REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/28/2017	Master's Thesis	AUG 2016 - APR 2017

4. TITLE AND SUBTITLE
Maneuver in the Cyberspace Domain: Dominating the Enemy

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Phillips, Jennifer L., Maj, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This thesis addresses the pressing requirement that our national defense organizations invest in capabilities, tactics, and training to successfully conduct tactical maneuver in the cyber domain in both an offensive and defensive manner. Placing emphasis on doctrinal concepts; tactics, techniques, and procedures (TTPs); and exercise and simulation trials to exploit tactical maneuver in the cyber domain to achieve effects in the virtual, physical, and cognitive dimensions is the proper focus of military theorists and planners at this juncture.

15. SUBJECT TERMS
maneuver; cyberspace; cyber domain; tactics; virtual; cognitive; physical; military theory; planning; offensive; defensive; multi-domain; doctrine

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Command and Staff College
Unclass	Unclass	Unclass	UU	43	19b. TELEPHONE NUMBER *(Include area code)* 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: Maneuver in the Cyberspace Domain: Dominating the Enemy

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

AUTHOR: Jennifer L. Phillips

AY 16-17

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: 5 May 17

Oral Defense Committee Member: _____
Approved: ✓
Date: 5MAY17

Executive Summary

Title: Maneuver in the Cyberspace Domain: Dominating the Enemy

Author: Jennifer L. Phillips

Thesis: This thesis will directly address the pressing requirement that our national defense organizations invest in capabilities, tactics, and training to successfully conduct tactical maneuver in the cyber domain in both an offensive and defensive manner. Placing emphasis on doctrinal concepts; tactics, techniques, and procedures (TTPs); and exercise and simulation trials to exploit tactical maneuver in the cyber domain to achieve effects in the virtual, physical, and cognitive dimensions is the proper focus of military theorists and planners at this juncture.

Discussion: The ability to conduct tactical maneuver in the cyberspace domain as part of a combined arms multi-domain maneuver operation will be an essential requirement for the United States in future operations in order to dominate the enemy. The emphasis on developing a viable approach to tactical cyber maneuver is based on a forecasting model that appreciates the exponential growth of the cyber domain at the system level and accepts that the cyber domain will become ubiquitous, pervading every aspect of human daily life over the next 20-40 years. Places without bases pose a problem in that they often limit our ability to seize the initiative and integrate offensive and defensive maneuver across all domains in the conduct of military operations. By virtue of operating in a place without a base, a situation becomes apparent where military actions are necessary but not at a time or place of our choosing. U.S. military forces may find that they can control certain strategic level considerations within the cyber domain, but the commercial, civilian, and systemic influences of the cyber domain will demand that tactical and operational military entities act through and in this domain. Military forces will both influence, and be influenced by, the existence of the Internet of Things (IoT) in the conduct of their duties across the range of military operations (ROMO).
When facing an enemy of technological and procedural parity, the military actor is at an asymmetric and/or technological disadvantage in the virtual, cognitive, and/or physical dimensions. The global trend towards an increasingly urban population is intertwined with a rise in non-state actor challenges to traditional concepts of post-Westphalian sovereignty. As a result, future conflicts not at a time or place of our choosing will require that the conceptual thinking regarding the cyber domain move away from a sole obsession with strategic-level decision making and operations as a necessary condition for achieving strategic national and military objectives.

Conclusion: Conceptualizing tactical maneuver options is imperative to ensuring that the United States fully exploits asymmetric advantages in military operations, without the alleged uniqueness of the cyber domain blinding them. Given the realities of the future world assumptions being made, extended ship to objective operations are likely to become commonplace in the future. As a result, the likelihood that a small unit will become isolated, either intentionally in the case of the Asia-Pacific scenario or not, for a period of time in this environment also increases. Maintaining an asymmetric advantage against an enemy will require thoroughly explored doctrinal concepts; tactics, techniques, and procedures (TTPs); and exercise and simulation trials to exploit the cyber domain in the future operating environment.

DISCLAIMER

Table of Contents

Tactical Maneuver in the Cyberspace Domain: Dominating the Enemy

As the Platoon clears the alley, 1stLt Stokely turns the corner and receives sniper fire from an elevated position near a cluster of high-rise apartment buildings. There is already chaos in the street from an unidentified explosion, and 1stLt Stokely can see that there are people clustered in the windows on multiple levels of the building from which the sniper fire is originating. After several moments of attempting unsuccessfully to neutralize the sniper, the unit is able to identify the sniper is located in the corner apartment of the sixth floor of the building. They are not able to call in kinetic support due to the high potential for CIVCAS in the area. The JTAC makes a call for fire – "CYBER01 THIS IS L63, IMMEDIATE SUPPRESSION GRID 211432, BLDG 2, FLOOR 4, SW CORNER AUTHENTICATION IS TANGO UNIFORM OVER." The response is immediate – "THIS IS CYBER01, IMMEDIATE SUPPRESSION, GRID 211432 BUILDING 2, FLOOR 4, SW CORNER, OUT." A moment later, an image materializes on the JTAC's Cyber ROVER screen of a man holding a rifle, his back to the camera device. "L63 THIS IS CYBER 01, TARGET CONFIRMED, REQUEST CONFIRMATION FOR IMMEDIATE SUPPRESSION." "THIS IS L63, CONFIRMED." The screen erupts in a cloud of smoke as the television set near the sniper explodes, sending glass and shrapnel through the room. The explosion disrupts the sniper, allowing the team to move quickly through the street, continuing on to their destination.

Imagine the opportunities if tactical teams were able to plan a raid that integrated not only air and ground support but also on-call fires in the cyber domain. In terms of achieving economy of force, limiting costs, and reducing physical collateral damage, the opportunities are endless. The most important idea introduced in this concept is that of maneuver through and in the cyber domain, exploiting opportunities to seize the initiative by destabilizing the enemy's cognitive decision-making capacities. The ability to conduct tactical maneuver in the cyber domain as part of a combined arms operation is an essential requirement for the United States in future operations to achieve an advantage over its opponents. Achieving operational and tactical maneuver success in the cyber domain requires advances in US military doctrine, tactics, and training far beyond current capacities. The concept of tactical cyber maneuver arises from a forecasting model that appreciates that the Internet of Things (IoT) will become ubiquitous, pervading every aspect of our daily lives over the next 20-40 years. The IoT will penetrate both large urban areas as well as the expanse of rural, virtually connected regions of the world currently considered "unconnected."

In the future operating environment beyond 2035, the large physical footprint that has been an advantage to U.S. military operations in the past becomes a liability, creating a target for our opponents to attack. The places without bases project seeks to capitalize on opportunities to seize the initiative by integrating offensive and defensive multi-domain maneuver in the conduct of military operations by disaggregated forces. Disruptive use of force within and manipulation of the cyber domain in both close and deep battle to create surprise and shock is achievable through tactical and operational cyber maneuver. By virtue of having to operate in a place without a base beyond 2035, military actions in such situations may be not at a time or place of our choosing. U.S. military forces may find that they can control strategic use of force in the cyber domain, but commercial, civilian, and systemic influences will demand that tactical military entities function offensively in this domain. These forces will interact with the Internet of Things (IoT) in the conduct of their duties across the range of military operations (ROMO).

When facing an enemy of technological parity, the military actor is potentially at a disadvantage in the cognitive, physical, and/or virtual dimensions. The global trend towards an increasingly urban, and connected, population accompanies a rise in non-state challenges to traditional concepts of post-Westphalian sovereignty. As a result, conceptual thinking about the cyber domain must move away from a sole obsession with strategic-level decisions toward full integration of cyber into combined arms for tactical and operational maneuver as a necessary condition for achieving national and strategic objectives. Our national defense mechanisms must invest in appropriate tactical capabilities to maneuver in the cyber domain in order to exploit opportunities to seize the initiative and dominate the enemy based upon sound strategic and operational concepts that integrate cyber into multi-domain approaches.

The operational and tactical initiative is empowered by exploiting cyber maneuver to cripple the enemy's cognitive linkages in both close and deep battle. Where time and space can be exploited by tactical and operational maneuver forces to gain strategic advantage, the implications of time and space also present challenges for intelligence, command and control, and logistics. Today's linear, strategically reactive approach to managing the cyber domain cannot overcome the tactical and operational coordination requirements to enable operational and tactical maneuver. An emphasis is needed on doctrinal concepts; tactics, techniques, and procedures (TTPs); and exercise and simulation trials to exploit tactical and operational cyber domain opportunities to achieve effects in the physical, virtual, or physical dimensions through exploitation of the virtual, cognitive, and physical dimensions. Three key attributes of the cyber domain compel the U.S. military to sharpen our integration of cyberspace in combined arms multi-domain maneuver considerations:

1. interactively complex system;
2. intersection of the physical, cognitive, and virtual; and
3. nonlinear, disproportionate strategic effects to be achieved by appropriately integrating tactical maneuver in the cyber domain as part of operational design through all phases of warfare.[1]

As has been forecast for a number of years now, by 2035 military forces will be required to conduct an operation in an urban littoral environment, regardless of specific geographic location. In the "future world" scenario considered as part of this undertaking one may assume the tactical forces operating in this future environment are assuming a grave level of risk. However, military commanders must not assume risk wantonly. Delegating control of cyber domain maneuver to the tactical commander is predicated on the assumption that doing so is a requirement to guarantee strategic and operational success by achieving limited objectives within a specific or limited duration while avoiding unnecessary risk and mitigating collateral damage.

Forecasting the Future Operating Environment

The need to develop a pathway ahead to conduct tactical maneuver in the cyber domain is based on a working group assessment of what the future operating environment might look like (littoral, urban, multiple actors, and inhospitable coastline) and the operating and technological implications of this forecasted future environment. By framing the future environment beyond 2035, and thus beginning with the enemy capabilities and environmental realities, the group hypothesized operational requirements that would emerge given the conditions in that future world scenario.

Within this future context, the need arises for effective tactical and operational maneuver as well as kinetic close air support (CAS) authorities in both an offensive and defensive role at these levels. Deceptive cyber capabilities and exploitation modeled as a call for fire by a small unit leader is a required capability when conducting extended maneuver in depth. These tactical units may rely upon a disaggregated expeditionary advanced base (EAB) infrastructure, including operational and strategic level resources and capabilities. In this environment, the ability to manipulate the cyber domain at the tactical level and effectively prosecute the "Three Block War"[2] through and in this domain will be essential to successful survival of both leave behind forces as well as forces actively engaged in combat operations. Forthcoming manuscripts from other members of this group will focus on multi-domain maneuver in this environment as part of a planned withdrawal as well as on operational maneuver considerations and tactics in a cyber domain denied environment. The requirement to conduct tactical maneuver in the cyber domain is equally applicable in an Asian Pacific context as it is in an African model explored by another sub-group members given the nearly ubiquitous nature of the Internet of Things (IoT) within the cyber domain 20-40 years in the future.

While current doctrine and joint work focus on cyber as a strategic weapon, the realities of future warfare warrant further investigation into the necessary coordination mechanisms to dominate the enemy through full integration of cyber in tactical and operational multi-domain maneuver. Achieving this goal requires that the United States military is not blinded cognitively by cyber's alleged uniqueness. Given the assumptions of the future world being made, extended ship to objective operations have the potential to become commonplace. As a result, the likelihood that a small unit will become isolated, either intentionally in the case of the Asia-Pacific scenario or not, for a period in this environment also increases. Dominating the enemy's cognitive decision making cycles will require thoroughly explored doctrinal concepts; tactics, techniques, and procedures (TTPs); and exercise and simulation trials to exploit cyber maneuver opportunities in the future environment.

The Future Operating Environment: Assumptions, Implications, and the Unknown

Given that current cyber doctrine reserves the use of the cyber domain at the theater and strategic levels of warfare,[3] operational and tactical planning as well as TTPs must adapt to meet the combat needs. Per Joint Publication 3-12 (R), *Cyberspace Operations*, "As authorized by CDRUSSTRATCOM, Commander, United States Cyber Command (CDRUSCYBERCOM) manages day-to-day global CO. Typically, CO require coordination between theater and global operations, creating a dynamic C2 environment." This reflects a common perception of cyber as a tool or capability that needs protection rather than a space in which military and civilian equities exist on a continual and ongoing basis. While to incorrect, the idea fails to capture the implications arising from interactively complex nature of the cyber domain.

While defending US cyber capabilities against exploitation by potential adversaries is a critical priority, realizing a paradigm shift in regards to understanding presence in the cyber domain is required. US military forces will interact both with the cyber domain itself as well as with civilian and governmental networks and infrastructure on a continual basis at a global, regional, and local level. There is no neat line between levels of warfare when attempting to conduct maneuver in this domain given the interconnectedness of the domain with other domains in the virtual, cognitive, and physical dimension. The reach of the cyber domain in the future is unknown today, but it will certainly become even more pervasive in the daily tasks and activities of humankind. The United Kingdom's Ministry of Defense echoes this sentiment in its Strategic Trends Programme document *Future Operating Environment 2035*, "Cyberspace will be ubiquitous by 2035, pervading every aspect of the physical environment to a far higher degree than today."[4]

The ubiquitous nature of the cyber domain and the Internet of Things (IoT) demands that we consider the connectors between cyber and the other domains, physical, virtual, or cognitive. While there is no clear way to describe these connectors, the term hinge seems suitable in that a hinge allows two objects to interact and enables action on a plane of movement. Certainly other terms would be acceptable such as bridge, portal, or link, but the idea is that there are physical, virtual, and/or cognitive hinges between domains, but the cyber domain is interactively complex and creates actions and reactions in a true multi-domain sense. This understanding of the connections between the dimensions of the cyber domain and other domains influences the implications derived from the future world military planning assumptions.

As former Chairman of the Joint Chiefs of Staff Admiral Michael Mullen observed in the introduction to *The National Military Strategy of the United States of America 2011,* "ongoing

shifts in relative power and increasing interconnectedness in the international order indicate a strategic inflection point."[5] An assumption of increasing interconnectedness in interactively complex system of the cyber domain is a key assumption of this approach. Ten military planning assumptions developed by this group arise from the implications of three global trends: 1) continued technological competition from countries such as Russia, China, Israel, and the United Kingdom;[6] 2) the continued expansion and growing influence of non-state actors in the international order; and 3) the growth of the world's population combined with migration towards large population centers in the littorals. These three global trends converge to create the necessary environmental conditions for the ten military planning assumptions to become true.

The ten assumptions of the future scenario are the result of a holistic synthesis of prior work by various different organizations and individuals. These ten factors coalesce to create an environment in which the cyber domain must be fully exploitable in real time by tactical elements during combat operations. In this environment, combat, and potentially non-combat, elements will not be able to remain forward deployed or to rely upon a stationary or predictable advanced base:

1- Technological Parity with a Near-Peer Competitor
2- Presence of Non-State/Non-Aligned actors
3- Presence of Advanced Anti-Access/Area Denial (A2AD) Threat
4- 100 miles of the coast
5- Densely populated urban center
6- Time or place not of our choosing
7- Requiring Ship to Objective Maneuver
8- Limited objectives/duration
9- Requiring both simultaneous and sequential synchronization across all domains
10- A HIGH Likelihood that conventional forces will become isolated

While the above 10 assumptions made in this forecasting exercise presume very specific military considerations for cyber employment, several larger assumptions are made about the strategic environment in which the United States military will operate.

The continued growth of the world's population and a trend towards an increasingly urban world, barring a global cataclysmic disaster, is all but a certainty. The world population will reach 11.2 billion by the year 2100, up from the current population of 7.3 billion. However, global population distribution is not expected to be equal across all countries, with "nine countries: India, Nigeria, Pakistan, Democratic Republic of the Congo, Ethiopia, United Republic of Tanzania, United States of America, Indonesia and Uganda, listed according to the size of their contribution to the total growth."[7] More important to the strategic assumptions in this analysis than the trajectory of population growth is the overall trend towards urbanization combined with growth in areas of the world that are already failing to meet key development indexes and experience internal and interstate strife, particularly in the littorals. As Figure 1 below illustrates, with only a few notable exceptions - particularly on the African continent – the overwhelming majority of growth in population size is along the global littorals.

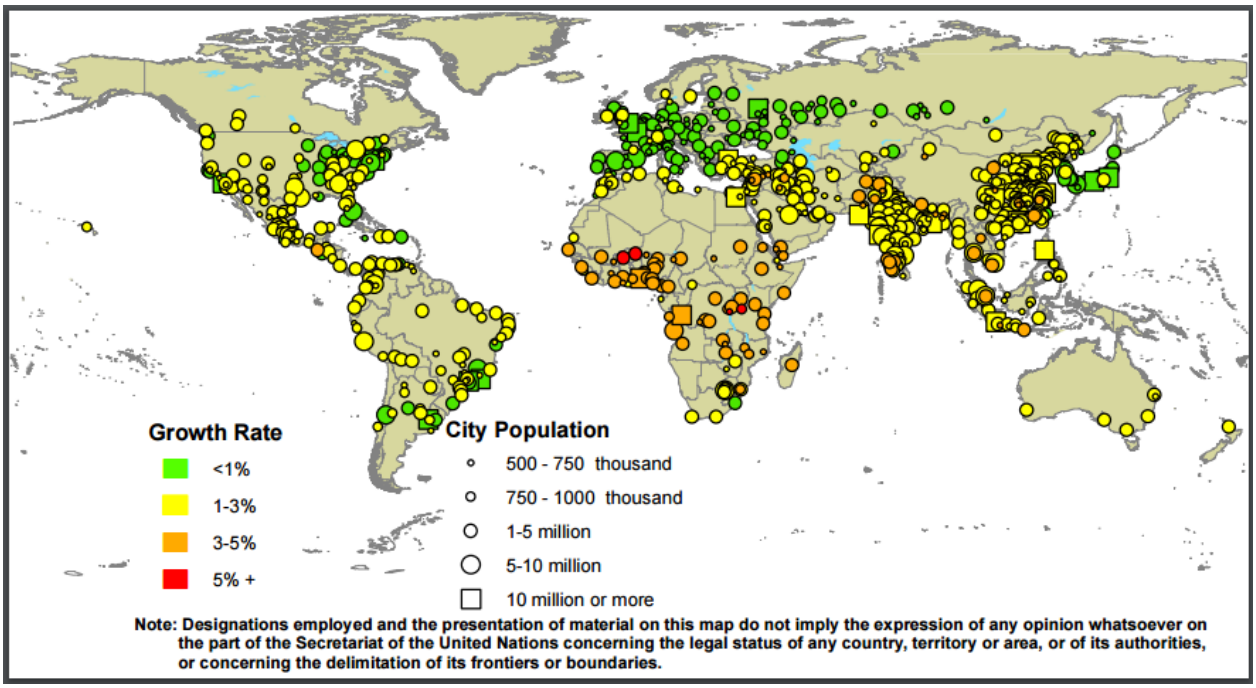

Figure 1: Growth rates of urban agglomerations by size class (2014-2030 C.E.)[8]

The combination of increasingly urban demographics coupled with the inability of a central state to meet the security, economic, and social needs of its population is a likely trigger for the need for an intervention by the United States civilian and military agencies at some point along the range of military operations (ROMO). Where civilian decision makers dictate limited military objectives, the flexibility to operate in a multi-domain urban, littoral environment across all echelons of command is essential to mission success for those military actors.

A key assumption of this future scenario is that operations will be conducted out of time sensitive need rather than at a time and place of America's choosing. As a result, the operational advantages derived from conducting preparatory actions in the cyber domain may be denied to the United States military. In the future world of tomorrow, exploitation of this domain in synchronization with operations in other domains will be essential to achieving desired effects. The observe-orient-decide-action loop of the operational and tactical forces will be compressed,

and information gathering and feedback loops in the cyber domain at the tactical level will become necessary.

Cyber Maneuver – Tying Strategic Considerations to Tactical Actions

Strategic objectives and limitations will continue to shape opertaional and tactical planning for military actors conducting operations across the ROMO. However, military planners at the operational and tactical level cannot afford to be limited to conducting defensive maneuver operations as a result of a narrow focus on strategic implications in the cyber domain. The US is compelled to invest in capabilities, tactics, and training development focused on enabling operational maneuver in a multi-domain combined arms capacity that fully integrates maneuver in the cyber domain as a component of multi-domain maneuver at all levels. Operational level planners and commanders cannot afford to be blinded by the alleged uniqueness of cyber, relegating cyber domain maneuver considerations to a few select specialists working at only the highest classification levels. The operational level commander is the heart and soul of joint planning, translating strategic guidance and objectives to military objectives and guidance to his staff and tactical commanders. Without an appreciation for the manner in which the cognitive, virtual, and physical dimensions of the cyber domain overlay and interact with the other domains in his operating environment, the operational commander and his subordinate elements will not succeed in disrupting the enemy.

Joint Publication 3-0 defines operational art as "the cognitive approach by commanders and staff's – supported by their skill, knowledge, experience, creativity, and judgment– to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means. The foundation of operational art encompasses broad vision; the ability to anticipate; and the skill to plan, prepare, execute, and assess."[9] Much as we seek to

disrupt our enemy's cognitive decision-making through maneuver, the commander relies on his own cognitive abilities and that of his staff. Again, the US military is compelled to thrust the operational and tactical planner and commander into the reality of the situation rather than attempting to simplify or "sterilize" the operating environment by removing cyber domain considerations through a linear, strategically defensive posture.

Moving Beyond the "Strategic Tool": A Review of Current Theory

Practitioners and theorists, both civilian and military alike, address a wide range of considerations with respect to cyber operations. Current discourse tends to center upon a core ideological divide regarding whether cyber is a tool used to achieve a purpose or whether the cyberspace domain is fundamentally a space in which humans maneuver both cognitively and physically. It is important to address these considerations within the broader framework of current theories regarding cyber in the realm of military operations. Within current literature on the cyber domain, three broad characteristics of cyberspace appear to be most influential in pushing discourse towards a narrowly defined focus on strategic effects: the nature of cyber as both cognitive and physical; the low cost to opt-in for multiple types of actors; and the ease of anonymity and attribution.

While much of the conversation today uses the terminology "cyber domain," the scope of current discourse is almost exclusively on the tools utilized in this domain to achieve strategic effect. However, the nature of the cyber domain itself exists in time and space, providing opportunities to exploit time and space to create ambiguity and neutralize the adversary. As put by Jon Lindsay in a 2014 *International Security* article, "Cyberspace – or any technological means of influence – does not escape Clausewitzian logic; it is ruthlessly constrained by it."[10] Cyber presents the opportunity to become the ultimate strategic weapon. For all of the perceived

order that exists within the infrastructure of the cyber domain, the human element of the cyber domain introduces both rational bounds and chaos. While there is an ongoing and robust debate regarding the strategic value of cyber weapons in the diplomatic and strategic realm, the debate more appropriately lies in teasing out theoretical and practical implications regarding the utility of investing in technologies and techniques for maneuver in this domain. Lucas Kello responds to Jon Lindsay's use of Clausewitz and his overall assertion regarding the future of cyber as a strategic coercive weapon with the following: "To the question: Where are all the catastrophic cyberattacks? The easy and obvious response is: Where are all the nuclear attacks?"[11] From this spirited dialogue emerges the central challenge that military theorists are grappling with – are cyber considerations better suited for the realm of strategic warfare? Is cyber destined for the same type of strategic détente witnessed with nuclear weapons in the Cold War between the United States and Russia? Perhaps understanding the cyber domain in terms of what it is not will be most helpful.

The cyber domain is not an elusive, non-physical realm that only operates in and through its own auspices. Cyber action, attacks, espionage, and defense are not new. The cyber domain possesses physical, virtual, and cognitive dimensions. The physical dimension (computer hardware, cell phones, fiber optic cable, etc.) and virtual dimension (data, information, programming languages, applications, etc.) interact in this domain, allowing humans to influence one another in the cognitive dimension. Like other domains, military actors employ both offensive and defensive considerations in the execution of their duties in support of the state's political policy, strategy, and objectives. Likewise, the cyber domain is a civilian domain in that both civilian economic and social enterprises maneuver in this domain. As Jon Lindsay further asserts in his discourse with Lucas Kello, "the physical boundary is very important to strategic

and pragmatic analysis [of cyber]."[12] Joseph S. Nye, Jr. also highlights the physicality of the cyber domain. He draws an important conclusion that the "interconnection of the physical and virtual layers of cyberspace" is crucial to understanding the full weight of cyber war as "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence."[13] Microsoft Corporation, in providing comments to the Department of Commerce regarding the agency's ongoing policy dialogue regarding the Internet of Things (IoT) has some particularly helpful insight – "the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world."[14] It is by exploiting this interaction between the cognitive and physical, between the virtual and the physical that the warfighter creates opportunities to seize the initiative.

Nye and other political scientists are rightfully concerned with the implications for cyber domain warfare on international relations theory. However, military theorists and historians are concerned with the implications for warfare in the cyber domain on the nature and character of warfare.[15] Much focus is given to considerations at the strategic level of planning, particularly from a defensive perspective to counter the threat of a catastrophic attack in the cyber domain, referred to by former Secretary of Defense Leon Panetta as a "cyber-Pearl Harbor."[16] The claim that there is a relative low cost for entry into the cyber domain for states (both strong and weak), non-state actors, and individuals drives much of the hyper-threat literature available today on the cyber domain. Kenneth Knapp and William Boulton's work emphasizes the relatively weak position of the commercial cyber infrastructure as critical vulnerabilities, which could make civilian infrastructure an ideal target for terrorist organizations seeking to undermine the United States government. Likewise, William Lynn III echoes this perception of the vulnerability of the

United States, and he calls for a cyber defense strategy consolidated at the highest levels of military and civilian authority.[17]

This discussion of the relative low cost for actors to buy-in to the cyber domain, and the fear that catastrophic attacks could be executed essentially "at will" by criminals, terrorists, and state actors, rests on another pillar – anonymity and attribution. Adam Liff asserts that the "proliferation of cyberwarfare capabilities for the character and frequency of war… will probably be relatively small."[18] Nye accepts that there are "rhymes" in matters of national defense and warfare that tend to come to the forefront when addressing the applicability of new technologies to combat. However, he also points to the fact that, as in the nuclear age, superpowers will have to confront the "'usability paradox'" with respect to cyber.[19] Can countries use these strategic "weapons" in cyberspace against an adversary without mutually assured destruction?

The crux of the challenge in determining a coherent policy for the future of conducting offensive and defensive operations in the cyber domain centers on the issue of attribution: from who are we defending ourselves, and how do we exploit the cyber domain for our own operational advantage to coerce our would-be foe? Erik Gartzke asserts this paradox between coercion and anonymity reveals the true limitation of the cyber domain in bringing revolutionary change to the character of warfare. It is not sufficient for an entity, no matter how large or small, to have the capability to inflict harm. From Gartzke's viewpoint, cyberwar must "fulfill the existing functions of terrestrial warfare if it is to rival the utility of existing forms of conflict…force can be used to punish… [or] to conquer."[20]

Jason Healey asserts that a key lesson that can be learned from cyber history, if we first accept there is actually a history of cyber, is that "the more strategically significant the cyber conflict, the more similar it is to conflicts on the land, in the air, and on the sea – with one critical exception… governments rarely play a central role in mitigating them."[21] Healey's work concentrates around an analysis of historical incidents of cyber espionage and cyber-attack as well as an assessment of the responses implemented by the United States and others in response to these incidents. He captures the evolution of the cyber domain as a matter of national defense quite succinctly in the following chart, cataloging the evolution of cyber policy in the United States into three categories – realization, takeoff, and militarization:

Figure 2: Phases of Cyber Conflict History[22]

	Realization	Takeoff	Militarization
Start Date	1980s	1998-	2003-
Dynamics	O>D: Attackers have advantage over defenders	O>D: Attackers have advantage over defenders	O>D: Attackers have advantage over defenders
Who Has Capabilities?	US and a few others	US, Russian, and Many	US, Russia, China, and many, many more
Adversaries	Hackers	Hacktivists, Patriot Hackers, Viruses, and Worms	Neo-Hacktivists, Espionage agents, Malware, National Militaries, Spies, and their Proxies, Hactivists
Major Incidents[23]	Morris Worm (1988), Cuckoo's Egg (1989), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Maze ELIGIBILE, RECEIVER, SOLAR SUNRISE, MOONLIGHT MAZE, ALLIED FORCE, Chinese Patriot Hackers	TITAN RAIN, Estonia, Georgia, BUCKSHOT YANKEE
Driving Policy/Policies	Various covering communications security, command and control warfare	PDD-63	HSPD-7/HSPD-23, NSPD/NSPD-54, CNCI
US Defense Organizations	CERT, NSA, and AF Information Warfare Center (1993), and AF 609 IW Squadron (1995)	JTF-CND, JTF-CNO, USSPACE, NSA, CERT	JTF-GNO, USSTRAT, Cyber Command, DHS/NCSD, NSA, and USCERT
US Offensive Organizations	Special Access Programs	JTF-CNO, USSTRAT	JFCC-NW, USSTRAT, US Cyber Command
Coordination Organizations	IOTC, CERT, JTRB	IOTC, NIPC, and ISACs	NCRCG, SCCs, ISACS, USCERT
US Doctrine	Information Warfare	Information Operations	Cyber
US Governance	Some NSC	J-39, NSC, PCIPB	National Security Council

This chart emphasizes that cyber is not a new concept. As a people and a nation, the United States has been addressing the competing priorities and asymmetric nature of actions in the cyber domain for over 30 years. Claims to "newness" are at best a result of the newness of personal experience and exposure to the complexity of the internet and at worst willful misrepresentation of the history of the cyber domain. Certainly, like any interactively complex system, the cyber domain is changing. Often these interactions are difficult to predict, control, and comprehend fully, but the reality of the cyber domain and its influence on human cognitive interaction with the physical and virtual world is not a new phenomenon.

The purpose of a concept of tactical maneuver in the cyber domain is to fulfill a function of terrestrial warfare in a specific manner and for a specific purpose. Operations in the cyber domain should seek to bring a measurable strategic advantage through operational and tactical maneuver in harmony with actions across other domains. Operations in this domain, as in others, can limit the vulnerability of the friendly force while also adhering to just war measures, such as proportionality and non-combatant immunity, and the laws of armed conflict through specific rules of engagement (ROE) for a given operation. The cyber domain should be understood as the "same" as other domains in that these same principles and rules govern human action in this domain just as in the other domains.

In discussing warfare and operations, reflection on traditional warfare theory is also important. The work accomplished in 2013 by the EUCOM JRISE, Detachment 8 Strategy and Plans team provides some useful insight. Figure 3 below condenses salient points from the larger study conducted in support of Red Team Decision Support Analysis by this entity:

Figure 3: Selected Military Theorists - Interpretations for Cyberwar[24]		
Theorist	**Theory and Considerations**	**Implications for Cyber Operational Art**
Aleksander A. Svechin (1878-1938)	"'We must keep in mind that the telegraph, radio, aviation, automobiles – all modern technology – are great devourers of space…' possible to trade space for time."	"Cyberspace offers a first-mover advantage to the offender…CNO should de-stabilize adversaries using multiple means of achieving pre-emptive shock during Phase 1 to gain and maintain the initiative."
Giulio Douhet (1869-1930)	"Target enemy air force to achieve air superiority…. Bomb vital centers to break your adversary's will…"	"CNA against critical infrastructure and key resources (CI/KR), or the credible threat thereof, can compel a political actor to back down in a crisis."
Mikhail Tukhachevsky (1893-1937)	"Use combined arms teams to launch attacks deep into your adversary's rear area… Confuse and destabilize along the entire front and in-depth…"	"Cyber is used in conjunction with a wide array of military and intelligence assets at all Phases… and relies on 'breakthrough forces'… to probe networks and establish possible access points and infrastructure for 'exploitation forces'… a premium on thinking about *simultaneity* and *depth*."
Alfred Thayer Mahan (1840-1914)	"Hold a central position on interior lines… favor the offense… principle of concentration."	"… use CNA to win a decisive battle with concentrated forces against rival networks in order to dominate the GIG (as a LOC)."
Sir Julian Corbett (1854-1922)	"Span of control… sea control may not require a decisive battle…[focus on] 'strategic combinations;' dispersing forces generates flexibility and free movement."	"… there is a span of control [in the cyber domain]; you can never completely dominate cyberspace, but you can exert localized control…Disperse your CNO capabilities and achieve 'strategic combinations."
Ernesto "Che" Guevara (1929-1967)	"use guerilla forces operating from safehavens (foco) to catalyze a national crisis."	"Cyber requires a large investment in a trained cadre who will lay the infrastructure to conduct CNO… persistent surveillance and low-level attacks."
Sun Tzu (544-496 BCE)	"War takes place first and foremost in the human domain (war of perception)… You can position yourself to win without fighting… Be formless…"	"Network configuration is not just material or machine based but includes people and stories…. Sometimes it is better to appear weak and give adversaries a false sense of confidence…"
Kautilya (300 BCE)	"Constant war in the shadows…"	"Positionality: is force posture… in terms of flexibility and the speed with which you can generate attack, defense, and exploitation options. Phase 0 positionality determines your ability to generate effects in Phase I, II, and III."

The above chart reflects the continuity in theory achievable by military tacticians when treating the cyber domain as similar to other domains in the sense of providing opportunities for maneuver in time and space. Without diminishing the relevancy of military principles and theory, the EUCOM JRISE was able to articulate the applicability of such theories to operational art.

Prior to the Platoon's departure for its current mission, they were provided the same pre-mission brief they did each time they were required to conduct a movement from their ship to the particular objective within the city. Since their operational objectives did not include establishing a fixed anchor point on land due to the need to maneuver and conduct raids as a means of introducing ambiguity into the true intentions of the US military force. Their missions were complicated by the presence of a small but increasingly active dissident group that often mistook US forces for the forces of the hostile state that the US and its allies were currently at war with on a larger scale. 1stLt Stokely's platoon and the entire SPMAGTF were providing a supporting effort to the main effort. Their pre-mission brief included a current map of the relevant cyber domain infrastructure and ROEs for requesting defensive and offensive fires. Since unintended civilian collateral damage was a concern, 1stLt Stokely's platoon had been assigned cyber controller – CYBER01 – to provide oversight and de-confliction with higher HQ and above missions. CYBER01 was actually an Air Force Technical Sergeant located within the 707th Intelligence Wing at Fort Meade, MD. Additionally, a combined Army-Marine Corps team at Fort Gordon, GA was monitoring for any bleed over of their missions into the civilian infrastructure and could provide support to neutralize any tool spillage from supporting fire provided by CYBER01. Both CYBER01 and the team at Fort Gordon, GA had a secure link to 1stLt Stokely's radio operator, the BN TOC, and the SPMAGTF HQ through a secure communications network that enabled instantaneous communication. The AWACS loitering in its orbit supporting other primary missions was standing by to provide a redundant communications relay in the event of communications disruption.

Operational Considerations for Tactical Maneuver in Cyberspace

a. Execution Authority

As the supported command for global cyber operations, CDRUSSTRATCOM has the authority to delegate cyberspace operations authority to CDRUSCYBERCOM where appropriate.[25] The March 2012 Joint Staff Transitional Cyberspace Operations Command and Control Concept of Operations (CONOPS) introduced the Joint Cyber Centers (JCC) and the

Joint Cyber Elements (JCE) into the Combatant Command structure. These two organizations are the coordination authority and liaison element between USCYBERCOM and the Combatant Commands. They serve as the representatives and advocates of the Combatant Commander's operational requirements to USCYBERCOM. Additionally, CYBERCOM has introduced an expeditionary CSE (exCSE) capability designed to integrate at the component level to support planning and coordination requirements. This exCSE capability is an important step in realizing integration of operational and tactical considerations of the cyber domain for planners at these levels. However, per JP 3-12(R), "The growing reliance on cyberspace around the globe requires carefully controlling OCO, *requiring national level approval*."[26]

Such a narrow focus of control over offensive action in the cyber domain does not lend itself to proper planning and integration of offensive cyber maneuver into operational campaign planning. The over-emphasis on classification and difficulty in folding cyber specialists into planning currently prevents consideration of the cyber domain as a systemic influence, interacting with the other domains during the course of problem framing. The failure to incorporate cyber in considerations of the environment translates into failing to consider maneuver sequentially or simultaneously actions through air, land, sea, and space in execution. The compounding effect of these failures introduces unnecessary risk to both the military warfighter and to the civilian population. Not taking advantage of opportunities to seize initiative in the physical, virtual, and cognitive dimensions of the cyber domain shapes a military force that is over-reliant on operations in other domains to achieve strategic and operational objectives.

The interactively complex nature of the cyber domain coupled with its potential for strategic consequences creates challenges, but these challenges are surmountable through foresight and planning. Implementation of reach back monitoring and control mechanisms could allow tactical

commanders to have greater advantage over offensive maneuver in cyber space while limiting the unintended consequences of their actions. These mechanisms could allow for a greater and more expansive delegation of authority for tactical action within the cyber domain to support specific named operations and activities for a limited duration and time. By approaching cyber maneuver as a component of multi-domain environmental conditions and maneuver options rather than standalone activity in the planning process, Combatant Commanders and components can be better prepared to delegate the authority to conduct offensive actions to the Joint Force Commander within his area of operation.

During mission execution for an assault, the tactical mission commander would receive the temporary authority to conduct offensive actions in the cyber domain as part of a pre-approved concept of operations (CONOPS). Reach back cells at the JFC, Combatant Command JCC, or at CYBERCOM could provide support in real time to monitor unintended consequences of the mission during execution, providing for corrective measures and "stop-gap" procedures to limit these impacts. The operational and tactical commander must be equipped with the confidence that authorities will not be revoked during mission execution.

b. Maneuver

Tactical maneuver elements must take advantage of virtual, physical, and cognitive connections between the cyber domain and other domains to achieve operational and tactical objectives through multi-domain maneuver. The success of distributed operations in the future will rely on the ability to achieve rapid maneuver in the cyber domain as part of sequential or simultaneous integrated movement across other domains. We must ~~to~~ move away from a static understanding of focusing on tools used to conduct offensive and defensive operations the cyber

domain to a focus on dominating the enemy by seizing the initiative through combined arms multi-domain maneuver that fully integrates manipulation of the cognitive, virtual, and physical dimensions of the cyber domain. According to MCDP-1, Warfighting:

> Success depends not so much on the efficient performance of procedures and techniques, but on understanding the specific characteristics of the enemy system. Maneuver relies on speed and surprise for without either we cannot concentrate strength against enemy weakness. Tempo is itself a weapon—often the most important. Success by maneuver—unlike attrition—is often disproportionate to the effort made. However, for exactly the same reasons, maneuver incompetently applied carries with it a greater chance for catastrophic failure.[27]

At the battalion level and below, tactical forces must effectively induce shock and surprise in the enemy, and the cyber domain may be the most effective means of doing so in a given particular situation. United States military forces are currently integrating robotics, unmanned aerial vehicles, artificial intelligence (AI), and other capabilities today. Combined arms maneuver already integrates the cyber domain throughout the military force, but a real understanding of the interaction, the hinges, between the cyber domain and other domains is limited to very few specialists at this time. The entire force needs to be better educated regarding the interplay between the cyber domain and other domains to bring about a paradigm shift in current concepts of multi-domain maneuver. Clearly, cyber is not a replacement for other forms of maneuver and fire, but it is part of a complete whole in terms of our approach to conducting operations.

Much of the technology exists today within commercial entities to support mapping, overlaying, and exploiting cyber environments. Adapting these technologies for operational military purposes will require a clear picture of maneuver in the cyber domain as both physically and temporally overlaid with human and physical terrain features of interest to military missions. The activities describes to support maneuver will also apply to the fires considerations and will require extensive investment in doctrine and training to understand the logistical and intelligence requirements needed to support these actions. Specifically, logistical considerations will need to

encompass the architectural support and configuration management requirements needed to integrate new and emerging technologies into a distributed network environment. However, the ideas and concepts related to maneuver within the cyber domain must precede investment in technology tools and materiel solutions.

c. Fires

With the proper authorities and C2 structure in place, calls for fire in the cyber domain may resemble those in other domains. Destroying or activating a virtual-physical connector to achieve lethal effects through cyber during a troops in contact (TIC) by what could be called a close cyber support (CSS) mission rather than a close air support (CAS) may or may not have physical effects visible to the naked eye. Tactics will need to meld both electronic warfare (EW) and information operations (IO) with coordination procedures to establish the equivalent of a cyber 9-line.

Fire support could be provided either through a cyber element embedded within a Tactical Operations Center (TOC) or through deep fires support provided through USCYBERCOM or the JCC established at the JFC. In the absence of secure and reliable communications to these reach back elements, the tactical unit of the future must also possess the ability to conduct its own organic fires support within the cyber domain to the greatest extent possible. For the Marine Corps specifically, this may mean refining the key skill requirements of the newly established Assistant to the Squad Leader position or integrating these capabilities with another squad member. The ability to engage in direct tactical cyber fire mission, originating from the team rather than a reach back element such as CYBER 01 described in the prior vignettes, would not

alleviate responsibility for those disaggregated elements supporting that team to monitor the effects of the tactical cyber direct fire in the virtual dimension as previously described.

Cyberspace coordination procedures and rules of engagement (ROE) established in advance are designed to mitigate cyber effects from spilling over and creating unintended consequences outside of the immediate cyber domain environment in which tactical maneuver is taking place. The environment(s) identified as viable for cyber maneuver in advance of the mission may or may not coincide with the specific area of operations (AO) within which the tactical unit is maneuvering physically. However, planners will take into account the physical, virtual, and cognitive dimensions that must be affected to support the tactical maneuver element. Even in a no communications or degraded communications environment, the reach back cells previously identified can monitor for spillover effects outside of the cyber environment, ensuring the JTF Commander and/or component commander is aware of changes in the cyber domain environment.

d. Command and Control

As can be seen from considerations discussed in regards to maneuver and fires, planners and operators will need to develop similar control mechanisms to Airspace Control Mechanisms (ACMs). However, geographic boundaries will not be sufficient given that applications and the network architecture supporting the IoT are not always co-located in the same city, region, or country as the device or program that must be manipulated to support maneuver and fires missions. Command and control of operations that integrate tactical maneuver in the cyber domain is essential in mitigating unintended consequences. Additionally, proper control mechanisms built into the C2 structure should support tactical decision-making and maneuver

within the cyber domain. The current over-arching C2 structure as depicted in Figure 4 below reflects an understanding of the need for control mechanisms in order to limit the strategic consequences of operations in the cyber domain. However, it does not allow for effective operational and tactical maneuver in support of a combined arms campaign.

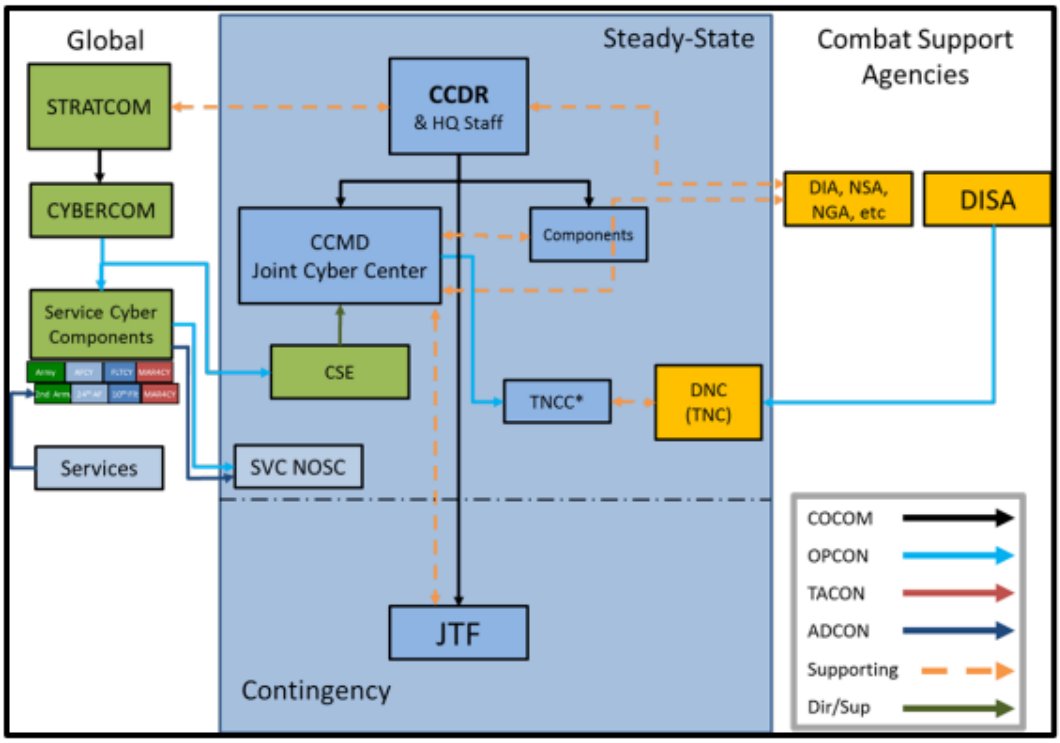

Figure 4: Strategic Cyber Command and Control[28]

Decision makers should examine opportunities to expand authorities to the tactical commander below the JTF level to conduct maneuver in the cyber domain for both offensive and defensive purposes. This expansion should include a careful analysis of the applicability of current Rules of Engagement and the Laws of Armed Conflict to examine applications of force in the cyber domain. Further investigation is warranted into how the military force can expand and logistically support passive and non-traditional mechanisms for monitoring, communication, and coordination in real time to support a more diverse approach in the future to command and control.

e. Just War Considerations

Gregory J. Rattray has posited an interesting idea related to force in the cyber domain that may be worth further consideration for its implications for military ROE. He specifically puts forward the concept of microforce, wherein "the use of nonviolent digital attacks to achieve political objectives must be understood as part of a new form of warfare… At issue here is the amount of energy unleased by a given weapon at the time of attack." [29] Putting aside the discussion of whether digital attacks represent a new form of warfare, understanding actions in the cyber domain as a form of energy or violence is useful to applying the precepts of just war theory. Perhaps the current concept of kinetic vs. non-kinetic force may need to be adapted to understanding force as the act of violence regardless of how discernable the effects of that force may be to the naked eye or sensor. As demonstrated in the opening vignette of this article, rendering effects through tactical maneuver in the cyber domain has the potential to cause unintended collateral damage to non-combatants either directly or because of bleed over of tools intended for military purposes on civilian networks.

Assuming the perspective that the cyber domain should be treated as an environment just like the other domains helps to clarify the cyber domain considerations in relation to *jus in bello*. *Jus in bello* as it applies to the United States military concerns the moral and philosophical western tradition of Just War Theory as well as the international agreements and treaties that comprise International Humanitarian Law. There are five principle criteria applied in the conduct of a just war: distinction, proportionality, military necessity, fair treatment of prisoners of war, and no means *malum in se*.

Tactical Maneuver in the Cyber Domain: Opportunities Arising From its Attributes

This section will elaborate on the considerations for tactical maneuver in the cyber domain, specifically balancing those considerations in light of the attributes of the cyber domain. Specifically, the following attributes of the cyber domain will be addressed – an interactively complex system; intersection of the physical, cognitive, and the virtual through the cyber domain; and nonlinear, disproportionate strategic effects achieved by appropriately integrating maneuver in the cyber domain at the tactical level as part of operational design through all phases of warfare. These considerations are examined through the lens of the principles of war with a particular emphasis not on the specific tools (Distributed Denial of Service [DDoS] attacks, malware, worms, etc.) but on the theory required to operate effectively in this domain at the tactical level.

Integration of tactical maneuver in the cyber domain by fielded forces focuses on achieving one's objective through offensive maneuver. While tactical deception and defense are addressed, this particular concept is primarily offensive in nature. Rather than emphasizing the *threat* of the individual actor and potential disproportionate effects achieved by the lone wolf, this concept seeks to *learn* from the lone wolf to inform tactical maneuver in the cyber domain. These lessons also inform the imperative for restraint in the conduct of tactical offensive operations in the cyber domain precisely because of the potential disproportionate consequences of interactions within this complex system.

a. The cyber domain as an interactively complex system

Military planning is an exercise in problem solving. When presented with a military scenario or challenge, the military planner must design an approach that will result in success based on effective and thorough framing of the problem. Future planners must frame the context of tactical action in all domains, including the interactive networks and configurations of the cyber domain. Traditional military planning assumes that by translating the Commander's guidance and mission to objectives and tactical tasks, the planner is able to maneuver and conduct operations across all domains in a simultaneous or sequential approach with success. However, proper planning requires careful analysis of the multi-faceted nature of the influences of these domains on human perceptions and the environmental conditions across these domains. While Horst W.J. Rittel and Melvin W. Webber conceptualized and described the properties of "wicked" situations in their 1973 paper "Dilemmas in a General Theory of Planning,"[30] military operational often fails to integrate a flexible approach to effectively understanding the dynamic nature of the supposedly "wicked" situations facing military planners. In the words of Rittel and Weber, "planning problems are inherently wicked."[31] Where modern theorists overlook the fact that Rittel and Weber were focused on handling systemic characteristics associated with city planning and infrastructure considerations, their concept of the interaction between the cognitive and physical dimension is particularly useful.

Integration of the cyber domain in tactical military planning appears to threaten the principle of simplicity. The over-dramatization of the domain in current strategic literature and discourse has a tendency to cloud clear thinking on problem solving in this domain. However, while the domain is an interactively complex system, effective techniques for developing an understanding of the multi-faceted connections and layers of the cyberspace domain are available

to planners today. Through disciplined investigation of connections, or hinges, between the virtual, physical, and cognitive dimensions of the cyberspace domain, military planners can hope to achieve opportunities to achieve both simultaneity and depth through the cyber domain in concert with other tactical actions. Keeping a close eye on the greater operational and strategic objectives is essential in all planning; integration of the cyber domain in planning is no exception.

A key component of future success in achieving simplicity in tactical maneuver in the cyber domain will be to move beyond a reliance on materiel solutions and to focus first on ideas and concepts such as presented here to evolve a shared understanding of the cyber domain. While common operating pictures (COPs), CND, and CNA tools will be requirements to conduct tactical maneuver in the cyber domain, a common, comprehensive understanding of the complexity of this domain in military operation is required. Integrating DOTMLPF-P[32] considerations as part of a functional solutions analysis is essential as a follow-on consideration of this initial work. Today's joint force is compelled to focus on baselining common knowledge of the cyber domain as essential to equipping military planners and operators with the necessary background for both understanding the cyber environment and conducting successful tactical maneuver in this environment.

While DoD Information Assurance training has become a standard tool for teaching airmen, soldiers, sailors, and marines how to protect their own activities within the cyber domain, there is no single source, mandatory training that attempts to shape a common vernacular or language for communication across the joint force regarding this domain. While Intermediate Developmental Education (IDE) introduces officers to cyber domain concepts, this training is too little and too late to equip the tactical force for planning required at the junior

officer and junior enlisted level. The Joint Publication 3-12(R), *Cyberspace Operations*, captures some of the current common terms, but it will require future revision to include tactical operations and considerations to support the future tactical force. A concerted effort to peel away the "mystique" of the cyber domain leads directly to clarity in planning and orders writing.

Finally, design should also consider the integration of just war principles in relation to the cyber domain. Myriad policies, legal considerations, and rules of engagement procedures will continue to influence the utilization of certain tactics within the cyber domain. The 1988 release of the Morris Worm by a Cornell University student, Robert Morris, is an example of the potential negative impact deriving from poor planning and risk mitigation. Morris's intent in releasing the worm was to tally the size of the internet at the time. However, the randomization measure Morris installed in the worm to ensure it would be able to succeed in penetrating systems resulted in a level of replication that effectively crashed every computer system it entered. As previously discussed, the utilization of TTPs and control mechanisms must include risk mitigation protocols to help to limit unintended consequences. Specifically, disruption of a particular WiFi or WiMax network in a village or town in order to prevent citizens from tipping local authorities to the location of a maneuver element could also have the unintended consequence of disrupting medical alert systems, home monitoring equipment for hospice patients, or other life-sustaining activities among the civilian population. As civil defense and civilian cyber infrastructures become more reliant on common architecture backbones, tools and TTP development must focus on discriminators and identification protocols for devices and networks in order to limit unintended collateral damage to the greatest extent possible.

Overcoming the perception that analyzing and problem solving within the cyber domain is too complex without extensive and specific subject matter expertise undermines the military

principle of unity of command. Problem solving by the military planning team necessarily involves both diagnosing the problem as well as explaining the challenge clearly and concisely to senior leaders. Conversely, senior leaders must be well versed in the risks, assumptions, and opportunities the interactively complex system that is the cyber domain presents. When a commander makes a determination regarding the objective, he must articulate clearly his desired effects and the implications in all domains. Finally, the commander must have confidence in the risks that the force is assuming in delegating freedom of action to the tactical level. The cyber domain proves to be no exception, but the commander who does not understand the domain will prove to be inherently more risk adverse.

b. Exploiting the intersection of the physical, cognitive, and virtual through the cyber domain

Planning in the future requires that planners visualize the cognitive, physical, and virtual properties of the cyber domain as co-existing and interacting simultaneously with the physical domains of air, land, sea, and space. Effectively framing the problem in military operations will include mapping the hinges previously discussed between the cyber domain and the other domains, identifying opportunities to exploit those bridges, and providing for deliberate mechanisms to take advantage of those bridges for either offensive or defensive purposes.

The case of the Stuxnet worm's ability to cause physical damage to the uranium gas centrifuge tubes at the Natanz nuclear facility in Iran is the clearest example of exploiting a hinge between the virtual and the physical through the cyber domain.[33] Like the Morris Worm, Stuxnet had a singular purpose, but designers scoped Stuxnet to specifications that attempted to limit effects only to those centrifuge tubes used at Natanz. Effective problem framing and

careful identification of the connection between the virtual and the physical dimensions were required to identify the desired means for limiting the expansion of Iranian enrichment programs. This problem framing effort allowed designers to achieve the desired effect in the physical dimension through manipulation in the virtual dimension. Additionally, the worm initially went undetected by the Iranian government and when the mechanical (physical) difficulties began to emerge, the initial assumption was that there was a physical defect or malfunction afoot. Stuxnet thus achieved both a physical and cognitive effect through virtual action in the cyber domain.

While the Stuxnet worm attack was authorized based on a strategic priority, the planning, worm development, and execution required tactical focus, including extensive cyber espionage by a skilled cadre of experts. In conducting the problem framing to determine how to disable the Natanz enrichment efforts, planners necessarily envisioned a path across the virtual hinge in the cyber domain to achieve a physical effect. In this respect, the cognitive interplay with the cyber domain is present in both the attacker and the victim of this attack. In this respect, Stuxnet informs the proper approach to tactical maneuver in the cyber domain from the perspective of economy of force and mass.

The Israelis achieved economy of force in the case of the Stuxnet worm through extensive intelligence preparation of the battlespace across all domains. This example also highlights the hinge between the technical and human considerations of the cyber domain. While the problem of identifying the appropriate hinge is essentially one of scientific method, the intended geopolitical effect and following consequences fit in the larger scheme of those "wicked" problems alluded to by Rittel and Webber. The decision to exploit an opportunity in the cyber domain became a selected option to resolve the Israeli problem precisely because it conformed to a range of "action-prospects" available to the decision makers.[34]

At this point in history, the United States military and policy paradigm prevents delegating maneuver decisions in the cyber domain to the tactical level from entering the realm of action-prospects, focusing decisions in strategic planning. Fielded forces and personnel are acted upon, influenced by, and influence the cyber domain at the tactical level in the virtual, cognitive, and physical dimensions. However, the interaction is more difficult to understand and manage beyond simple cyber security defensive measures to protect cyber networks.

A team properly equipped with a "map" of identified hinge opportunities could maintain the offensive during tactical maneuvers while limiting unintended civilian collateral damage with further refinement of military doctrine, training, and tactics. Even in the least connected countries today, the widespread use of cellular and Wi-Fi technologies (and in the absence of such technology-integrating networks the devices capable of being networked independently) creates opportunities to seize the initiative and exploit tactical advantages. Where it may be unacceptable to use a high tonnage air dropped munition on an apartment building from which a combatant is firing upon a team, it may be possible to see passively into the room from which the shooter is firing through connected devices such as televisions and phones. If the team is able to pinpoint the exact source of the hostile fire, utilizing a hinge to initiate a physical effect by short-circuiting the electricity, overheating a phone battery to create a low yield explosion, or turning on the television as a distraction all become possibilities. The objective of neutralizing the enemy is achieved.

Tactical maneuver in the cyber domain is only possible if embraced as a viable component of combined arms multi-domain maneuver. US military current force posture and technology certainly does not permit this scenario to come to fruition today, but a reorientation in

doctrine and policy will allow for the full realization of DOTmLPF-P solutions to meet these requirements.

c. Nonlinear, disproportionate strategic effects achieved at the tactical level

Joint Publication 3-0, *Joint Operations*, states "Commanders conduct CO [Cyber Operations] to retain freedom of maneuver in cyberspace, accomplish the JFC's objectives, deny freedom of action to enemies, and enable other operational activities."[35] However, as addressed, the majority of military and policy discourse remains focused on strategic cyber or simply focusing effects in the cyber domain based on cyber-centric considerations rather than based on a multi-domain maneuver approach. Limiting activities in the cyber domain to the strategic level of warfare is a mistake as this domain easily lends itself to adaptability across the echelons of military command and operations. While leadership and strategy to task metrics dominate discussions of leadership, training, planning, and kinetic operations in warfare, a consistent trend with respect to the cyber domain is to compartmentalize its application because of the alleged "uniqueness" of the cyber domain. However, all tactical tasks performed on the battlefield should trace back to strategic aims. Tactical and operational cyber maneuver provides the potential to achieve nonlinear, disproportionate strategic effects for military forces.

To understand this vision of tactical cyber maneuver, the phrase "nonlinear, disproportionate strategic effects" should be taken in the proper context of problem solving. As discussed earlier, military planning seeks to solve problems, possessed of both scientific as well as human factors. The purpose of warfare is to crush the enemy's will, denying him the desire or ability to continue to fight. Human will is both expressed and influenced through the cyber domain. While policy makers cannot ignore the importance of strategic control of this medium,

targeting the will of the individual is essentially a matter of tactical maneuver – exploiting his weaknesses while making one's own weakness appear as strength. To do so effectively requires a shift in our conceptualization of the cyber domain. Russia's ability to conduct tactical maneuver in the cyber domain during the 2008 Georgia crisis provides valuable insight into the utility of applying multi-domain maneuver principles that integrate the cyber domain for future military operations.

Though it has been asserted that Russian targeting of Georgian cyber infrastructure as part of its overland maneuver was not conducted a the tactical level, the value of seizing the initiative and achieving economy of force through preparatory cyberspace fires in this operation is clear. The Computer Network Attacks (CNA) conducted on a wide scale against Georgian civilian and governmental cyber infrastructure, though not formally tied to the Russian government, achieved clear military objectives in the "informational and psychological impact on Georgia: it effectively isolated [Georgia] from the outside world."[36] The CNA prevented accurate estimations of the strength and direction of Russian overland movements, preventing communication and queuing between observers, military elements, and senior policy experts. The cyber domain attack was able to prevent an effective initial response to Russian aggression due to ambiguities and a lack of information. Additionally, the attack took advantage of pro-Russian sentiments of a portion of the civilian population, lending confusion to the true nature, intent, and extent of the Russian invasion. As the campaign moved forward, the extent, duration, and scope of Russian maneuver in the cyber domain would change to meet the military needs of the Russian planners.

Rather than focusing on the actions undertaken in the cyber domain, be they denial, deception, espionage, attack, or maneuver, the cyber domain must be first visualized as an

organic environment. Man both influences and is influenced by the cyber domain, much the same as he is the air, land, sea, and space. Individuals pass through the cyber domain in the same way they walk upon the land or sail across the sea. In a future world, the cyber domain is ubiquitous, connecting humans, devices, and even multi-layered networks both passively and actively to one another.

Conclusion

Maneuver in the cyber domain is not a new concept given that we as individuals interact with and manipulate the physical, virtual, and cognitive dimensions of the cyber domain on a daily basis. Tactical maneuver in the cyber domain as part of a combined arms multi-domain approach to military operations is a concept that must be further explored and elucidated in military doctrine, tactics, and doctrine development. Effective education of the force regarding the cyber domain is essential to grooming future planners, operators, and leaders who are able to grapple cognitively with this domain. The future force must be able to visualize the operational and tactical hinges between the cyber domain and the other domains as they conduct problem framing and design campaigns to achieve strategic military and national objectives. The attributes of the cyber domain discussed in the final section directly impact operational and tactical considerations in this domain that have consequences for how the future force is manned, trained, and equipped. A common understanding of the cyber domain as ubiquitous in civilian and military life is the first step for military forces to be prepared for this eventual future.

Bibliography

Internet Policy Task Force and Digital Economy Leadership Team. *Fostering the Internet of Things*. Washington, DC, Department of Commerce, January 2017.

EUCOM JRISE, Detachment 8, Strategy and Plans. "What are Cyber Operational Design Elements? Red Team Decision Support Analysis." Powerpoint briefing for U.S. European Command (EUCOM). Stuttgart, DE: EUCOM HQ, 4 November 2013.

Future Operating Environment 2035. 1st ed. Ministry of Defence. London: Strategic Trends Programme, December 15, 2015.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall 2013): 41-73.

Healey, Jason. "Part 1: A Brief History of US Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Edited by Jason Healey. Washington, DC: CSSA, 2013. 14-87.

Rittel, Horst W. J. and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4 (1973): 155 – 169.

Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, DC: Joint Chiefs of Staff, January 17, 2017.

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

Krulak, Charles C. "The Strategic Corporal: Leadership in the Three Block War." *Marines Magazine* (January 1999). http://www.au.af.mil/au/awc/awcgate /usmc/strategic_corporal.htm.

Liff, Adam. "Cyberware: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *The Journal of Strategic Studies* 35, no. 3 (June 2012): 401-428.

Lindsay, Jon R. and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security* 39, no. 2 (Fall 2014): 181-192.

Lynn III, William J. "Defending A New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.

Lynn III, William J. "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack," *Foreign Affairs* online (September 28, 2011). https://www.foreignaffairs.com /articles/2011-09-28/pentagons-cyberstrategy-one-year-later.

Mullen, Michael. *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*. Washington, DC: Department of Defense, 2011. http://www.defense.gove/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf.

Nye Jr., Joseph S. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly* (Winter 2011): 18-38.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Boston: MIT Press, 2001.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* (Nov-Dec 2011): 63-68.

United Nations Department of Economic and Social Affairs/Population Division. *World Population Prospects: The 2014 Revision*. New York, NY: United Nations, 2014.

United Nations Department of Economic and Social Affairs/Population Division. *World Population Prospects: The 2015 Revision, Key Findings, and Advanced Tables*. New York, NY: United Nations, 2015.

United States Marine Corps. *Warfighting*. MCDP-1. Washington,DC: Headquarters Department of the Marine Corps, 20 June 1997.

End Notes

[1] The term phase specifically refers to the phases of an operational plan as articulated in Joint Publication 3-0. For further reading, see Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: Joint Chiefs of Staff, January 17, 2017), V-6.

[2] The term 'three block war' was first used by Marine General Charles C. Krulak in 1999 to highlight the leadership paradigm facing marines operating in the tactical, urban environment in a highly volatile and changing situation. While the term has fallen out of favor, the image of the tactical unit maneuvering in the urban environment that this conjures is of value to the overall objectives of this paper. Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999, http://www.au.af.mil/au/awc/awcgate /usmc/strategic_corporal.htm.

[3] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12R (Washington, DC: Joint Chiefs of Staff, February 5, 2013), x.

[4] *Future Operating Environment 2035*, 1st ed., Ministry of Defence (London: Strategic Trends Programme, December 15, 2015), 28

[5] Michael Mullen, chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership* (Washington, DC: DOD, 2011), 1, http://www.defense.gove/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf.

[6] Though these countries are not necessarily opponents in the military sense, they are countries that are capable of contesting technological superiority in future possible scenarios. The relative status of an ally or partner in the traditional national security sense is not a consideration in the fields of science, technology, and mathematics.

[7] United Nations Department of Economic and Social Affairs/Population Division, *World Population Prospects: The 2015 Revision, Key Findings, and Advanced Tables* (New York, NY: United Nations, 2015), 4.

[8] United Nations Department of Economic and Social Affairs/Population Division, *World Population Prospects: The 2014 Revision* (New York, NY: United Nations, 2014), https://esa.un.org/unpd/wup/Maps/CityGrowth/CityGrowth.aspx.
[9] JCS, *Joint Operations*, xii.
[10] Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (Fall 2014): 185.
[11] Ibid., 189.
[12] Ibid., 186.
[13] Joseph S. Nye, Jr, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly* (Winter 2011): 20-21.
[14] Microsoft Corporation Comment, *Fostering the Internet of Things*, Department of Commerce Internet Policy Task Force and Digital Economy Leadership Team (Washington, DC, Department of Commerce, January 2017), 5.
[15] Neither of these specific ongoing theoretical discussions and investigations are the subject of this work. However, for insightful discussion on the topic of cyber warfare, see: Jon Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014/2015): 7-47; Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace, 1986-2012 (Vienna, VA: Cyber Conflict Studies Association, 2013); Erik Gratzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316-348; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41-73; Joseph S. Nye, Jr, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly* 5, no.3 (Winter 2011): 18-38; Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (Fall 2014): 181-192; Benjamin M. Jensen, Ryan C. Maness, and Brandon Maness, "Cyber Victory: The Efficacy of Cyber Coercion" (unpublished manuscript, January 2017), Microsoft Word file; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Journal of Strategic Studies 35, no. 3 (2012): 401-428; Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 81-99.
[16] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack," *New York Times*, October 11, 2012.
[17] William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack," *Foreign Affairs* (September 28, 2011), http://foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later; William J. Lynn III, "Defending A New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108. See also the work and comments of Shane Courville and Wesley K. Clark and Peter L. Levin regarding the need for cyber to become a national security item of concern, particularly due to a lack of defensive capability on the part of the United States: Shane P. Courville, "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future" (Maxwell, AL: Center for Strategy and Technology, Air War College, 2007), http://www.au.af.mil/au/awc/awcgate/cst/csat63.pdf; Wesley K. Clark and Peter L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs* 88, no. 6 (November/December 2009): 2-10.
[18] Adam Liff, "Cyberware: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *The Journal of Strategic Studies* 35, no. 3 (June 2012): 401.
[19] Nye, 24.
[20] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 49 and 54.
[21] Jason Healey, "Part 1: A Brief History of US Cyber Conflict," in *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, ed. by Jason Healey (Washington, DC: CSSA, 2013), 85.
[22] This table is taken directly from the work by Jason Healy referenced in Endnote 19 without modification. Jason Healey, 18.
[23] These "major incidents" mark high profile events that have been either widely publicized or that the author, Jason Healey, viewed as particularly monumental in shaping U.S. cyber policy or shaping general world views regarding cyberspace.

[24] Italicized text is original to the source material. EUCOM JRISE, Detachment 8, Strategy and Plans, "What are Cyber Operational Design Elements? Red Team Decision Support Analysis," powerpoint briefing for U.S. European Command (EUCOM) (Stuttgart, DE: EUCOM HQ, 4 November 2013).
[25] JCS, JP 3-12(R), II-7.
[26] Ibid. Italics are author's emphasis and not that of the original source.

[27] United States Marine Corps, *Warfighting*, MCDP-1 (Washington, DC: Headquarters Department of the Marine Corps, 20 June 1997), 38.
[28] Bradley A. Reuter, "Cyberspace Integration within the Air Operations Center" (Air Force Institute of Technology: Wright Patterson AFB, OH: May 2013), file:///C:/Users/ofda%20user/Downloads/ADA582763%20(1).pdf, 8.
[29] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Boston: MIT Press, 2001), 20.
[30] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4 (1973): 155 – 169. http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf .
[31] Rittel and Webber, 160.
[32] DOTmLPF-P: Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities, Policy.
[33] For a detailed case study on the Stuxnet worm, see Chris Morton, "Stuxnet, Flame, and Duqu – The OLYMPIC GAMES," in *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, ed. by Jason Healey (Washington, DC: CSSA, 2013), 212-231.
[34] Rittel and Webber, 166.
[35] Joint Chiefs of Staff, Joint Operations, JP 3-0 (Washington, DC: Joint Chiefs of Staff, January 17, 2017), III-9.
[36] Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* (Nov-Dec 2011), 63.