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
Hiding in Plain Site: Cyberspace Denial Enabling Small Team Operations in Places Without Bases

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Unger, Zachary D., 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 will directly address the current and future challenges that United States forces face with the growing ability of enemy forces to maneuver within the domain of cyberspace. Traditional instruments of United States National Security, military small team operations, face an enemy that can maneuver around them and highlight their presence essentially negating the asymmetric advantage the United States has historically possessed in unconventional warfare through small team operations. Unless the United States military begins to employ the same willingness to operate within, or deny, this domain, the enemy will close on American military advantage until ultimately, achieving parity or advantage.

15. SUBJECT TERMS
small team operations; cyberspace; cyber domain; denial; blockade; military theory; planning; offensive; defensive; doctrine; EW;

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	39	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

Hiding in Plain Site: Cyberspace Denial Enabling Small Team Operations in Places Without Bases

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

Major Zachary D. Unger, USAF

AY 16-17

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____

Oral Defense Committee Member: _____
Approved: ✓
Date: 5 MAY 17

Executive Summary

Title: *Hiding in Plain Site*: Cyber Denial Enabling Operations in Places Without Bases

Author: Major Zachary D. Unger, USAF

Thesis: This thesis will directly address the current and future challenges that United States forces face with the growing ability of enemy forces to maneuver within the domain of cyberspace. Traditional instruments of United States National Security, military small team operations, face an enemy that can maneuver around them and highlight their presence essentially negating the asymmetric advantage the United States has historically possessed in unconventional warfare through small team operations. Unless the United States military begins to employ the same willingness to operate within, or deny, this domain, the enemy will continue to close on American military advantage until ultimately, achieving parity or advantage themselves. This paper will highlight a forecast of the future world, assumptions and threats, methods to operate within the cyber domain to ensure American military advantage.

Discussion: The future operating environment will likely include instances of United States forces operating in places without bases. With the growing ability of the nation's enemies to close the technology gap the United States currently enjoys, as well as the future of United States military superiority, it is quite possible that operations in the future will be in anti-access and area denied (A2/AD) regions where no US base exists or during the US being forced from an existing base. Further difficulties will be presented[1] given that future growth trends lean towards 70% of the world's population moving into the urban littoral regions of the world.[2] While new and creative means of diplomatic engagement in the international arena will most certainly be needed, different avenues of military operations and norms will also be needed. Invariably, the growing domain of cyberspace will further complicate all the above-mentioned considerations. As cyberspace comes into the forefront as a means for actors, both state and non-state, to wage battle, the United States will have no choice but to treat and maneuver within cyberspace as if it were any other domain, such as air, land, space, and sea.[3] Cyber denial, cyber blockades, cyber exclusion zones, and cyber dead zones will be a provocative yet necessary means of waging an offensive defense to ensure the United States is still able to achieve its objectives while protecting its forces from technologically advanced enemies. By eliminating all use of cyberspace and specific EW functions within an area of operation, forces will regain an advantage in initiative while preventing both enemy and neutral civilian forces from maneuvering in cyberspace around them. With a state of degraded equilibrium of technology within the operating area, United States forces will maintain small, highly maneuverable forces operating through operational maneuver from the sea or advanced expeditionary operations within a cyberspace dead zone. This maneuver will induce a level of chaos that will make their presence in plain sight go unseen, or at a minimum, create a better chance of being unseen.

Conclusion: Embracing cyberspace as a domain in which denial operations can be waged is paramount for United States military forces if military advantage is to be maintained. Denial operations within the cyberspace domain will ensure small teams can continue to operate in plain sight without their digital signature highlighting them while simultaneously preventing enemy capability to achieve rapid mobilization and maneuver around them within the domain.

DISCLAIMER

Table of Contents

Page

Introduction

The future operating environment will likely include instances of United States forces operating in places without bases. With the growing ability of the nation's enemies to close the technology gap the United States currently enjoys, as well as the future of United States military superiority, it is quite possible that operations in the future will be in anti-access and area denied (A2/AD) regions where no US base exists or in the course of the US being forced from an existing base. Further difficulties will be presented[4] given that future growth trends lean towards 70% of the world's population moving into the urban littoral regions of the world.[5] While new and creative means of diplomatic engagement in the international arena will most certainly be needed, different avenues of military operations and norms will also be needed. Invariably, the growing domain of cyberspace will further complicate all the above-mentioned considerations. As cyberspace comes into the forefront as a means for actors, both state and non-state, to wage battle, the United States will have no choice but to treat and maneuver within cyberspace as if it were any other domain, such as air, land, space, and sea.[6] Cyber denial, cyber blockades, cyber exclusion zones, and cyber dead zones will be a provocative yet necessary means of waging an offensive defense to ensure the United States is still able to achieve its objectives while protecting its forces from technologically advanced enemies. By eliminating all use of cyberspace and specific EW functions within an area of operation, forces will regain an advantage in initiative while preventing both enemy and neutral civilian forces from maneuvering in cyberspace around them. With a state of degraded equilibrium of technology within the operating area, United States forces will maintain small, highly maneuverable forces operating through operational maneuver from the sea or advanced expeditionary operations

within a cyberspace dead zone. This maneuver will induce a level of chaos that will make their presence in plain sight go unseen, or at a minimum, create a better chance of being unseen.

OSU 2016: A Contemporary Example of Social Networking Technology as a Savior, and Future Threat

"Buckeye alert: Active Shooter on campus. Run, Hide, Fight. Watts Hall. 19th and College."[7] In near real time Ohio State University successfully collected data from on campus individuals witnessing the beginnings of a threat and sent alerts to its campus body via social media outlets such as twitter and Facebook. Far from a normal warning siren, the campus was locked down near instantaneously with multiple updates from unsuspecting sensors -- the student body and faculty. Flurries of tweets and other social network posting would alert both students and first responders to the current or possible locations of the perpetrator. Like a modern-day tornado siren against on campus shooters, the alert network allowed individuals on campus the critical opportunity to flee, barricade themselves, and provide initial routing to law enforcement. Ultimately, the scenario would end much quicker and with less bloodshed than the Virginia Tech campus shooting in 2009, which resulted in the slaughter of 30 individuals.

The case of the Ohio State University attack in 2016, history also serves as a warning to United States forces operating against a similarly interconnected future population. In the case of operating forces, this incident predicts the potential consequences of an entire population digitally maneuvering around them via every device tied into cyberspace, ultimately ending in defeat. Noting warning signs such as Ohio State University in 2016, other contemporary examples also present caution, specifically in the following examples of potentially hostile government forces harnessing cyberspace and social media as a means of operations.

Examples of Government, Militaries, and reporting agencies using social media for operations	
Georgia/Russian War 2008	Georgian civilian social networking photographs and updates provided early proof of Russian forces in country
Libya, 2011	Protesters' social media coordination tracked and targeted with text messages during protests
Sochi Olympics, Russia 2014	Broad based monitoring of all internet traffic using key words to monitor for disruptions or attacks at the 2014 Sochi Olympics
Crimea, 2015	Russian troops identified and reported via social media posts
Turkey Coup Attempt 2016	During attempted coup, government officials monitored social networking sites real-time for developments
Ohio State Attack 2016	Police, students, and administrators communicated actions, precautions, and location of possible attacker
Ukraine, 2016	Social media used to track and report Russian troop movements
United States, 2017	Police use of social media to track violent counter-protests
Figure 1	

Whereas the above historical anecdote demonstrates how technology has changed attacks in the US, the above examples within figure 1.0 also demonstrate how they have been militarized. As technology continues to advance and the domain of cyberspace opens for increased maneuver, United States forces must look to these historical examples and more as a call to enter and expand into the domain of cyberspace. The examples in figure 1 examples demonstrate our adversaries already are.

Problem Statement: Assumptions, their risks, and how they affect United States Non-Traditional Small Team Forces

Inherent risks often surround non-traditional small team operations. This risk is multiplied in in places without bases. Often, these teams are operating outnumbered in hostile environments far away from immediate support, save airborne support. These risks can often be mitigated by advanced technologies that allow for reinforcements, quick reaction teams, close air support, and weapons technology superiority. Additionally, in the current era, most United States forces find themselves operating in the vast openness of Afghanistan, Africa, and less populated Middle East areas. These environments provide for ease of unidentified movement and make them safe from the threat of rapid enemy mobilization as seen in Operation Gothic Serpent when a large Somali force was able to rapidly overwhelm a smaller United States team. However, in a future where the enemy possesses technological parity within an established littoral urban center, the safety of technological superiority disappears. If anything, technology provides a more robust signature to highlight location, report movement, and even identify the intent of friendly forces.

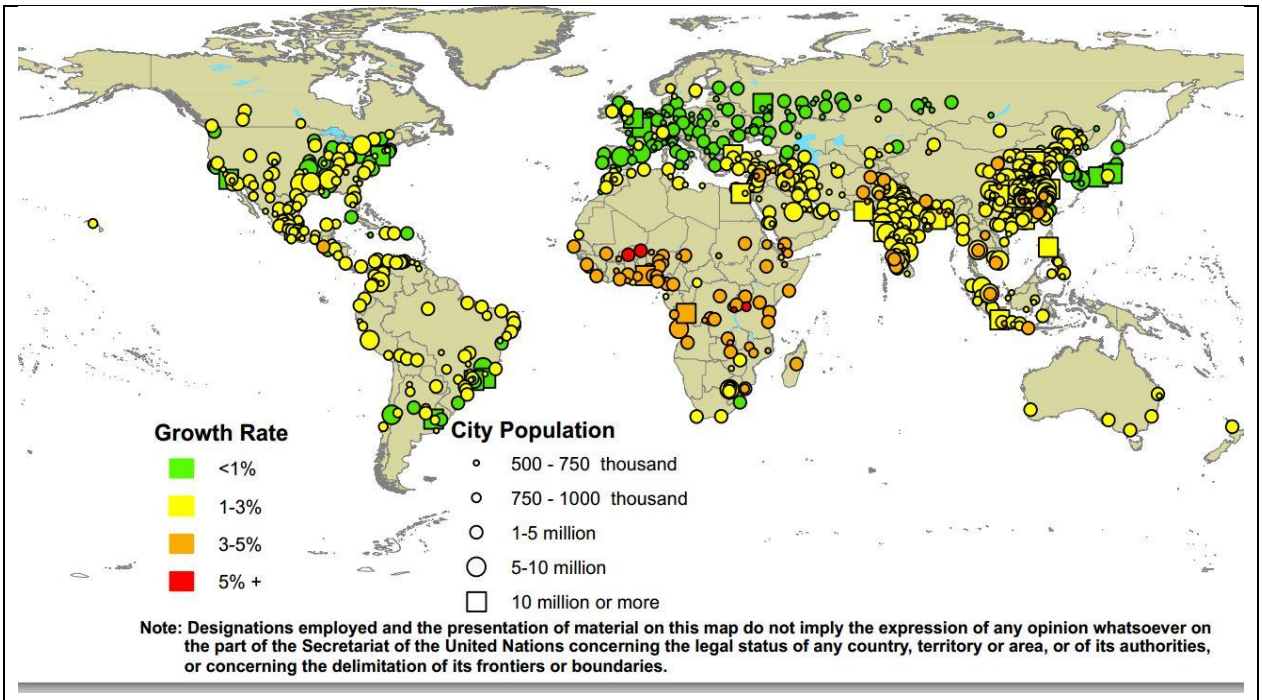


Figure 2. United Nations Growth Map[8]

Technological parity, which is quite possible by 2030, would allow an enemy to use a small team's electronic signatures against them, stripping away continuous overhead support, communications, and, most dangerously, reinforcement. The following short scenario demonstrates the danger in how a current tactical operation would fall victim to the future assumptions of technological parity and operations within the forecasted large scale urban littoral population center.

A flight of CV-22s call sign Nightmare 21/22 proceeds from its base of operations overhead Mosul on the Mediterranean. The 32-man team inside plans to interdict a target inside the large scale urban population center that has been, until recently, quiet all evening. On approach the pilots notice increasingly activity on the crowded streets below them. As Nightmare flight begins to offload the team, enemy forces, already alerted to the general area of the landing via exploitation of the aircraft and team's electronic signatures, begin to mass and fire upon the

United States forces. The team scatters because of the ambush. As each member winds through the population center, the enemy continues to electronically find and fix each individual, identifying, and anticipating their movements through radio communications, blue force trackers, wireless devices, and the endless number of unseen passive sensors presented by the internet of things. Each electronic device a member walks by, every internet router, every cell phone camera or appliance capable of wireless technology, highlights the unsuspecting victim. At an increasing rate, friendly personnel are captured. Those that manage to escape the drag net are eventually tracked through social media reports from every day citizens and passive collection until each member is hunted down, imprisoned, or killed via PGM. No quick reaction force ever is mobilized for reinforcement as the entire area is now a hostile area, and the enemy has amassed.

Although this scenario paints a bleak and deadly result of operating in a place without a base against an enemy of technological parity inside a littoral urban center, it is all too likely that the result would occur if the operation inside that environment took place under today's tactics and EW/cyber employment doctrine. The scenario itself is an example of the future confluence of growing trends towards technological parity and large scale urban littoral city centers. Such a future environment would nullify the tactics that United States military forces take as a given (such as technological superior equipment usage) for success in the current operating environments.

Assumptions of Problems and Potential Solutions

Places without bases pose a problem in that they often limit our ability to seize the initiative, exercise the full range of military operations (ROMO), and often deprive our forces of "home field advantage." Furthermore, with the advancement of Anti-Access Area-Denial

(A2AD), current and future operations face an increasingly uncertain ability to establish lodgment within the borders of an area of operation. By operating in a place without a base United States forces could find themselves in a situation where their actions are reactionary and not at a time or place of their choosing. This will place them these forces at an asymmetric and/or technological disadvantage. With the opportunity to reach across international borders, cyberspace presents an opportunity for military operations to maintain the initiative, given the future operating environment will likely see challenges for military operations based upon the advancement of technology and the increased usage of the cyberspace domain.

Places without bases provides an Advanced Program Studies (ASP) group-level lens that poses what the future operating environment might look like (littoral, urban, multiple actors, inhospitable coastline) and the operating and technological implications. By framing what the environment looks like and beginning with the enemy capabilities in mind, the ASP group hypothesized how to exist and operate within that future environment. At this stage the environment is conceptualized as containing the following assumptions central to the problem of future operations.

1- Technological Parity
2- Presence of Non-State/Non-Aligned actors
3- Not at a time or place not of our choosing
4- Within 100 miles of coastline
5- Containing a large population center
6- Denied
7- Requiring OMFTS/AEBO/Ship to Objective maneuver
8- Limited in objectives/duration
9- Requiring both simultaneous and sequential synchronization across all domains
10- Presenting a high likelihood that conventional forces will become isolated

Based off these assumptions and forecast, four future forecast four worlds were modeled for consideration of potential operating considerations. Further explanation of the four models can be found in Appendix 1.

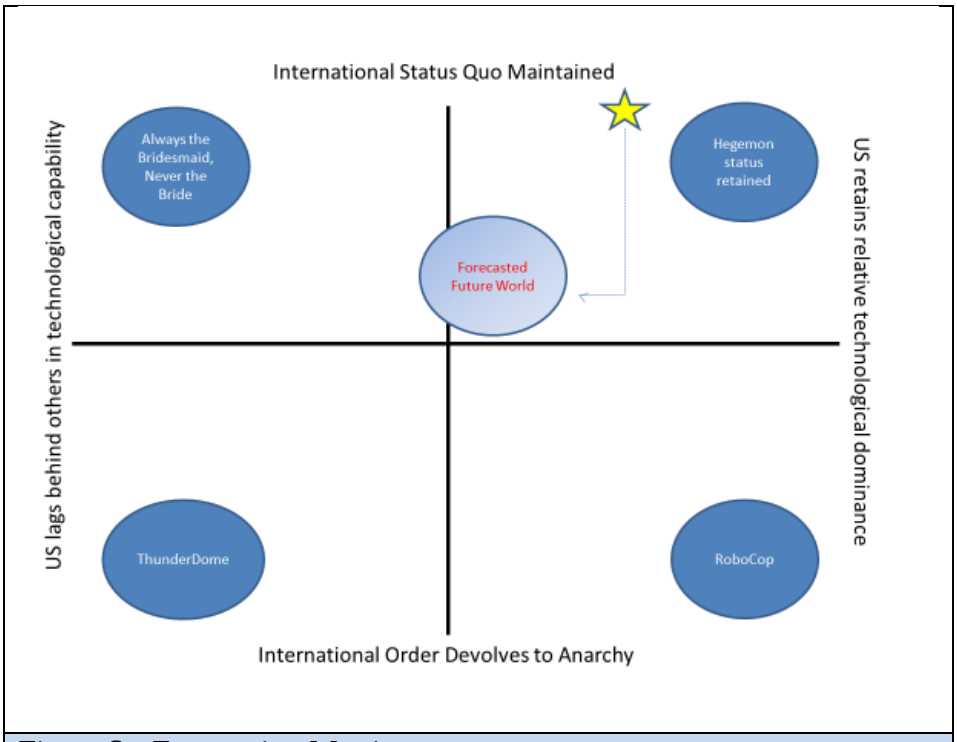


Figure 3 - Forecasting Matrix

Within the group there arose two subtopics of *tactical cyber and electronic warfare in places without bases*; one focused on offensive and defensive cyber capabilities and exploitation modeled as a tactical cyber call for fire, the other on the creation and operation within a camouflaged/denied cyber and electronic warfare "dead zone corridor." Specifically, the creation of a model of warfighting within a camouflaged dead zone provides a new way to exercise maneuver warfare with unconventional and nontraditional warfare in the future operating environment conducted through operational maneuver from the sea (OMFTS) and advanced expeditionary base operations (AEBO). By eliminating enemy cyber and EW capabilities as potential threats through creation of a dead zone, small, constantly maneuvering, highly mobile raiding forces can conduct unconventional warfare (UW) and Nontraditional operations.[9] The two concepts of the dead zone as well as tactical cyber calls for fire will be complementary and

interconnected to each other, most likely if one concept fails, the other will need to be implemented almost immediately.

Forecast Assumptions

Operating in a place without a bases model, the ten assumptions listed in figure 1.0 enable problem framing based on forecasted factors.

Ten Operating Assumptions of Future Operations in Places Without Bases
1- Technological Parity with a Near-Peer or Non-State Competitor 2- Presence of Non-State/Non-Aligned actors 3- Not at a time or place of our choosing 4- Within 100 miles of the coast 5- Containing a densely populated urban center 6- Presence of Traditional Anti-Access/Area Denial (A2AD) Threat 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
Figure 4

Although each of these assumptions are sound with respect to the forecasting provided within this analysis as well as in the Future Operating Environment, [10] there exists a distinct possibility they could be falsified or rendered untrue. Specifically, assumption one and eight could be assumed to be true while simultaneously being manipulated unknowingly by the enemy.

For this analysis, they will be assumed to be present; however, the following paragraphs will discuss how they could be proven false.

Assumption one states that the enemy the United States will operate against in the future operating environment will have technological parity. Should no technological or enemy capability parity exist, it is most likely the United States would have or be in the process of establishing a large base of operations (assuming no presence of A2AD or PGM environment). However, the situation that the United States does not/cannot have a base suggests that red force technology constrains it. Although the assumption of technological party could be true, it also could be influenced by red force psychological operations or military deception. As the Allied forces demonstrated in World War II with their use of inflatable military weaponry, enemy forces could use the same concept to create the illusion that a technological parity or A2/AD threat is present when it in fact is not and the enemy is less capable than assessed.[11]

Assumption eight poses another idea that although the United States can assume it or plan for it to be true, it could in fact, be proven to be false. Should operations occur during for a limited period or for non-enduring objectives, tactical execution would be used in a manner indicative of short term use. However, as evidenced in Operation Iraqi Freedom, the United States has demonstrated before that with a change in what defines success, could evolve non-enduring operations into open ended, long-term armed conflicts. The possibility of this assumption is more likely to be hazardous to tactical use of future cyber and EW operations. The continued tactical use would be hazardous as it would provide the enemy more opportunities to analyze and exploit cyber and EW tactics used and find a way to operate within their confines or turn them against friendly forces.

How to Operate the Future: Tactical Cyber and Electronic Warfare Enabling Non-Traditional and Unconventional Small Team Operations in Places Without Bases

Warfare is waged in different domains, land, air, sea, space, and in the current era, cyberspace. To fully understand the implications, advantages, disadvantages, and maneuver opportunities when conducting operations against the enemy, it is imperative military planners integrate operations in the cyber domain in training and planning activities. Failure to do so provides the enemy free range of movement in a domain against United States forces.[12] In the future operating environment in places without bases, the enemy could be considered to already have a distinct advantage against the environmentally driven small team forces operating without large infrastructural base support. Granting the enemy an additional domain to operate in against overmatched small teams makes already difficult odds of success further limited. To limit the advantages posed by an enemy utilizing the cyber domain in a future operating environment, US forces must render the cyberspace domain useless. Furthermore, removing the millions of nodes the enemy could use against United States forces, keeps the battlefield more evenly matched and benefits the initiative should the United States take it. The following paragraphs will discuss the requirements for successful dead zone operations, including considerations, proposed team constructs, and movement and retrograde considerations. Before concluding, a final portion of this section will discuss training and preparation for future operations within cyber dead zones.

Pre-Op and Force Ingress

In the time, immediately before the force prepares to ingress to the target area, the desired cyber affects must be achieved - cyberspace blockade of the area of operations, creation of a corridor for the ingress route and target area of operations through EW jamming, and cyber

denial of critical infrastructure and key resources (CI/KR).[13] These three actions will be timed sequentially so that they are implemented immediately before the force moves in to the area of operation. These actions are meant to achieve the effect of inducing a sense of chaos within the local populace, while simultaneously inducing confusion on enemy military and/or paramilitary forces within the area of operations. The induced panic and ensuing enemy force confusion will create uncertainty regarding friendly force presence, infill, and intentions.[14] Within this state of chaos, and supplemented by the EW jamming corridor, friendly forces will infiltrate free of detection, seizing the initiative and achieving surprise.[15] Whether performed by operational maneuver from the sea or from an advanced expeditionary base of operations, the corridor into the dead zone will create a geographic area in which the possible observed movement of the forces will not be detectable. Ideally, enemy forces and any visual observations will be unable to report activity via voice communications or cyberspace means.

Actions On

Once infilled to the area of operations, forces must maintain a disaggregated and highly mobile posture. Such movements will ensure forces avoid being fixed, and it will ensure they never remain static long enough to establish a pattern of life or be identified.[16] Whether simply moving to a single objective or conducting operations over a matter of days, disaggregated teams maintaining a highly mobile posture will create a target that is difficult to separate from the chaotic multitudes surrounding them. Forces will be prepared to operate without any external communications from the team back to headquarters. Additionally, without traditional communication measures, crews must be prepared to use no-call procedures for support, exemplified by a no-communications call for fire between ground parties and a fixed wing

airborne fires platform. If able, overhead platforms will consist of aircraft suited to operate devoid GPS, datalinks, and radio communications that the dead zone bubble will establish.

Sensors and weapons employed will be specifically weaponeer for operations free of cyberspace, GPS, or radio inputs. Legacy platforms not requiring data linked inputs as well as future aircraft with airborne laser technology provide good choices for support platforms that can operate devoid of the data that will be denied within the dead zone. Forces will use a series of checkpoints based upon time and location for events such as tactical re-supply, emergency exfil, CASEVAC, and other contingency operations. Ultimately, forces will use a final checkpoint/extract point concept for retrograde.

Retrograde

Once forces reach the pre-determined exfiltration location, they will retrograde via the retrograde vehicles or other-pre-determined egress options. The dead zone and transit corridor will be maintained until back out to the sea base or advanced expeditionary base of operations. Once outside of hostile territory, both the corridor and the dead zone will be removed. Removing the corridor and dead zone immediately and simultaneously will limit the negative effects upon the civilian population as well as deny enemy opportunities to analyze and exploit the cyber effects experienced. Post operations reflection will be utilized to the maximum extent possible. Active monitoring cyberspace and enemy voice traffic communications is required to determine whether counteractions May be forthcoming from the enemy force.

The above model is but one example of how to operate using a dead zone corridor. The overall simplicity is only possible through a combination of manning, training, and equipping a force comfortable in their ability to operate in a degraded and congested environment. However,

simplicity is only possible if the required degraded environment effects are created. A breakdown of either one of these facets would most likely result in mission failure. Manning, training, and equipping, as well as dead zone creation considerations, will be discussed in the following paragraphs.

Identification or re-designation of an already fielded force or creation of a new force specifically trained to degraded operations is ideal for operating in cyber dead zones in the construct of places without bases. Training the force to operate devoid of any cyberspace capability as a norm should drive all training functions. Strong survival, evasion, resistance, and escape skills (SERE) training would be a required baseline. Additionally, the addition of one position/billet per team, trained in cyberspace operations would provide a real-time expert to monitor the efficacy of the cyber dead zone and any remaining evidence of cyber/EW activity should contingencies arise. Additionally, a baseline level of understanding should be possessed by other team members (current example would be a JTAC billet but other members on the team no how to perform emergency close air support). Given the need to be small and highly maneuverable, teams should be sourced from units no larger than an Army Ranger Battalion, as an example. Although numerous teams can be used in a disaggregated manner, as suggested by Marine Corps Operating Concept 2025, they should remain dispersed and highly mobile to elude identification, fixing, and other actions within the enemy targeting cycle.[17]

To operate within a cyber dead zone requires simplistic, and possibly, dated equipment. Equipment should include only weapons and devices designed to operate devoid of cyberspace infrastructure and capability. The one exception to this would be specialized emergency equipment to use if compromised. Degraded and/or historically simple methods of communication tools should be the norm. A few examples of these being marking devices,

strobes, or in some cases, unsuspecting frequencies (e.g. HF). Supporting forces should operate a military weapon system (MWS) that can operate in degraded environments devoid of cyberspace inputs. Examples of these include aircraft not tied to datalinks, GPS, and/or requiring of external data inputs for navigation and/or attack.

Cyber forces enabling both creation of the dead zone as well as transit corridors and EW attack should be sourced to provide and monitor the capabilities contained in Figure 5 below as a starting point.

Cyber effects needed to create a cyber exclusion dead zone	
Infrastructure Denial	At a minimum, the denial of power and access to cyberspace within designated zone(s). Isolation of telecommunication switches.
DDoS (Or current version of overwhelming)	Overwhelm and exhaust access to operating sites within zone.
Disaggregated & Distributed EW Barrage Jamming	Enables corridor and denies use of radio waves for maneuvering forces to coordinate or pass information on friendly forces.
GPS and other position data denial	Limit ability of PGMs, enemy equipment operations, or enabling of forces to locate and interdict friendly forces.
Other desired Cyber Effects	Any denial of day-today civilian services designed to invoke panic/chaos and create an environment where small teams of forces moving about in the masses would go unnoticed, or at least unreported and unhindered.

Figure 5

Operations in Cyberspace: Issues for Consideration

Introduction

Cyberspace represents the newest and possibly least understood domain to wage war. As a result, great caution and limited use principles continue to guide doctrine on cyber domain

implications and maneuver within. With respect to military operations in cyberspace, the US Military Joint Publication 3-12 *Cyberspace Operations* specifically addresses it as such, stipulating it is not an operation but a domain in which IW and other operations can occur.[18] Air, land, and sea all represent domains that have been used by mankind to wage warfare for thousands of years. What these domains have in common, along with space, is they exist with or without mankind. Now a new domain exists in which man is compelled to prepare to wage war upon his enemies, the domain of cyberspace. Unique to the other domains is the fact that cyberspace is manmade.[19] What is not unique about cyberspace is that warfare waged inside of cyberspace will often negatively affect civilians using the same domain for business, pleasure, transportation, security, medical care, communications, and numerous other important day to day life activities. Just as the naval blockades, sieges, and aerial bombardments disrupt the civilian populace and economics of their targets, so too can cyberspace cause disruptions beyond their intended targets.

During the cyber-attack on Estonia in 2007, the Estonian Minister of Defense stated, "when the navy of another country blocks a country's ports or the air force of another country blocks a country's airspace, this is in no way different from blocking access to pages of another country with cyber-attacks."[20] Furthermore, just like sieges, aerial bombardments, and naval blockades can be used in retribution by an enemy, so too cyberspace be used against the original attacker. Continued exploration of the weaponization techniques within the domain of cyberspace is being pursued, like that of the other domains, in professional articles and military publications, books, military doctrinal publications, and political policy. This section will review in closer detail current writings on the discussions surrounding cyber as a weapon, historical uses of cyber by one state against another, national policies and positions for its use, and implications

resulting from these discussions. Ultimately, with the above-mentioned items matched against places without bases operations, this section will conclude with considerations that discuss the use of cyber dead zones in future small team operations.

Cyber Attack, Defense, and Denial

Cyberspace represents an opportunity for three distinct, but not limited to, methods of warfare - cyber-attack, cyber defense, and cyber denial —to be discussed in the proceeding section. [21] In their work *Weaving Tangled Webs,* Eric Gartzke and Jon Lindsay, pose the possibility that cyber-attack could be easier than cyber defense. The ease with which an enemy can reach across hemispheres to perform an attack outside of declared hostilities presents a compelling case for the need for cyberspace defense and/or denial. The United States military, specifically the Marine Corps Operating Concept 2016, has cited cyber protection as of equal importance to that of command and control, fires, or mobility. [22] The United States Air Force and Army seek individuals with cyberspace skillsets for placement in their cyber units, ultimately destined, due to growth, to join new major commands (MAJCOM) created specifically for cyber warfare.[23] Specifically, the Air Force will do this through the combination of the 24th and 25th Air Force and the Army through creation of an Army Cyber Directorate with EW capabilities.[24] Ultimately, the creation of CYBERCOM serves as an indicator to the importance of the domain. These measures come during a period in which the last ten years has seen sophisticated cyber-attacks like STUXNET worm, which the United States supposedly invented and gave to the Israelis to target Iranian nuclear infrastructure, and the hacking of the Democratic National Committee (DNC), a possible effort to undermine the US national election. These measures are especially prudent considering the White House stated that reported cases of cyber-attacks

against the United States have increased ten percent over the last year and PEW research suggests they will continue to rise.[25] PEW further suggests though, that, as attacks increase, so too will countermeasures (defense).

Expansion of cyberspace defense continues to grow with the rate of cyberspace attacks and highlights the nation's susceptibility to cyber-attack, evidenced by the most recent hack of the DNC in the 2016 election. United States defense and research agencies, in this case Defense Advanced Research Project Agency (DARPA), continue to use and further develop technologies and techniques that alert the presence of electronic attack. Additionally, the developed techniques are expanding to include methods of defense through deception, actually luring attackers to predetermined locations and presenting false data.[26] The United States Department of Defense (DOD) has stated its three cyber missions are: "Defend DoD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and provide cyber support to military operational and contingency plans."[27] Not only does the DOD underscore a posture of defense in cyberspace, but the last of the three missions discusses use to provide support to the military. These potential uses will be discussed in section four of this paper as a requirement for small team operations in places without bases.

Our final topic for review, cyber denial, specifically thwarts access or free flow of information to and from the respective target. Allison Russell mentions refusing free flow of information in her work *Cyber Blockades* as a "cyber blackout" targeted at an enemy state. Denials of information in the cyberspace domain generate a stoppage of data needed for critical infrastructure, communications, and flow of information.[28] The cases of Estonia in 2007 and Georgia in 2008 demonstrate the use of blockades for cyber denial. Both attacks used methods

such as DDoS attacks, designed to prevent the flow of information in and out of the country and to paralyze critical infrastructure. Of note, the attack in Georgia was near simultaneous with the invasion of Russian forces, setting perhaps the first precedent for cyber denial to accompany or even mask troop movement. Russian movements were synchronized against a target now severely degraded with respect to information and communication flow. In both cases, the attack against an entire state and willingness to either directly target its public or accept them as collateral damage, is presenting itself as a new capability and new norm for other countries, Russia as an example. Although the cases suggest that this sort of cyberspace attack is a new warfighting consideration, in the case of the Russian attack on Georgia, it also highlights the ability to attribute attacks to states.

As offensive cyber warfare continues to expand, it provides the ability of friendly and enemy forces to disable each other's critical equipment by reaching across international borders or the forward edge of the battle area (FEBA).[29] The notion of reaching across borders via cyberspace benefits the idea that United States forces can in some instances affect the targets it wishes to without setting foot on enemy ground. It also comes with the condition that if performed, it provides the enemy an opportunity to exact retribution upon attribution, or in some cases, reverse engineer, and re-attack in kind.[30] Thus, the use of cyber techniques pose as a double edge sword by providing an opportunity to affect the enemy but also creating an opportunity for the enemy to counterattack in certain cases. Some examples would be spears being thrown back at the originator, the arms race generated by the first use of a nuclear weapon, recreation of electronic warfare techniques, and the reverse engineering of numerous Russian man portal air defense systems (MANPADS) by the Chinese.[31] However, the fear of attribution that might normally prevent a force from using the cyber domain in a tactically offensive manner

could be rendered worth the acceptable level of risk dependent upon the strategic need of its use.[32] Knowing that employment of tactical cyber for strategic operations could create attribution or retribution in kind, appropriate selection of employment techniques in the cyber domain is needed in the calculus of operational art. Cyber denial is one such technique that could limit attribution.

Cyber denial represents an opportunity to render an entire nation or region unable to use the domain of cyberspace. Specifically, as noted by Russell, the use of cyber denial denies critical infrastructure and systems as well as the ability of information to flow. This denial ultimately prevents a state from accessing cyberspace. [33] This use of denial, or a blockade, is very similar in concept to blockades in other domains, such as a naval blockade denying access to the sea or an enemy integrated air defense system (IADS) denying use of the air.

Where denial of the cyber medium could provide for decreased threat to United States forces through suppression of enemy forces, others have noted that the consequences to non-combatants of certain cyberspace operations could constitute Geneva Convention violations.[34] Russell notes that even if a policy is in place, without attribution, punishment for such consequences are rendered moot. Ultimately in the case of Estonia and Georgia, Russian involvement was assumed but unanswered through lack of attribution. Whereas the result of both cases demonstrated the damage possible through cyber blockades, it also demonstrated that the international community is unprepared to address these issues as it would with other domains where physical harm is present. This failure could also be in part to the more difficult challenge of attributing a cyber blockade to a specific state as opposed to other domain blockades, which also poses problems in identifying legalities and implications of use.[35] Additionally, the ambiguous nature as to the existence of international norms and laws governing the legal use of

cyber warfare are cause for concern but are continually being addressed and it is reasonable to assume in the next 2-40 years these rules could be in place.[36]

Legalities and implications of use of the cyberspace domain present many open-ended implications as international laws and definitions are still being debated in literature. *The Tallinn Manual on the International Law Applicable to Cyber Warfare* presents one example of a NATO sponsored effort to frame the problem of international law and cyberspace as a weapon. Although a thorough number of agreements or treaties exist, the experts involved in publication consistently note that jus ad bellum and jus in bello are applicable to cyber warfare. They go on to address that there exist relevant norms of law and conflict that can be applied and suggest that objects can be targeted for attack in accordance with laws of conflict.[37]

Attribution and retribution in this case then could be considered moot points assuming cyberspace domain operations were conducted within the spirit of laws of armed conflict in mind. If actors were to use methods of operating within the cyber domain that posed a rational attack upon an enemy in combat, it would present the same expectation as an attack on an enemy in any of the other domains. This interpretation suggests that in the scenario of places without bases, the risk of using a cyber blockade or creation of a cyber dead zone could be warranted if planners can assess that the tactical use and ensuing consequences are both worth the risk and meet the threshold of military necessity as well as proportionality in execution.

Rule 69 – Zones

To the extent that States establish zones, whether in peacetime of during armed conflict, lawful cyber operations may be used to exercise their rights in such zones. ~ Tallinn Manual on the International Laws Applicable to Cyber Warfare [38]

Rule 69 and its discussion of zones demonstrates the applicability of just war norms applicable to cyber war. *The Tallinn Manual* notes that some experts consider a cyber blockade to be lawful and directly related to a blockade of another domain. Thus, a cyber blockade is subject to the applicable blockade laws. However, as retribution or counter-attack from the enemy can always be assumed, US forces can expect similar methods to be employed against them in some cases. Ultimately, implications of cyber use present a large challenge to its use and must be considered.

Summary

Current literature and analysis highlight the risks associated with exploiting cyberspace as a domain in which to wage war. The use of the cyber domain risks retribution in kind, and international sanctions if employed in a manner outside of accepted norms or in accordance to the spirit of current just war ideals. However, like the use of the nuclear weapon in the climax of World War II Pacific operations, history has shown that strategic goals can drive the use of such initial uses of new modes of warfare. Ultimately, just as the nuclear weapon, after initial uses of cyber techniques, opportunities are presented for duplication or retribution. The following section will discuss the ASP groups forecast for the future places without bases environment that would drive such considerations for the use of tactical cyber denial and attack techniques. The follow-on section will highlight small team's operations within such a cyber denial environment if the future places without bases scenario as experimented with during the 2017 "Wargames to Inform the Marine Corps 2025."

Trial Use During "Wargame to Inform the Marine Corps 2025"

During the first series of iterations of "Wargames to inform the Marine Corps 2025," the tactical use of a cyber dead zone as a possibility was posed. The scenario presented a large,

littoral, urban center with both enemy state and non-state actors, a neutral population, and in some cases, enemy technological parity, or advantage. The problem posed was how to infiltrate American forces into the population center against an overwhelming and hidden force capable of influencing the local population to its cause. The enemy had access to multiple surface to air weapons system, anti-ship cruise missiles, launch rocket systems, and heavy, anti-tank weapons, and multiple different small arms to include heavy machine guns. Additionally, the enemy possessed sophisticated unmanned aerial systems (UAS) and multi-faceted command and control communications. The cyber dead zone was posed for use during the transition from phase one to phase two.

In the transition from phase one to phase two, the American forces would infiltrate to multiple disaggregated zones via covert tilt rotor and amphibious landing craft. Planners posed isolating the population center and its surroundings to prevent the enemy from communicating, mobilizing, and most importantly, degrading kill chain communications with the desired effect of forcing the enemy into an autonomous mode. As this paper foresaw in the above text, the course of action drew immediate apprehension from the planners within the deception cell who were concerned with civil and public affairs. Objections cited the lack of proportionality should civilians lose access to power and other emergency services. Furthermore, planners from the maneuver cell raised the issue that the same effects could be achieved through communications jamming only. Upon war gaming, the course of action was deemed inappropriate and the wargame proceeded without any form of cyber denial.

As the wargame proceeded, the enemy was ultimately able to exploit the cyberspace domain free of interference. The enemy utilized social media and television to influence the local population against United States forces. Furthermore, the enemy could communicate with each

other via cyberspace methods and ultimately could fire multiple ASCM at the US naval fleet. They were also able to shoot down one MV-22, injuring all aboard. It was determined that lack of denial had contributed to the enemy's freedom of action during this phase.

The lack of willingness by the Marine Corps in the wargame against an enemy that was willing to utilize cyber demonstrated the concept mentioned in the literature review that US forces must be prepared to operate and attack in cyberspace or risk losing to enemies who are willing to operate in the domain. Although this example occurred in a wargame and not an actual armed conflict, the visceral reaction against the use of cyber denial, and resulting enemy advantages as a result, posed that more analysis and experimentation must be dedicated to cyber denial in support of US forces when operating in urban centers against an enemy with technological parity. Upon conclusion of the debrief and wargame hot wash, the white cell in charge of adjudication as well as the red cell in charge of enemy forces did state that denial of cyber would have resulted in an enemy inability to fire the ASCMs as well as give the order to shoot down the helicopter and mobilize. Further discussion of proportionality was highlighted. In the case of wargame one it was determined that the risk to friendly forces to facilitate civilian comfort or avoid secondary order effects was unactable. Thus, the need for further doctrine to be developed that identifies proportionality was highlighted.

Although the preceding wargame example of non-utilization of this method demonstrated results with multiple casualties, it could not be known what danger the forces may or may not have faced from a populace without access to cyberspace preceding the move. Best assumptions were made regarding enemy and public disposition from both the from the white cell, red cell, and blue cell. This was noted for consideration in wargame two.

The second wargame provided the same scenario. During mission planning, a cyber blockade was implemented into the chosen course of action (COA). Upon commencement of the amphibious assault, enemy forces were unable to effectively coordinate during the initial assault. Without effective coordination, they were accustomed to, enemy forces were forced to communicate via personnel acting as physical messengers. The resulting breakdown of communication contributed to the enemy failing to mass and employ ASCMs and effective coordination of effort as demonstrated in the first wargame. The reduction in communication speed and degradation in communication quality allowed the US forces to move swiftly to and into the objective area only encountering only small arms fire and ballistic, indirect rockets which failed to score direct hits. No aircraft or amphibious vehicles were lost and injuries were reduced to one platoon that advanced on a re-enforced enemy position.

The second wargame demonstrated that successful employment of a cyber blockade could keep the enemy from communicating and coordinating as well as finding and fixing the friendly force beyond visual acquisition. By reducing the advanced methods of communication and decreasing the speed of the remaining abilities to communicate, the blockade degraded the ability of the enemy to quickly mobilize. Through denial of the enemy ability to find and fix friendly forces via cyberspace and electronic identification measures, the enemy was unable to employ technology driven precision fires upon the friendly force. This degradation occurred for the duration of the wargame (approximately 48 hours). Additionally, friendly personnel and equipment losses were reduced because of the cyber blockades use.

The first wargame was an example of non-utilization of this method. Failure to use the cyber blockade resulted in multiple casualties. However, it could not be known in advance what danger the forces may or may not have faced from a populace without access to cyberspace. The

second wargame demonstrated its success, but given the shorter duration, it was difficult to ascertain how prolonged cyber denial would have impacted the civilian populace. Ultimately, the course of action proved a viable solution to enable forces in a large, urban, littoral city center to achieve its objectives and prevented loss of friendly life and equipment. As a result, considerations for the course of action were published in the Marine Corps Warfighting Lab Ellis Wargame Series April 2017 edition. Lastly, the trial use highlighted the following risk analysis of strengths and weaknesses.

Risk Analysis

Evaluation of Cyber Space Dead Zone Creation Considerations	
Strength	Weakness
Eliminates reporting of friendly force disposition	Limits friendly force ability to report disposition
Provides LPI (Low Probability of Intercept)	Negatively affects civilian population, loss of life
Disrupts precision guided munitions	Negatively affects civilian economy
Degrades targeting cycle	Negatively affects emergency services for civilians
Degrades/denies enemy communication	Relies on antiquated communication, navigation, weaponry capabilities
Camouflages friendly forces amongst multitudes of civilians	Difficult to judge proportionality
Ability to switch from denial to deception and attack once in place	

Figure 6

Recommendations for Future Research

This paper has recommended an option for operating in future places without bases against an opponent with technological parity residing in a congested, denied, littoral environment. Much more research is needed as the United States moves into a future where

emerging enemies continue to close the technology gap the United States currently enjoys. Listed below are current recommendations at the time of this paper's design.

1- What will be the acceptable level of risk that would drive the United States to use a cyber exclusion zone, more specifically as described by this paper, a cyber dead zone? Possible options could be nuclear disarmament, capture/kill of a high value target, seizing of infrastructure, and/or forcible entry.
2- What are the expected future legal implications of use of a cyber dead zone? Although the legalities of cyber-attack and the laws of armed conflict continue to develop, will the future see use of cyber-attack as convoluted and ill-defined as they currently are?
3- How will the United States handle the high likelihood of losing increased amounts casualties, troops that become cut off, or that troops that the US forces never regain contact with.
4- What technology can the United States possibly design or repurpose that can operate within a small localized network and remain unencumbered by the dead zone?
5- How can the United States limit attribution/retribution for cyber-attacks, assuming they are not considered a new norm of future warfare?
6- What would a collateral damage estimate analysis/model be when performing risk analysis and decision making when implementing a cyber blockade?

Conclusion

As the United States prepares to operate in the future, its defense community must consider that the future will present challenges that threaten previous United States dominance in technology and limit its ability to operate freely in places of its own time and choosing.

Operating in places without bases could become the norm. Enemies with technological parity will continue to present themselves. Cyberspace will continue to develop as an increasingly popular and provocative domain in which to wage warfare. As the United States faces a future of potential increasing A2/AD environments and an entire nation of enemies maneuvering in cyberspace around its forces, the need for non-traditional and irregular warfare operations will continue to grow. Using disaggregated, non-traditional, small team operations, hiding in plain sight inside the confines of a cyber/EW dead zone, the ability to operate will be preserved.

---

[1] Marine Corps Warfighting Laboratory*, Littoral Operations in a Contested Environment: Developing a New Naval Operating Concept. Quantico VA. Marine Corps Gazette.* Feb 2016.
[2] Magnuson, Stew. "Marine Corps Focuses on Urban Scenarios." *National Defense Magazine*, November 2015. http://www.nationaldefensemagazine.org/archive/2015/November/Pages/MarineCorpsRDFocusesonUrbanScenarios.aspx.
[3] Headquarters US Marine Corps, Intelligence, Surveillance, and Reconnaissance Enterprise Plan. Washington DC, Headquarters US Marine Corps, Sep 2014.
[4] Marine Corps Warfighting Laboratory*, Littoral Operations in a Contested Environment: Developing a New Naval Operating Concept. Quantico VA. Marine Corps Gazette.* Feb 2016.
[5] Magnuson, Stew. "Marine Corps Focuses on Urban Scenarios." *National Defense Magazine*, November 2015. http://www.nationaldefensemagazine.org/archive/2015/November/Pages/MarineCorpsRDFocusesonUrbanScenarios.aspx.
[6] Headquarters US Marine Corps, Intelligence, Surveillance, and Reconnaissance Enterprise Plan. Washington DC, Headquarters US Marine Corps, Sep 2014.
[7] Brian Flood, Ohio State Attack Plays out on Social Media in Real Time. The Wrap. November 28, 2016.Thewrap.com
[8]Population Division, United Nations. (2016) http://mediad.publicbroadcasting.net/p/wfae/files/201408/UN_Growth_Map.JPG
[9] Headquarters US Marine Corps. Marine Corps Operating Concept: How an Expeditionary Operating Force Operates in the 21st Century. Washington DC, Headquarters US marine Corps, Sept 2016.
[10] *Future Operating Environment 2035*. 1st ed. Ministry of Defence. London: Strategic Trends Program, December 15, 2015.
[11] Erik Gratzge & Jon Lindsay (2015) Weaving Tangled Webs: Cyber Offense, Defense, and Deception in Cyberspace Security Studies, 24:2, 316-348
[12] Andrew Metcalf & Christopher Barber Tactical Cyber: How to Move Forward. Small Wars Journal. (2014)
[13] Ingress to and from areas of operations will be IAW Maj Laird's (USMC) Command and Staff College AY17 Advanced Study Program Operating Concept. In this concept, he poses infil and exfil of forces using reduced signature tactics as well as deception tactics.
[14]Allison Russell*, Cyber Blockades* (2014, Washington DC. Georgetown University Press) 90.
[15] Clark, Bryan and Mark Gunzinger. *Winning the Airwaves: Regaining America's Dominance in the Spectrum*. Washington, DC: Center for Strategic and Budgetary Assessments, 2015.
[16] Headquarters US Marine Corps. Marine Corps Operating Concept: How an Expeditionary Operating Force Operates in the 21st Century. Washington DC, headquarters US marine Corps, Sept 2016.
[17] Headquarters US Marine Corps. Marine Corps Operating Concept: How an Expeditionary Operating Force Operates in the 21st Century. Washington DC, headquarters US marine Corps, Sept 2016.

[18] Joint Publication 3.12 Cyberspace Operations. 5 Feb, 2013.
[19] Allison Russell*, Cyber Blockades* (2014, Washington DC. Georgetown University Press) pp1-3
[20] Baltic News Service "US, European Specialists Help Estonian Deal with Cyber Attacks.
[21] Cyber deny, attack, defense
[22] Headquarters US Marine Corps. Marine Corps Operating Concept: How an Expeditionary Operating Force Operates in the 21st Century. Washington DC, headquarters US marine Corps, Sept 2016.
[23] Welsh, Mark, A., Speech to 24th and 25th Air Forces, 26 Aug 2015.
[24] Judson, Jenn. *Army Electronic Warfare Strategy Nearing Completion*. Defense News, 1 Dec 2016.
[25] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/
[26] Hugh Thompson et. al. Anomaly Detection at Multiple Scales (ADAMS) (final report, Defense Advanced Research Agency)
[27] https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy
[28] Allison Russell*, Cyber Blockades* (2014, Washington DC. Georgetown University Press) 90
[29] Erik Gratzge & Jon Lindsay (2015) Weaving Tangled Webs: Cyber Offense, Defense, and Deception in Cyberspace Security Studies, 24:2, 316
[30] Ibid 331-332
[31] Joseph Nye, Nuclear Lessons for Cyber Security. Strategic Studies quarterly. (2011)
[32] Erik Gartzge, The Myth of Cyberwar, Brining Warfare Back Down to Earth. (Fall 2013). International Security, Vol. 38, No 2. p47.
[33] Allison Russell*, Cyber Blockades* (2014, Washington DC. Georgetown University Press) pp1-3
[34] Nato Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Laws Applicable to Cyber Warfare. Cambridge University Press 2013.*
[35] Allison Russell*, Cyber Blockades* (2014, Washington DC. Georgetown University Press) 123.
[36] [36] Nato Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Laws Applicable to Cyber Warfare. Cambridge University Press (2013) 3.*
[37] Ibid. 7.
[38] Ibid 202.

Bibliography

Baltic News Service "US, European Specialists Help Estonian Deal with Cyber Attacks.

Brian Flood, Ohio State Attack Plays out on Social Media in Real Time. The Wrap. November 28, 2016.Thewrap.com

Clark, Bryan and Mark Gunzinger. *Winning the Airwaves: Regaining America's Dominance in the Spectrum*. Washington, DC: Center for Strategic and Budgetary Assessments, 2015.

Gratzge, Erik & Lindsay Jon. (2015) Weaving Tangled Webs: Cyber Offense, Defense, and Deception in Cyberspace Security Studies, 24:2, 316

Headquarters US Marine Corps, Intelligence, Surveillance, and Reconnaissance Enterprise Plan. Washington DC, Headquarters US Marine Corps, Sep 2014.

Headquarters US Marine Corps. Marine Corps Operating Concept: How an Expeditionary Operating Force Operates in the 21st Century. Washington DC, Headquarters US marine Corps, Sept 2016.

Joint Publication 3.12 Cyberspace Operations. 5 Feb, 2013.

Judson, Jenn. *Army Electronic Warfare Strategy Nearing Completion*. Defense News, 1 Dec 2016.

Magnuson, Stew. "Marine Corps Focuses on Urban Scenarios." *National Defense Magazine*, November 2015. http://www.nationaldefensemagazine.org/archive/2015/November/Pages/MarineCorpsRDFocusesonUrbanScenarios.aspx

Marine Corps Warfighting Laboratory, *Littoral Operations in a Contested Environment: Developing a New Naval Operating Concept. Quantico VA. Marine Corps Gazette.* Feb 2016.

Nato Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Las Applicable to Cyber Warfare. Cambridge University Press 2013.*

Metcalf, Andrew & Barber, Christopher. *Tactical Cyber: How to Move Forward*. Small Wars Journal. (2014)

Rainee, L. Anderson, J. & Connolly, J. Cyber Attacks Likely to Increase. PEW Research Center. (2016).

Russell, *Allison, Cyber Blockades* (2014, Washington DC. Georgetown University Press) pp1-3

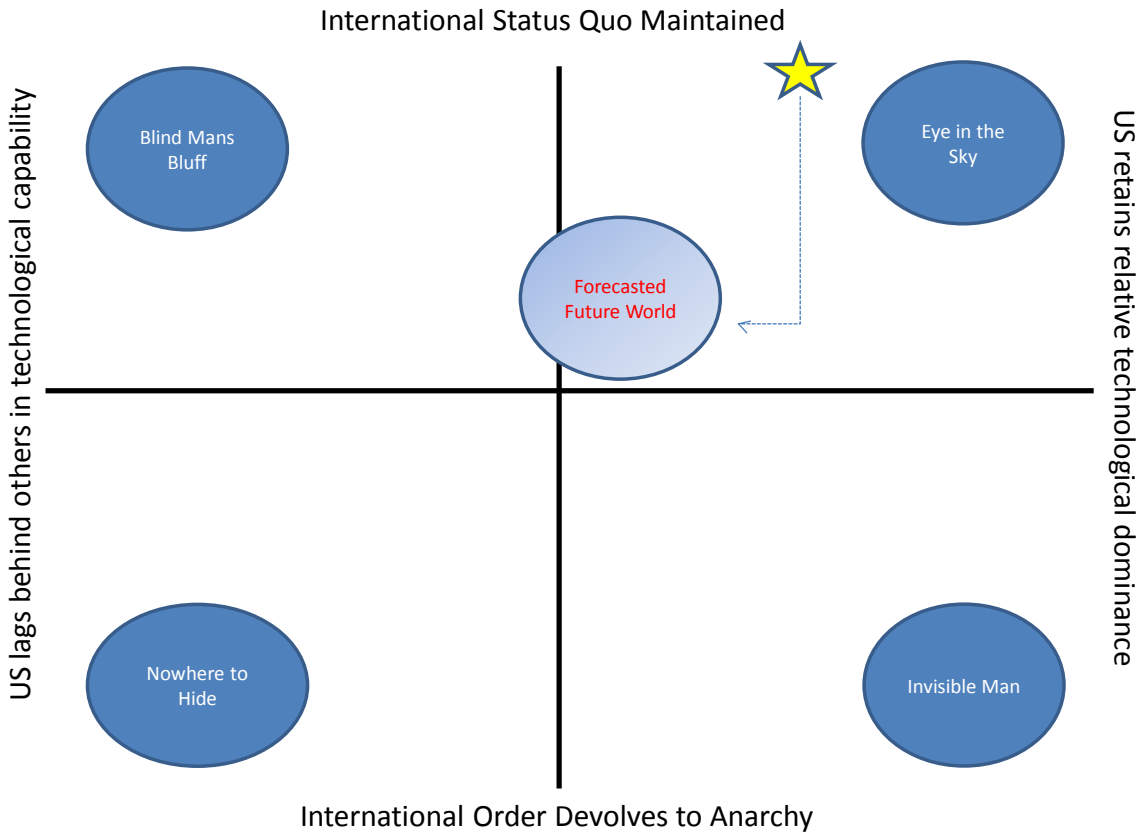
Thompson, Hugh., et. al. *Anomaly Detection at Multiple Scales (ADAMS*) (final report, Defense Advanced Research Agency) Washington DC.

United States Department of Defense. Special Report: *Cyber Strategy*. (2016) https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

Welsh, Mark, A., Speech to 24th and 25th Air Forces, 26 Aug 2015.

Appendix One

Future World Forecast Quad-Chart



Matters of Concern and Characteristics:

Blind Man's Bluff: International order remains intact. However, the US is no longer enjoying hegemon status. Past allies and adversaries take over lead in technology development and capability. US still conducts self as a superpower but no longer the perennial champion. Enjoys the benefit of other allies and superpowers tolerant of its existence but skates by on past laurels and exists at the leisure of other superpowers.

Nowhere to Hide: No control over cyber infrastructure; threatened money market systems; terror increases; U.S. turns inward. At this point the ability to remain undetected is no longer a possibility. Any movement or position is detectable due to proliferation of open market technology. Disorder exists in the sense that traditional governments and militaries no longer rule but more the haves versus the have nots dictate order. Resources are taken, those with technological edge and resources rule the day.

Eye in the Sky: Continued partnering in international system; U.S. retains hegemon status; U.S. partnership and arms sales increases due to desire of other countries to remain engaged and allied; small interventions dwindle, terror continues but at level even less capable of disturbing United States interests. Any involvement the United states chooses to get into is done with relative comfort because of technological superiority, as it can move around undetected for limited duration operations at will.

Invisible Man: Resource competitions more likely to lead to war without diplomatic intervention; increased population and turbulence in the littoral regions. Multi-state conflict becomes more common; law and order pursued in the interest of U.S. The U.S. moves about to interdict where it can for limited duration, either to quell rebellion, gather resources, or prevent the rise to power of players or technology that threaten little advantage remaining. U.S. limited in ability to deploy large forces due to partnership limitations; civil liberties decline worldwide.