national-level long-range cyber activities that are likely to be as equally futile as the British preparatory artillery barrages when pitted against a near-peer adversary.[44]

Strategic Parallels between Cyberspace and the MG

The MG and cyber warfare share similar paths in that they originate as defensive weapons and gradually expand offensively. For the MG, the inability of the U.S. and its

Allies to conceptualize its future role for creating mass effects delayed the effective development of strategy and doctrine until forcefully pitted against the German's effective employment of the weapon during WWI. Correspondingly, fifty years of delay allowed nearly every nation to develop a cyber-defense program with at least 120 nation states "working on cyber-attack" programs as well.[45] There is no question that "cyberspace is now a contested operating realm at the strategic, operational, and tactical levels of war."[46] Nations with advanced cyber capabilities have the ability to "leap over traditional U.S. military forces and directly influence the decision calculations of political and military leadership."[47] In addition to global reach and abilities to circumnavigate U.S. military strengths, threats of cyberspace integration and synchronization with air, land, maritime and space as part of complex attack to deliver "physical, economic, and psychological consequences" against the Joint Force is real and present danger.[48] The U.S. is in a race to conceptualize cyber warfare's full potential, communicate a warfighting vision, and establish a strategy, and the following six strategic parallels describe the consequential similarities between cyberspace and the MG that will help contribute to a the development of cyber warfare strategies, theories, and doctrine.

Strategic Theorists

MG theory made its debut from prominent champions such as Theodore Roosevelt and Lieutenant John Parker who were the first to employ MG's offensively at the Battle for San Juan Hill in 1898 during the American-Spanish War.[49] In Theodore Roosevelt's assessment, the MG ascended as "inseparable companions throughout the siege," and he foresaw a future where "under almost all circumstances…could be pushed fairly to the front of the firing line."[50] By 1899, John Parker warned against the

Army's "mere gun" attitude, and emphasized that in order to become a serious "factor in warfare" it required a strategy and logistical employment concept to accompany the infantry for all mission types.[51] Together these two pioneers advocated that the American military needed to formulate a new organizational structure, develop employment strategies (including a combined-arms approach), and train both defensively and offensively with the MG.[52] However, even with a future President's theory of decentralized offensive employment, there remained no major organizational or doctrinal changes in the Army until December 10, 1917. On this date, Major General John Biddle, Acting Chief of Staff for the U.S. War Department, approved the publishing of a confidential circular on the employment of MGs based on experiences gained since the Battle of the Somme.[53] In today's complex strategic environment where adversaries are attempting to "counter U.S. and NATO power projection" with cyber capabilities, envisioning a cyber warfighting strategy is not clairvoyant.[54] Even so, General Robert Neller, 37th Commandant of the U.S. Marine Corps, appears to be a prominent visionary promoting the development of a cyber warfare strategy. General Neller has poignantly stated that "changes in the operating environment and adversary capabilities drive us to increase emphasis on maneuver in a cognitive sense, expanding our employment of combined-arms to space and cyberspace."[55] While not a theorist per se, General Neller possesses a powerful and credible advocacy voice analogous to Theodore Roosevelt. Whether his voice will prevail over strong detractors diverting the focus away from cyber warfare remains to be seen.

Distractions from Performance Attributes and Tools

Automating command, control, fires, sustainment, and other key warfighting functions created a vital competitive advantage for the military. However, it also

culturally reinforced a myopic focus on network and application functionality that hindered envisioning the future environment of globally interconnected platforms, and the ability to appreciate the full scope of what cyberspace would unleash as a warfighting domain.[56] The MG suffered a similar distraction where the military put little effort into the reform required to develop offensive and defensive doctrine due to being enamored with performance and evaluation criteria rather than operational capabilities.[57] During MG procurement, leaders became overly-fascinated with performance metrics and ideal features. Technical aspects of the gun such as discovering its ideal caliber, weight, and rate of fire supplanted strategic thinking opportunities, and failed to promote divergent thinking about doctrine and employment strategies.[58] This parallels challenges in cyberspace where the emphasis is on performance enhancing tools and technical capabilities rather than defining an encompassing cyber warfare strategy.[59] The cyberspace tool focus is not entirely surprising given the prevailing computer theory was Moore's law --a performance-based and exponential learning model that predicted the rate of a computer's speed was based on manufacturing advancements.[60] The military became enamored with rapidly increasing processing speeds, efficiency, storage, security, encryption, and transmission rates. Like the MG, methods of thinking and resources become mired into a subcategory of performance-based metrics that inhibit the development and alignment of doctrine. Even the 2017 NSS perpetuates this alignment impediment by appealing for improvements in "our cyber tools across the spectrum of conflict" at the expense of offing guidance for developing cyber strategies, integrating government agencies, or delegating cyberspace operational authorities down to operational levels.[61]

Conceptual Barriers to Strategic Vision

Conceptualization challenges from being caught with “methods and thinking in transition” between centuries and failing to “ask the right questions” delayed strategic leaders from envisioning the full disruptive potential of both the MG and cyberspace.[62] For the MG, this meant the Army was unprepared for war in 1917 due to its inability to “respond adequately to the organizational and doctrinal changes" necessary for machine warfare, and because many officers “did not have the necessary skills, command structure, [or] view of technology” that would have enabled them “to imagine a mechanized and offensive battlefield.”[63] The Battle of the Somme cast aside these barriers and rapidly transformed previous conceptions about offensive operations, horse-mounted cavalry, frontal attacks, and unsupported offensive raids. It also forced new innovative MG countermeasures such as the tank. The Army’s fifty-year failure to develop effective machine doctrine was finally mended on December 10, 1917 when Major General John Biddle, Acting Chief of Staff for the U.S. War Department, approved a confidential U.S. Army War College publication for employing the MG.[64]

In cyberspace, conceptualizing the more frequently occurring issues such as cyber-espionage, cyber-crimes, and cyber-terrorism are far easier than visualizing cyber warfare which has yet to materialize in the form of “large-scale cyber-attacks” contributing to physical damage.[65] Even when cyber warfare has been applied such as in “Estonia(2007), Georgia(2008), and Iran(2010)” these applications have all “been relatively ‘isolated’ and ‘low-level’ in nature.”[66] Yet the potential for adversaries to employ cyberspace operations to cause mass disruption due to global reach, windows of superiority, and the ability to produce multi-domain effects “greater than the sum” of their envisioned capabilities could become equally devastating as the Battle of the

Somme for Joint Force operating in a contested environment.[67] Twentieth century leaders were “unused to thinking deeply about technology and its effect upon the nature of battle” and were “unable to draw upon past experiences for guidance.”[68] Leaders today are also forced to “’muddle through’” and learn about the many diverse taxonomies of cyberspace in the midst of a long war.[69] Cyberspace has been largely uncontested in Iraq, Afghanistan, and against the Islamic State of Iraq and the Levant (ISIL), which reinforces assumptions that centrally managed cyber warfare dependably achieves favorable results. Likewise, years of competing in cyberspace against great powers that deliberately operate “below the threshold of provoking conflict” also reinforces the unsupported convictions that a centrally managed national-level organization and cyberspace strategy postures the U.S. effectively for the future strategic environment.[70] Believing that these past successes will hold true during a high-intensity conflict against a great power amounts to being a dangerously "stubborn adherence to an erroneous theory" that can cause “decision makers become structurally blind to significant changes in the environment.”[71] Andrew Hill and Stephen Gerras call this the "troublesome legacy of success" where "theories that were once the basis for dominance” become “barriers to innovation and frustrate adaptation."[72]

Social and Cultural Barriers to Developing Effective Doctrine

Research conducted by Elizabeth Kier suggests that the preference to principally develop a defensive approach is rooted in social and cultural issues more than “structural conditions or functional needs.”[73] This premise is already recognized for the MG, and intimates that culture serves as a barrier toward developing cyberspace offensive doctrine.[74] Kier argues that culture has an “independent causal role” that “significantly affects choices between offensive and defensive military doctrines.”[75] The

interaction between constraints within civil-military cultures determines the “choices between offensive and defensive military doctrines” and affects “both the likelihood that wars will break out and the outcome of wars that have already begun.”[76] Although comparing cultural environments of the U.S. during the period of the MG and cyberspace was initially outside the scope of this research, the following sections will briefly highlight apparent risks with civil-military; military; literature; and individual-level social and cultural factors. Each of these areas is worth researching further in regarding to biases for assimilating new technologies into defensive-centric doctrine.[77]

Kier’s research fundamentally means that “military preferences cannot be deduced from the functional needs of military organizations,” and that DOD’s attempts to adapt to the future cyber warfare environment may be culturally constrained by domestic prioritization to defend the homeland.[78] For example, during WWI, the French’s “version of peace at home took precedence over sources of instability abroad” that resulted in building the Maginot Line instead of developing offensive doctrine and technologies.[79] Domestic resistance to DOD’s offensive cyber capabilities, which could fearfully be employed as a “political instrument,” as well as shifts in the “balance of control” have culturally influenced strategy by increasing operational oversight and restricting the level of delegated authorities for cyberspace operations (DACO).[80] Conversely, unbearable domestic ramifications (political, social, economic) resulting from a cyberattack of significant consequence on the homeland have expanded DOD’s defensive cyberspace obligations to protect nation interests residing across other instruments of national power to the degree that the “categories of political and military

matters are difficult to distinguish."[81] Further research is required to examine civil-military social and cultural barriers affecting cyber warfare strategies.

The military's internal cultural beliefs can also "shape how the organization integrates the changes in its external environment with its doctrinal orientation."[82] Even if domestic cyberspace constraints for defending the homeland were alleviated and warfighting authorities were granted, cultural differences across the military services, and among allies would account for different doctrinal preferences.[83] Complacency with technological exceptionalism is another cultural risk. The more complacent DOD becomes with operating successfully in the current environment, the greater the chances of DOD overlooking key strategic factors as they evolve, especially for major combat operations. Further research is necessary to determine if cultural differences across the services or technological complacency are interfering with developing cyber warfare doctrine.

Literature also culturally influences doctrine. Despite numerous German accounts crediting the French for effective employment of the mitrailleuses, prejudicial literature following the Franco-Prussian War played a large role in shaping opinions about the MG snice the victors were not inclined to endorse "the tactics and arms of their defeated adversaries."[84] There is risk today with literature trumpeting successes of a nationalized approach helping thwart attacks on the homeland, and successful cyber-attacks against asymmetric adversaries supplanting efforts to develop a comprehensive cyber warfare strategy during high-intensity conflict.

At the individual level, many nineteenth century military officers came from "landowning classes that had been left behind by the Industrial Revolution" and

attempted to shape the army with the “attitudes and the life-style that had characterized the pre-industrial world.”[85] To them, machine warfare contributed to more than just destructive fires, but also the destruction of “the traditional social order” and “the old certainties of the battlefield – the glorious charge and the opportunities for individual heroism.”[86] Stubborn adherences to a “myopic outlook amongst military leaders” of the nineteenth century.”[87] Just before the start of WWI, some commanders wanted to “'take the damned things [MGs] to a flank and hide them!'"[88] Understanding how individual cultural may present barriers for cyberspace is worth further research. The effects of the Information Revolution on senior officers could culturally influence how they shape the military with attitudes of lifestyles characterizing a pre-Informational world.

Defense-Centric Employment Approaches

Early traces of MG reform began in 1910 with the U.S. War Department’s Circular No. 2, which advocated breaking up company-sized MG units to employ them tactically as “integral parts of regiments rather than as separate organizations.”[89] However, the circular resonated with the prevailing bias both toward the MG and a defense-centric employment. The MG was touted as “mere auxiliary weapon” particularly adapted for defense whose moral effect was its “nerve-racking rattle.”[90] As aforementioned, the revised version of this publication following the Battle of the Somme rectifies both organizational and employment biases. In cyberspace, current strategy also defense-centric focusing on protecting national infrastructure, homeland security, and against cyber-criminal activity, cyber hacktivists, and disruption.[91] Furthermore, efforts to develop cyber norms and laws concerning cyber-crimes, data protection, network defense, and response actions to cyber-attacks are also defense-centric in nature. While protecting the national infrastructure, the homeland, and

networks are necessary aspects of cyber warfare, they are not sufficient to develop a comprehensive cyber warfare strategy that also includes Joint Operations in contested environments.[92] An onerous focus on protecting national interest yields a narrow interpretation of cyber as being a 'means' to an 'end' to conduct "reconnaissance, espionage, influence, and even attacks in cyberspace."[93] This in itself is a barrier to conceptualizing the future environment because this perspective overlooks the more dangerous scenario where cyber, as a combined-arm, becomes a 'means' to a more sophisticated 'ways' to deliver complex and catastrophic consequences to Joint Forces operating beyond the protection of national-level cyberspace defenses. Case in point, many cyber incidents against the U.S. share a similarity with ineffective MG employment that "'seriously got on the nerves of those subjected to their fire" but the significance of its employment was transitory."[94]

The 2017 NSS sets the conditions for a substantial homeland defense bias to permeate throughout subordinate strategy with a constrained interpretation that threatening cyberspace actions will be used to manipulate political, economic, informational, and even military activities.[95] While the NSS certainly must broadly relate security to all instruments of national power, it falls short of providing sufficient DOD guidance to generate an effective cyber warfare strategy. As an example, the 2018 NDS urges "continued integration of cyber capabilities into the full spectrum of military operations," but the NSS's homeland defense influence results in a misalignment of "what" and "who" to defend against.[96] This misalignment can be observed in the NSS's depicted cyberspace environment which omits association to the major state actors and myopically categories cyber threats as being "terrorists, trans-national criminal

organizations, cyber hackers and other malicious non-state actors" that have "transformed global affairs with increased capabilities of mass disruption."[97] Even the 2017 NDAA, which calls for innovation fails to promote DOD cyber warfare capabilities beyond countering adversaries using cyber.[98] This misalignment trickles down even further into the five strategic initiatives found within the *DOD Strategy for Operating in Cyberspace*, which also disproportionally weighs defending the homeland.[99] As one might expect, Joint Publication 3-27 (JP 3-27), *Homeland Defense*, is homeland defense-centric. However, JP3-27 also arbitrarily extends cyberspace strategy objectives into the "forward regions" and places requirements on the Joint Force to "detect, deter, prevent, or when necessary defeat threats to the US" based on "increased capability for cyberspace operations against the United States Government, Department of Defense, and nations' critical infrastructures."[100] Collectively, the NDS, *DOD Strategy for Operating in Cyberspace*, and JP 3-27 fail to establish a warfighter's strategy for cyberspace comprised of cyber maneuvering and combined-arms for winning wars.[101] Even Joint Publication 3-12(R) (JP 3-12(R)), *Cyberspace Operations*, which prioritizes "Nation States" as the most dangerous of four cyberspace threats to a Joint Force Commander (JFC), immediately becomes misaligned by describing the cyber threat as other nations' abilities to "employ cyberspace to either attack or conduct espionage against the U.S."[102]

Aligning cyberspace strategy principally with defending the has become a crucial impediment to understanding the strategic environment and conceptualizing the potential and actual implications of cyber warfare.[103] Similar to the MG, current strategy imposes risk that current means and approaches are inadequate to support Geographic

Combatant Commands (GCCs) with viable decentralized cyberspace capability during high intensity or simultaneous conflicts.

Cyber-Specific Barriers

This research exposes three cyber-specific challenges toward understanding and employing cyber warfare. The first is the late-start in recognizing cyberspace's potential for gaining advantages in combat delayed the natural progression of its strategy development and was confounded by an abundance of cyber taxonomies. Also unique to U.S. cyberspace operations is a civil-military relationship imbalance from having the preponderance of strategic military guidance geared toward protecting the homeland without a corresponding cyber warfare strategy for the Joint Operating Force. This has enabled military defensive cyberspace capabilities to branch out across into other instruments of national power to help protect national infrastructure, whereas cyberspace authorities needed for CCDRs to conduct cyberspace operations remain in control by civilian authorities.[104]

Lastly, the most consequential challenge is the cognitive dissonance between current strategy and Joint operating concepts as to whether cyberspace is a domain, a combined-arm, or both. In the U.S., cyberspace is the only warfighting domain that has its own combatant command. Making cyberspace one of "five warfighting domains has led the joint force into a conceptual cul-de-sac that undermines the ability to think holistically."[105] Considering cyberspace solely as a domain is particularly "problematic because the construct denotes terrestrial ownership and implied uniformity" with other domains such as basic assumptions about time and space, which are constantly changing in cyberspace.[106] Herein lies a common fallacy when it comes to controlling cyberspace-- control is not zero-sum, "but is instead a trichotomous concept: one may

deny control to others, one may take-it for oneself, and one may subsequently exercise it."[107] In cyberspace, it is fully possible to “deny control to another without being able to acquire and exercise it oneself."[108] This trichotomous concept must become a vital element of cyber warfare theory, and another compelling reason why the U.S. needs a theory for cyber warfare.

For years scientist argued whether light was a wave or a particle before eventually it was proven that light simultaneously behaves as both as a particle and a wave.[109] A similar dual-nature struggle exists today in cyber warfare between being a domain and a combined-arm. Concepts documents such as the Multi-Domain Battle Concept calls upon the “Joint Force and its partners to defeat the enemy’s conventional forces in a rapid campaign of maneuver across all areas of the expanded battlespace in multiple domains and locations simultaneously.”[110] The Capstone Concept for Joint Operations (CCJO) states “the future Joint Force will view jointness as a holistic application of force from a global cross-domain perspective rather than limiting it to integration of Service capabilities.”[111] Even Joint Publication 3-12(R) (JP 3-12(R)), Cyberspace Operations, reinforces that commanders need to “be prepared to conduct operations under degraded cyberspace conditions” and that they must conduct cyberspace operations “to retain freedom of maneuver in cyberspace, accomplish JFC objectives, deny freedom of action to adversaries, and enable other operational activities.”[112] U.S. cyberspace strategy as currently written hinders these concept documents from attaining “improved flexibility in delegating authorities and allocating resources” and improving “the Joint Force’s ability to operate in contested and degraded

information environments, maintaining advantages in cyberspace, space, and across the electromagnetic spectrum."[113]

The current emphasis for a national-level centralized cyber defense does not sufficiently address Joint Force requirements or their challenge to "improve the Joint Force's ability to operate in contested and degraded information environments, maintaining advantages over adversaries in cyberspace, space and across the electromagnetic spectrum."[114] This is especially true in cases where adversaries that are flattening their organization structure by integrating cyberspace and electronic warfare into their operational units.[115] Cyberspace inherently is more than just a warfighting domain for the Joint Force, and must become part of the evolution of combined-arms. The Joint Force will need to "integrate the full range of capabilities across time and space to create windows of advantage that enable maneuver in contested environments."[116] Cognitive Dissonance between cyberspace strategy and concept documents will persist so long as the preponderance is aligned and focused on defense of the homeland, failure to recognize its combined-arms attributes, and failure of force structure to provide resilience and support to the warfighter.

Conclusion

The research reveals that drawing upon past MG lessons will position the U.S. with a great advantage toward developing a cyber warfare strategy.[117] Common barriers for conceptualizing the future environment include a lack of having a relevant theory for understanding and analyzing strategic and disruptive potentials, becoming enamored with performance attributes, and defensive-centric biases. This research also concludes that delays in recognizing cyberspace's warfighting advantages combined with confounding distractions from various cyber taxonomies perpetuated several cyber-

specific challenges. These challenges are cognitive dissonance between current strategy and Joint operating concepts and civil-military tensions within the DOD cyberspace framework that could challenge distinguishing between political and military matters during wartime.

Current DOD cyberspace strategies and authorities, align primarily at the national-strategic level to defend the homeland, without sufficient bridging guidance to translate into national military and theater-level strategies. Defending the homeland against existential threats must remain part of a cyber warfare strategy, but it is equally important to develop strategy aspects focused on enabling CCDRs to prosecute theater level operations in a degraded environment isolated from the homeland. For this, a cyber warfare theory is needed to devise a warfighting strategy that fully embraces the dual-nature of cyberspace as both a domain and a combined-arm. Joint concept documents are gradually shifting the cyber warfare focus toward the GCCs. It is time for cyberspace authorities currently retained at the highest level to be delegated to operational units promoting alignment between operational force expectations and actual Joint capabilities.

These crucial impediments obstruct conceptualizing the potential and actual implications of cyber warfare, and posturing DOD effectively for the future strategic environment. Left unresolved, a formidable adversary's overmatch in cyberspace integration and synchronization could isolate a Joint Force from national-level cyber capabilities and serve as a catalyst for organizational and doctrinal changes as occurred with the machine gun.

Recommendations

Establish a DOD think-tank to function as the “inventive genius” to contemplate on the relevance of existing theory while identifying the unique characteristics of cyber warfare in order to postulate a theory that depicts cyber warfare’s dual-nature as being both a domain and a combined-arm. The resulting theory would then aid in developing a cyber warfare strategy that embraces Joint concepts and DOD homeland defense requirements to best determine cyberspace’s “tactical place, organization, and uses.”[118]

Update the NSS and NDS to remove distracting cyber taxonomies and provide cyber warfighting guidance aligned with the major state actors distinct from homeland defense and national-level cyber objectives. This update is essential achieving a balanced civil-military relationship across defensive and offensive cyberspace operations, and for developing a military cyber warfare strategy with military end states. These actions will also help ensure that strategic preparedness for the future strategic environment can “be measured against some benchmark” without misidentified threats that shape the U.S. response.[119]

Delegate cyberspace authorities with accompanying rules of engagement to operational levels to empower the GCCs to fight both defensively and offensively in a contested environment without USCYBERCOM coordination requirements.

Restructure and modernize the Cyber Mission Force to enable Joint Force Commanders to conduct cyberspace operations with organic combat mission forces of armed conflict without USCYBERCOM coordination requirements.

Endnotes

[1] Carl von Clausewitz, *On War*, ed. and trans.by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 127.

[2] David A Armstrong, *Bullets and Bureaucrats: The Machine Gun and the United States Army, 1861-1916,* vol. 29 (Westport, CT: Greenwood Press, 1982), xiii, 212.

[3] Ibid., xv.

[4] Ibid.

[5] Robert M. Gates, "United States Military Academy," public speech, US Military Academy, West Point, NY, February 25, 2011, http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1539 (accessed March 11, 2018); For background on two examples military reform resulting from crisis to include the minie ball and logistics, see Allan W. Howey, "The Widow-Maker," *Civil War Times Illustrated Online* 38, no. 5 (1999): 46-51, in ProQuest (accessed March 16, 2018); Robert D. Paulus, "From Santiago to Manila: Spanish-American War logistics," *Army Logistician Fort Lee Online* 30, no. 4 (July/August 1998): 18-23, in ProQuest (accessed March 16, 2018).

[6] Clausewitz, *On War*, 594.

[7] Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: Simon & Schuster, 2002), 243.

[8] John Ellis, *The Social History of the Machine Gun* (New York: Pantheon Books, 1975), 16; Robert Bruce, *Machine Guns of World War I* (London: Windrow & Greene, 1997), 6.

[9] Samuel P. Mowery, *Defining Cyber and Focusing the Military's Role in Cyberspace,* Strategy Research Project (Carlisle Barracks, PA: US Army War College, March, 2013), 15.

[10] Glen Alexander Crowther, "The Cyber Domain," *Cyber Defense Review Online* 2, no. 3 (Fall 2017): 66, http://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2017.pdf (accessed January 15, 2018).

[11] Ellis, *The Social History of the Machine Gun*, 10-11, 16.

[12] Ibid., 16-17.

[13] For background on the US War Department's first classified release on machine gun employment concepts see US Army War College ed., *Notes on The Employment of Machine Guns no. 712*, Training Circular No. 2 (Washington DC: Government Printing Office, 1918).

[14] Vinton G. Cerf, "The Day the Internet Age Began: Forty Years Ago Today the First Message was Sent Between Computers on the ARPANET," *Nature 461 Online,* no. 7268 (October 2009): 1202-1203, in ProQuest (accessed January 7, 2018).

[15] Cerf, "The Day the Internet Age Began," 1202-1203; Clausewitz, *On War*, 127; US Department of Defense, *The Department of Defense Cyber Strategy* (Washington, DC: US

Department of Defense, April 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed November 20, 2017).

[16] Cerf, "The Day the Internet Age Began," 1202-1203.

[17] Ibid.

[18] Ibid.

[19] For background information on C4ISR expenditures between 2011 to 2013 see John Keller, "DOD Earmarks at Least $31.6 Billion for C4ISR Procurement and Research Next Year," *Military & Aerospace Electronics Online*, February 2012, http://www.militaryaerospace.com/articles/2012/02/dod-earmarks-billions-for-c4isr-in-2013.html (accessed February 14, 2018); For background information on C4ISR expenditures between 2015 and 2016 see John Keller, "2016 DOD Budget for Communications, Electronics, and Intelligence Headed Up After Two Flat Years," *Military & Aerospace Electronics Online*, February 2015, http://www.militaryaerospace.com/articles/2015/02/2016-ceti-budget.html (accessed February 14, 2018).

[20] James A Green, *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge, 2015), 1; Andrew Hill, *The Devil You Know: Strategic Thinking in Complex Adaptive Systems*, Faculty Paper (Carlisle Barracks, PA: US Army War College, August 2017), 2-3.

[21] US Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: US Joint Chiefs of Staff, January 17, 2017), V-7, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed December 14, 2017).

[22] Sean Lawson, "General Alexander's Confirmation and The Failure of Cyberwar Transparency," *Forbes Online*, May, 13, 2012, http://www.forbes.com/sites/firewall/2010/05/13/general-alexanders-confirmation-and-the-failure-of-cyberwar-transparency/ (accessed October 26, 2017).

[23] US Cyber Command, "All Cyber Mission Force Teams Achieve Initial Operating Capability," October 24, 2016, linked from the *US Department of Defense Home Page* at "Article," https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/ (accessed November 22, 2017).

[24] Ibid.

[25] Barack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27, http://nssarchive.us/NSSR/2010.pdf (accessed December 15, 2017).

[26] Lawson, "General Alexander's Confirmation and The Failure of Cyberwar Transparency."

[27] Green, *Cyber Warfare: A Multidisciplinary Analysis,* 3.

[28] US Code Title 10 - Armed Forces (1956) with 2017 changes), I, §§113, 153, http://uscode.house.gov/browse/prelim@title10&edition=prelim (accessed November 8, 2017).

[29] US Senator John McCain (Chairman) and US Senator Jack Reed (Ranking Member), *National Defense Authorization Act For Fiscal Year 2017: NDAA FY17 Executive Summary* (Washington DC: Senate Armed Services Committee, 2017), https://www.armed-services.senate.gov/imo/media/doc/FY17%20NDAA%20Bill%20Summary.pdf (accessed November 30, 2017); Obama, *National Security Strategy;* For background on US Cyber Command's (USCYBERCOM) activation, reference US Strategic Command, "Fact Sheet, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed February 19, 2018); US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: US Department of Defense, 2011), 5, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed February 18, 2018).

[30] Ellis, *The Social History of the Machine Gun,* 10, 15; Bruce, *Machine Guns of World War I,* 6.

[31] Ibid., 15; Ibid., 6.

[32] Unknown Author, *The Gatling Gun: Official Reports of Trials, Description, General Directions, Targets, &c* (Hartford, CT: Case, Lockwood & Brainard Co., printers, 1878), 4-27, 44; Honorable Gideon Welles, *Official Report of the Naval Officers* (Washington DC: US Navy, May 30, 1868) quoted in *The Gatling Gun,* 6-7; Special Committee on Mitrailleuses, *Official Report of Trials at Shoeburyness* (Shoeburyness, England: British Navy, October 28, 1870) as quoted in *The Gatling Gun*, 8-9.

[33] Ellis, *The Social History of the Machine Gun*, 37.

[34] Armstrong, *Bullets and Bureaucrats,* 18.

[35] Ibid., 19.

[36] Ibid.

[37] John H. Parker, *Tactical Organization and Uses of Machine Guns in the Field* (Kansas City, MO: Hudson-Kimberly Publishing Co, 1899), 15.

[38] Ibid., 19.

[39] Ibid., 14-15.

[40] Armstrong, *Bullets and Bureaucrats,* xi.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Thomas P. Galvin, *Military Preparedness*, Faculty Paper (Carlisle, PA: US Army War College, Department of Command, Leadership and Management, US Army War College, 2016), 3.

[45] Green, *Cyber Warfare: A Multidisciplinary Analysis*, 3.

[46] Secretary of Defense Jim Mattis, *A Written Statement for the Record: Statement of the Secretary of Defense before the Senate Armed Services Committee*, 115th Cong., 1st sess., June 13, 2017, https://www.armed-services.senate.gov/imo/media/doc/Mattis_06-13-17.pdf (accessed February 13, 2018).

[47] US Joint Chiefs of Staff, *The Joint Force in a Contested and Disordered World*, Joint Operating Environment 2035 (Washington, DC: US Joint Chiefs of Staff, July 14, 2016), 7, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917 (accessed January, 15, 2018).

[48] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community: Statement of the Director, National Intelligence Agency before the Senate Select Committee* 115th Cong., 1st sess., May 11, 2017, 1, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf (accessed November 28, 2017); US Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R) (Washington, DC: US Joint Chiefs of Staff, February 5, 2013), I-7, http://www.jcs.mil/doctrine/new_pubs/jp3_12R.pdf (accessed January 10, 2018).

[49] For more information on Lieutenant John Parker, Theodore Roosevelt's Gatling detachment Officer during the Spanish-American War, reference Parker, *Tactical Organization and Uses of Machine Guns in the Field.*

[50] John H. Parker, *History of the Gatling Gun Detachment, Fifth Army Corps, at Santiago: With a Few Unvarnished Truths Concerning that Expedition* (Kansas City, MO: Hudson-Kimberly Publishing Co, 1898), 2-4.

[51] Parker, *Tactical Organization and Uses of Machine Guns in the Field*, 6-7.

[52] Ibid., 9.

[53] For background on US War Departments study of scientific machine gunnery and employment concepts learned since the Battle of the Somme on 1 July, 1916 see US Army War College ed., *Notes on The Employment of Machine Guns no. 712*.

[54] Joseph Dunford, *A Statement of the Posture of the 19th Chairman of the Joint Chiefs of Staff before the 115th Congress Senate Armed Services Committee Budget Hearing,* Posture Statement presented to the 115th Cong., 1st sess. (Washington, DC: CJCS, June 13, 2017), https://www.armed-services.senate.gov/imo/media/doc/Dunford_06-13-17.pdf (accessed February 13, 2018).

[55] General Robert B. Neller, Commandant United States Marine Corps, A *Statement on the Posture of the Department of the Navy Before the Senate Committee on Armed Services,* Posture Statement presented to the115th Cong., 1st sess. (Washington DC: USMC, June 15, 2017) https://www.armed-services.senate.gov/imo/media/doc/Neller_06-15-17.pdf (accessed February 13, 2018).

[56] For more information on the theory of enhanced attitude as a result of repeated encounters, reference "Mere Exposure Effect," *Psychology Research and Reference Online*,

https://psychology.iresearchnet.com/social-psychology/social-influence/mere-exposure-effect/ (accessed Sept 10, 2017).

[57] Armstrong, *Bullets and Bureaucrats*, 211.

[58] For more information on Machine Gun trials reference *The Gatling Gun.*

[59] For more information on challenges and emphasis placed on cyber tools, reference Cyber Security Community, "Over Reliance On Monitoring Tools - Let Us Understand Few Pre-Setup Steps," linked from the *Cyber Security Community Home Page,* https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/05/05/over-reliance-monitoring-tools-let-us-understand-few-pre-setup-steps (accessed February 19, 2018); Preston Brown, Kallan Christensen, and David Schuster, "An Investigation of Trust in a Cyber Security Tool," *SAGE Journals Online* 60, no. 1 (September 15, 2016): 1454-1458, http://journals.sagepub.com/doi/abs/10.1177/1541931213601333 (accessed February 19, 2018).

[60] For more information on Moore's Law, reference Mark Lundstrom, "Moore's Law Forever?" *Science Online* 299 no. 5604 (January 2003): 210, http://science.sciencemag.org/content/299/5604/210 (accessed February 17, 2018).

[61] Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 32, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed February 20, 2018).

[62] Armstrong, *Bullets and Bureaucrats,* xv, 214.

[63] Armstrong, *Bullets and Bureaucrats,* xv; Parker, *Tactical Organization and Uses of Machine Guns in the Field,* 8; Elizabeth Kier, *Imagining war: French and British Military Doctrine Between the Wars* (Princeton, N.J: Princeton University Press, 1997), 144.

[64] For background on US War Departments study of scientific machine gunnery and employment concepts learned since the Battle of the Somme on 1 July, 1916 see US Army War College ed., *Notes on the employment of machine guns no. 712*.

[65] Green, *Cyber Warfare,* 1.

[66] Ibid.

[67] US Department of Defense, *Capstone Concept for Joint Operations: Joint Force 2030 (CCJO)*, Draft Working Document, Predecisional (Washington, DC: US Department of Defense, as of June 28, 2016), 3, 6.

[68] Armstrong, *Bullets and Bureaucrats,* xiii.

[69] Ibid.

[70] US Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017* (Washington, DC: Office of the Secretary of Defense, May 15, 2017), i, 19, 53-54,

https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF (accessed February 15, 2018).

[71] Andrew Hill and Stephen Gerras, "Systems of Denial: Strategic Resistance to Innovation," *Naval War College Review* 69, no. 1 (Winter 2016): 114-115.

[72] Ibid.

[73] Kier, *Imagining war*, 140.

[74] Ellis, *The Social History of the Machine Gun*, 9, 17.

[75] Kier, *Imagining war*, 5.

[76] Ibid., 3, 5.

[77] Ibid., 144.

[78] Kier, *Imagining war*, 143; General Robert B. Neller, A *Statement on the Posture of the Department of the Navy.*

[79] Kier, *Imagining war*, 141.

[80] US Department of Defense, *The Department of Defense Cyber Strategy*, 2, 6; US Joint Chiefs of Staff, *Joint Operations*, III-6; Andrew Hill, "Military Innovation and Military Culture," *Parameters* 45, no. 1 (2015): 89-92.

[81] Kier, *Imagining war,* 140; US Department of Defense, *The Department of Defense Cyber Strategy*, 5; US Joint Chiefs of Staff, *Cyberspace Operations*, I-8; Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime,* 243.

[82] Kier, *Imagining war*, 143.

[83] Ibid., 4.

[84] Parker, *Tactical Organization and Uses of Machine Guns in the Field*, 22.

[85] Ellis, *The Social History of the Machine Gun,* 16.

[86] For background on how honorable warfare relates to cultural resistance, see Hill, "Military innovation and military culture," 88-93; Ellis, *The Social History of the Machine Gun,* 17.

[87] Ellis, *The Social History of the Machine Gun,* 17.

[88] Ibid., 17-18.

[89] US War Department, *Training Circular No. 2* (Washington DC: Government Printing Office, January 14, 1910), 4.

[90] Ibid.

[91] For background on national cyberspace precedence on defending the homeland, see Trump, *National Security Strategy of the United States of America*, 31-32; Jim Mattis, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington DC: US Department of Defense, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed February 1, 2018); US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*; US Joint Chiefs of Staff, *Homeland Defense*, Joint Publication 3-27 (Washington, DC: US Joint Chiefs of Staff, July 29, 2013), I-9, http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf (accessed January 19, 2018).

[92] Andrew Hill and Stephen Gerras, *Stuff Happens: The Art and Science of Causation in Policy and Strategy,* Working Paper (Carlisle Barracks, PA: US Army War College, August 2016), 4.

[93] Coats, *Worldwide Threat Assessment of the US Intelligence Community, 1.*

[94] Bruce, *Machine Guns of World War I*, 7.

[95] Trump, *National Security Strategy of the United States of America*; Obama, *National Security Strategy*.

[96] Mattis, *Summary of the 2018 National Defense Strategy of The United States of America*, 3, 6.

[97] Ibid.

[98] McCain and Reed, *National Defense Authorization Act For Fiscal Year 2017*.

[99] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*. 5-12.

[100] US Joint Chiefs of Staff, *Homeland Defense*, I-9.

[101] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 5-12.

[102] US Joint Chiefs of Staff, *Cyberspace Operations*, I-6.

[103] Green, *Cyber Warfare: A Multidisciplinary Analysis*, 3.

[104] US Department of Defense, *The Department of Defense Cyber Strategy*, 2.

[105] Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," May 26, 2017, linked from the *Strategy Bridge Home Page*, 6, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal (accessed January 7, 2018).

[106] Heftye, "Multi-Domain Confusion," 3; For background information on cultural assumptions about reality and truth see Edgar H Schein, *Organizational Culture and Leadership,* 3rd ed. (San Francisco, CA: John Wiley & Sons, Inc, 2004), 137-140.

[107] Lukas Milevski, "Fortissimus Inter Pares: The Utility of Landpower in Grand Strategy." *Parameters* 42, no. 2 (Summer 2012): 7.

[108] Ibid.

[109] Ecole Polytechnique Federale de Lausanne, “The first ever photograph of light as both a particle and wave” March 2, 2015, linked from the *Phys.Org Home Page* at “Optics & Photonics,” https://phys.org/news/2015-03-particle.html (accessed March 27, 2018).

[110] US Army and US Marine Corps, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040*, Draft v1.0 (Washington, DC: US Army and US Marine Corps, October 2017), 22.

[111] US Department of Defense, *Capstone Concept for Joint Operations: Joint Force 2030 (CCJO)*, 6.

[112] US Joint Chiefs of Staff, *Cyberspace Operations*, I-1, I-6.

[113] US Department of Defense, *Capstone Concept for Joint Operations: Joint Force 2030 (CCJO)*, 9.

[114] Ibid.

[115] For background information on Russian integrated combined arms in maneuver forces, see Scott Boston and Dara Massicot, “The Russian Way of Warfare: A Primer,” linked from the *Rand Corporation Home Page*, https://www.rand.org/pubs/perspectives/PE231.html (accessed February 19, 2018).

[116] US Army and US Marine Corps, *Multi-Domain Battle,* 2-3.

[117] Parker, *Tactical Organization and Uses of Machine Guns in the Field*, 11.

[118] Parker, *Tactical Organization and Uses of Machine Guns in the Field*, 5; For more information on military genius, reference Clausewitz, *On War*, 100-112.

[119] Galvin, *Military Preparedness*, 4.