NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNCONVENTIONAL CYBER WARFARE: CYBER OPPORTUNITIES IN UNCONVENTIONAL WARFARE

by

Christopher R. Eidman
Gregory Scott Green

June 2014

Thesis Advisor: Dorothy Denning
Second Reader: Doowan Lee

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
UNCONVENTIONAL CYBER WARFARE: CYBER OPPORTUNITIES IN UNCONVENTIONAL WARFARE

5. FUNDING NUMBERS

6. AUTHOR(S) Christopher R. Eidman, Gregory Scott Green

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	**12b. DISTRIBUTION CODE**
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

Given the current evolution of warfare, the rise of non-state actors and rogue states, in conjunction with the wide availability and relative parity of information technology, the U.S. will need to examine new and innovative ways to modernize its irregular warfare fighting capabilities. Within its irregular warfare capabilities, the U.S. will need to identify effective doctrine and strategies to leverage its tactical and technical advantages in the conduct of unconventional warfare. Rather than take a traditional approach to achieve unconventional warfare objectives via conventional means, this thesis proposes that unconventional warfare can evolve to achieve greater successes using the process of unconventional cyber warfare.

14. SUBJECT TERMS attack, COIN (counterinsurgency), computer network operations, computer networks, conflict, cyber-attacks, cyber power, cyber warfare rules, cyber terrorism, department of defense, electronic security, electronic warfare, information security, information warfare, insurgency, international politics, Internet, irregular warfare, military applications, military capabilities, military doctrine, military operations, military strategy, network centric warfare, non-state actors, power diffusion, special forces, special operations command, special operations forces, strategic impact, unconventional warfare, warfare, Anonymous, armed attacks, law of armed conflict(LOAC), asymmetric warfare, collateral damage, computer crimes, computer security, conventional warfare, crowdsourcing, cyber militia, cyber espionage, cyber warriors, cyberspace, DDoS Attacks, defense policy, deterrence, ethics, soft power, hard power, hacktivists, hackers, international law, use of force, technology and foreign policy

15. NUMBER OF PAGES 99

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UNCONVENTIONAL CYBER WARFARE: CYBER OPPORTUNITIES IN UNCONVENTIONAL WARFARE

Christopher R. Eidman
Major, United States Army
B.S., Auburn University, 2000

Gregory Scott Green
Major, United States Army
B.A., Mississippi State University, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Authors: Christopher R. Eidman
Gregory Scott Green

Approved by: Dorothy Denning
Thesis Advisor

Doowan Lee
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Given the current evolution of warfare, the rise of non-state actors and rogue states, in conjunction with the wide availability and relative parity of information technology, the U.S. will need to examine new and innovative ways to modernize its irregular warfare fighting capabilities. Within its irregular warfare capabilities, the U.S. will need to identify effective doctrine and strategies to leverage its tactical and technical advantages in the conduct of unconventional warfare. Rather than take a traditional approach to achieve unconventional warfare objectives via conventional means, this thesis proposes that unconventional warfare can evolve to achieve greater successes using the process of unconventional cyber warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. GENERAL AREA OF RESEARCH....1
B. STATEMENT OF PURPOSE AND SCOPE....1
C. BACKGROUND....2
D. RESEARCH QUESTION....2
E. CENTRAL CLAIM....3
F. METHODOLOGY....3
1. CONCEPTUAL FRAMEWORK....4
2. CASE STUDIES....5
G. THESIS STRUCTURE....7

II. WARFIGHTING AND UNCONVENTIONAL CYBER WARFARE....9
A. IRREGULAR WARFARE....9
B. UNCONVENTIONAL WARFARE....12
C. CYBER WARFARE....14

III. LEGAL, ETHICAL, AND ATTRIBUTION ASPECTS OF UNCONVENTIONAL CYBER WARFARE....19
A. LEGAL CONSIDERATIONS....19
B. ETHICAL CONSIDERATIONS....21
C. ATTRIBUTION....25

IV. CASE EXAMINATION....27
A. CASE 1: THE RUSSO-GEORGIAN WAR: CYBER MILITIA IN SUPPORT OF CONVENTIONAL OPERATIONS....27
1. THE WORD....29
2. THE MESSENGER....30
3. THE DEED....31
B. CASE 2: SYRIAN ELECTRONIC ARMY: CYBER MILITIA IN SUPPORT OF THE STATE....35
1. THE WORD....36
2. THE MESSENGER....39
3. THE DEED....40
C. CASE 3: ANONYMOUS – NON-STATE ACTORS AS CYBER MILITIAS....45
1. BACKGROUND....45
2. CHAIN OF EVENTS....48
3. CONCLUSION....54

V. UNCONVENTIONAL CYBER WARFARE: A THEORETICAL FRAMEWORK....59
A. WHEN TO EMPLOY UCW....59
B. UCW FRAMEWORK....64
1. PREPARATION....66

2. INITIAL CONTACT 67
3. INFILTRATION 69
4. ORGANIZATION 70
5. BUILDUP 71
6. EMPLOYMENT 72
7. TRANSITION 72
C. CONCLUSION 73
VI. CONCLUSION 75
LIST OF REFERENCES 77
INITIAL DISTRIBUTION LIST 83

LIST OF FIGURES

Figure 1. Warfighting areas conceptual diagram 5
Figure 2. Screenshot of an alleged Facebook message sent to the Syrian Electronic Army notifying them of their page removal. 38
Figure 3. Syrian Electronic Army Facebook page announces that over 50 websites have been attacked, and that it did not destroy content of any of the websites. 41
Figure 4. Screenshot of defaced website of Royal Leamington Spa Town Council at http://www.leamingtonspatowncouncil.gov.uk. 41
Figure 5. Claimed defacements by IP and country, May 16–June 19, 2011. 42
Figure 6. Screenshot of defaced website of Israeli Member of Knesset Arieh Eldad. 43
Figure 7. Syrian Electronic Army documents its "virtual demonstration" on U.S. President Barack Obama 44

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Top 20 countries of mobile phones per 100 people 60
Table 2. Top 20 countries by number of Internet users per 100 people 61
Table 3. The most repressive countries in the world 62
Table 4. Map of the Top 10 most censored countries 62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

.pdf	portable document format
4GW	fourth generation warfare
ARSOF	Army Special Operations Forces
CDs	compact disks
COIN	counter insurgency
CMO	conventional military operations
DIMEFIL	diplomatic, information, military, economic, financial, intelligence, and law enforcement
DDoS	distributed denial of service
DNS	domain name server
DOD	Department of Defense
EW	electronic warfare
GPF	general purpose forces
GRU	Russian Foreign Military Main Intelligence Directorate
HTML	hypertext markup language
ICT	information communication technology
IDS	intrusion detection service
IP	Internet protocol
IRC	Internet relay chat
ISP	Internet service provider
IW	irregular warfare
MCO	major combat operations
MySQL	open-source relational database management system
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PE	preparation of the environment
PVT	private
QDR	Quadrennial Defense Review
RBN	Russian Business Network
Scribd	digital library

SEA	Syrian Electronic Army
SOF	Special Operations Forces
TCP/IP	transmission control protocol / Internet protocol
UCW	unconventional cyber warfare
UCWOA	unconventional cyber warfare operational area
UN	United Nations
UW	unconventional warfare
UWOA	unconventional warfare operational area

I. INTRODUCTION

A. GENERAL AREA OF RESEARCH

With the current evolution of warfare shifting from conventional to irregular conflicts, with the rise of non-state actors and rogue states, in conjunction with the wide availability and relative parity of information technology, and with current and expected future cuts in defense spending, the U.S. will need to examine new and innovative ways to modernize its irregular warfighting capabilities. Within its irregular warfare capabilities the U.S. will need to identify effective doctrine and strategies to leverage its tactical and technical advantage in the conduct of unconventional warfare. Rather than take a traditional approach to achieve unconventional warfare objectives via conventional means, this thesis proposes that unconventional warfare can evolve to achieve the same, as well as greater successes using unconventional cyber warfare.

B. STATEMENT OF PURPOSE AND SCOPE

The purpose of this thesis is to identify and explore a new irregular warfare option for the United States: unconventional cyber warfare (UCW). Specifically, this thesis will demonstrate cyber warfare is a viable option during unconventional warfare and how UCW can employ existing capabilities to achieve successful unconventional warfare interventions. Marine Corps General James E Cartwright, former Vice Chairman of the Joint Chiefs of Staff provides this definition for cyber operations: "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[1] FM 3-05.130 *Army Special Operations Forces Unconventional Warfare* (U) provides the current definition of UW as follows: "operations conducted by, with, or through irregular forces in support of a resistance

[1] James E. Cartwright, *Joint Terminology for Cyberspace Operations*, JCS Memorandum, November 2010, 8, http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint Terminology for Cyberspace Operations.pdf.

movement, an insurgency, or conventional military operations."[2] For the purposes of this thesis, unconventional cyber warfare (UCW) will be tentatively defined as seeking to achieve military objectives or effects in or through cyberspace by, with, or through irregular forces in support of a resistance movement, an insurgency, or conventional military operations. Initial research indicates that the U.S. has yet to formulate clear guidelines on how to employ cyber warfare to coerce, disrupt, or deter adversaries. However, examination of research on cyber warfare indicates that these capabilities have been and will be employed in an offensive manner by states and non-state actors within the scope of cyber warfare to achieve national, regional, and local objectives.

C. BACKGROUND

Recent events have demonstrated the rise in global technical acumen as well as the national will of our adversaries and allies alike to employ cyber warfare as a means of accomplishing political and military objectives. As a result the Department of Defense has increasingly emphasized cyber warfare with the creation of Cyber Command to address concerns and to develop a national capability with regard to the conduct of cyber warfare. A major concern for cyber warfare and unconventional warfare is the apparent lack of doctrinal integration.

D. RESEARCH QUESTION

This thesis intends to answer the following research question: how can cyber warfare be utilized in unconventional warfare campaigns? To answer this question two additional research questions will be examined. First, the thesis will attempt to determine if existing cyber warfare capabilities will allow for successful unconventional warfare interventions. Secondly, it will examine whether working through surrogates will allow for greater access and preserve the clandestine or covert nature of an UCW intervention. While few countries have engaged in UCW as a strategy within the confines of our definition, historical cases of UCW do exist to warrant the main research question.

[2] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare* (Washington, D.C.: Headquarters, Department of the Army, 2008), 1–2, http://orfeu-marketing.com/data/documents/A9R7039.pdf.

E. CENTRAL CLAIM

The central claim of this thesis is that cyber warfare can be an effective tool in achieving U.S. strategic goals within the measured response available via a UW campaign, and that it should play an important role in future UW campaigns. However, the appropriate use of cyber warfare depends less on the operational environment than other factors, including the capabilities of the opposing forces, level of access to their systems, and the resistance force to be used as a cyber-militia. Looking at the spectrum of unconventional warfare objectives: disrupt—coerce—overthrow, in relation to the relative technical capabilities of a given country, will assist in determining what goals the U.S. should work to obtain via cyber warfare. For instance, one set of conditions on the ground, such as the ones found in Georgia, may mean that cyber means could be used in an effort to disrupt the nation's capabilities in parallel with a concurrent ground offensive. On the other hand, in Syria for example, cyber means were employed in support of the oppressive Assad regime and its policies. To help strategists determine whether and how cyber warfare can support a UW campaign in a given country or situation, this thesis will develop an unconventional cyber warfare employment methodology.

F. METHODOLOGY

The amount of literature addressing how existing cyber warfare capabilities should and could be employed is extensive and expresses opinions that range from cyber warfare being a near infinite threat to governments and organizations to cyberwar has never happened, and will never happen.[3] This thesis will identify theories or principles of cyber warfare, approaches to address cyberwar concerns, potential vulnerabilities to cyber-attacks, and how the cyber domain compares to other domains of warfare. It is the goal of this thesis to provide a possible scenario whereby the U.S. might employ offensive cyber warfare in a manner that brings offensive military intervention into the 21st century.

[3] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, doi:10.1080/01402390.2011.608939.

The research question will attempt to examine if working through surrogates allows for greater access and preserves the clandestine or covert nature of an UCW intervention. Previous research examines how "guerrilla warfare" is the least likely form of unconventional warfare that will occur in modern times, how the focus should be on indirect activities of unconventional warfare: subversion, sabotage, and intelligence activities, and goes so far as to espouse the establishment of a separate branch of military service, solely focused on the conduct of unconventional warfare.[4] It does not, however, examine how new and emerging capabilities could be employed, within the traditional tenants of unconventional warfare, to achieve the desired state intervention that is traditionally associated with the conduct of unconventional warfare. This thesis will scrutinize empirical evidence from selected case studies to determine the critical factors of how to accomplish the essential components of unconventional warfare intervention.

As the U.S. moves away from employment of conventional military power into the IW realm of cyber operations and unconventional operations, strategists and military theorists will need to embrace the capabilities of emerging technologies while recognizing the real world requirement of working by, with, and through indigenous forces to achieve our foreign policy objectives. Conventional military intervention in response to threats to national security by state and non-state actors may not be feasible. Kinetic operations may be too risky or have too much collateral damage associated with their outcomes, and may also curtail the opportunity for a measured response. Under certain conditions, UCW may serve as a more effective means of conducting an unconventional intervention to achieve national military objectives.

1. CONCEPTUAL FRAMEWORK

The conceptual framework of this thesis draws from three major areas, conventional warfare, irregular warfare, and cyber warfare. The conventional warfare area is comprised of conventional military weapons and battlefield tactics. The area of irregular warfare is similar to conventional warfare in that it encompasses conventional

[4] Steven P. Basilici and Jeremy Simmons, "Transformation: A Bold Case for Unconventional Warfare" (Monterey, CA: Naval Postgraduate School, 2004), 4.

weapons and tactics. However, it differs in that it is primarily via indirect or asymmetrical means. This area also includes the sub-area of unconventional warfare. The cyber warfare area is comprised of actions taken against an entity's computers or networks. Based on the overlapping regions of these areas there are eleven sub-areas as illustrated in Figure 1.

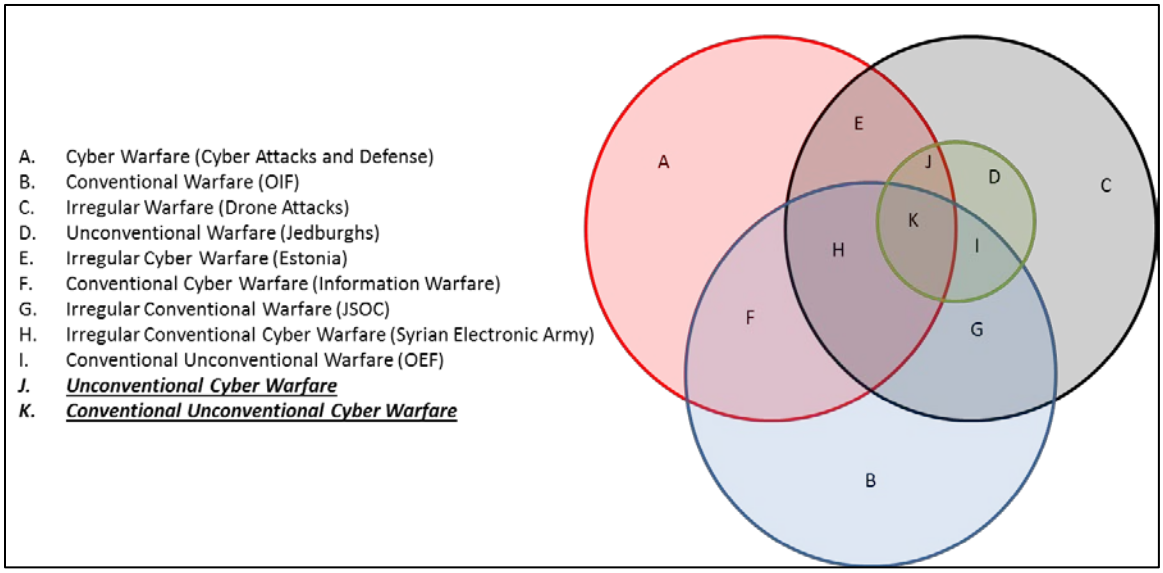

Figure 1. Warfighting areas conceptual diagram

Nine of the sub-areas will be briefly addressed, but not analyzed as previous research or governing doctrine already exists for them. The focus area for this thesis will be the remaining two sub-areas, where unconventional warfare, cyber warfare, and conventional warfare overlap. This focused area of overlap highlights the required pre-conditions for the employment of unconventional cyber warfare to accomplish a successful intervention

2. CASE STUDIES

This thesis will primarily use the method of discovery and the congruence method to examine when and how to successfully conduct unconventional cyber warfare. The method of discovery will rely on historical process-tracing to analyze the event chain in each case to illustrate how these cyber organizations used a unifying message, their means of disseminating the message, and their cyber means to achieve the desired effects.

This inductive approach will allow the examination of the cases into causal chains, highlighting each individual evolution in the chain.

Empirically, three cases will be analyzed in detail: the Russo-Georgian Conflict; the Syrian Electronic Army; and the Anonymous operations during the Arab Spring. These cases each demonstrate key facets that will make them valuable when developing a future model for UCW. The Russo-Georgian conflict was a combined cyber-kinetic conflict pitting Russian nationalist hackers and the Russian military against Georgia. In this conflict, via a distributed denial of service (DDoS) attack, the attackers were able to disrupt access to Georgia's Internet and several government websites while the Russian military was able to invade in support of the South Ossetian breakaway region of Georgia.[5] This case will contribute to the proposed UCW framework by its employment of a nationalist cyber militia and in its contribution to the overall success of the concurrent conventional conflict. The second case, Syrian Electronic Army, is a series of coordinated cyber-attacks by non-state Syrian actors loyal to the Assad regime targeting opposition forces, both foreign and domestic, in support of the regimes position in the Syrian civil conflict.[6] This case contributes to the proposed UCW framework in that it demonstrates a possible means of creating a cyber-militia leveraging existing expertise in the UCWOA. The third case, Anonymous, involved multiple cyber-attacks against national infrastructure in order to support revolutionary movements during the Tunisian chapter of the Arab Spring.[7] This case will contribute to the proposed UCW framework by demonstrating the opportunity to leverage an existing cyber-militia like organization by repurposing an existing organization to serve the need of the sponsor in a UCW conflict.

---

[5] Dancho Danchev, "Coordinated Russia vs Georgia Cyber Attack in Progress," Security, *ZDNet*, August 11, 2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

[6] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," *Infowar Monitor: Tracking Cyberpower*, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/.

[7] Sulome Anderson, "Anonymous Threatens Morsy with Cyberwarfare," *Foreign Policy*, November 28, 2012, http://blog.foreignpolicy.com/posts/2012/11/28/anonymous_threatens_morsy_with_cyberattacks.

G. THESIS STRUCTURE

The remainder of the thesis is organized as follows: Chapter II describes the three areas of warfare that relate to UCW: irregular warfare, unconventional warfare, and cyber warfare. Chapter III discusses legal, ethical, and attribution issues associated with UCW. Chapter IV covers the three cases outlined above. Chapter V discusses when and where to apply UCW and offers a framework for its application based on the current phases of UW. Finally, Chapter VI offers our concluding thoughts and recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WARFIGHTING AND UNCONVENTIONAL CYBER WARFARE

In this chapter, we will examine the areas of warfighting that bear upon the concept of UCW. These areas consist of irregular warfare (IW), unconventional warfare (UW), and cyber warfare. We will seek to define each domain, look at key factors of the domain, and how they may influence our proposed warfighting concept, UCW.

A. IRREGULAR WARFARE

With a concept as complicated as irregular warfare it is usually best to start with a definition to create a common frame work. The Department of Defense defines irregular warfare as:

> Irregular Warfare is a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.[8]

When examining the foundation of an IW operation it is important to understand who is conducting the action, how the action is being conducted, and why the action is being conducted.[9] The underlying principle that differentiates IW from conventional warfare is its focus on a specific population. In an IW campaign it is necessary to exert control or influence over said population, for the purpose of either stabilizing or destabilizing the legitimacy of the political authority over the specific population.[10]

Since World War II, the majority of warfare that the U.S. has been involved in has been irregular in nature. Our opponents today, both state and non-state alike, are not likely to be defeated by conventional military power alone. In order for the U.S. to be

---

[8] U.S. Special Operations Command and U.S. Marine Corps, "Irregular Warfare Joint Operating Concept" (Department of Defense, September 11, 2007), http://www.au.af.mil/au/awc/awcgate/dod/iw_joc.pdf.

[9] Ibid.

[10] Ibid.

successful in battle, it must intertwine the facets of social, cultural, political, information, and economic activities with the added complexity of supporting or destabilizing foreign governments, and their security forces, to defeat an unconventional enemy via unconventional means.[11] U.S. forces currently confront a conundrum with regard to ways and means regarding IW operations. From an organizational, training and equipping standpoint, the U.S. is much better suited and configured to meet its responsibilities regarding a conventional conflict, however, from an IW perspective, U.S. forces are not equally trained, equipped, nor organized to meet its responsibilities regarding that spectrum of conflict.[12] By the end of the 2006 *Quadrennial Defense Review* (QDR), the Department of Defense (DOD) senior leadership determined that it was underfunded in both general purpose forces and special operations forces (SOF), as well as both capabilities and capacity to conduct protracted IW.[13]

When it comes to the actual execution of IW, how do we know if and when we are successful? The basis for acquisition and operational planning for U.S. forces has traditionally been dependent upon analysis of conventional war fighting and presents a real bias towards "measuring physical effects on near-peer forces, played out over days or months, of a maneuver attrition campaign."[14] Traditional measures of success in military operations, which have largely consisted of control of the battle space, and the size and force structure of the friendly order of battle, would be effective at evaluating "force-on-force battles in a Clausewitzian style engagement."[15] Applying these measures of effectiveness to an IW scenario, where the forces are generally small, may not necessarily have territory under their control, and seldom engage via traditional tactics or means, would be ineffective at best.[16] Traditional IW assessments have been tied to three factors,

---

[11] Kenneth C. Coons, Jr. and Glenn M. Harned, "Irregular Warfare Is Warfare," *Joint Force Quarterly* 1st Quarter 2009, no. 52 (2009): 99.

[12] Ibid., 98.

[13] Ibid.

[14] James Clancy and Chuck Crossett, "Measuring Effectiveness in Irregular Warfare," *Parameters* 37, no. 2 (June 22, 2007): 13.

[15] Ibid.

[16] Ibid., 91.

sustainability, legitimacy, and environmental stability, with the measures of effectiveness (MOE) of an irregular force determined by these three factors.[17] Based on current definitions of IW, measures for success should be population oriented, rather than adversary oriented, with measures of success tied to winning the support of friendly populations, supporting friendly authorities, and eroding the power structures of adversarial powers.[18]

The world we live has changed dramatically. The familiar landscape of the Cold War is giving way to a mosaic of state and non-state actors, all jostling for power and position, while employing the elements of national power they may be able to bring to bear. With the number of failed states on the rise and a growing trend in some parts of the world for physical security to become an article of trade, powers arise to contest with the central government. In addition, there are cases where the legitimate government can no longer provide for the security of their populaces.[19] These forces, by their nature as non-state actors, will have to look to asymmetric means, such as IW, because they will lack the capabilities to employ and succeed by means of conventional warfare. Answering an irregular threat with a conventional response is a recipe for disaster; in order for our efforts to be successful we "must use a blend of political, informational, military, economic, and sociocultural approaches, in combination with foreign governments, security forces, and populations."[20] Employing an indirect approach, via cooperative action with a surrogate force within a contested area, would allow the U.S. to tailor its response to enable these partner forces to combat irregular threats via training, equipping, technology sharing, and other similar proven practices.[21] An indirect approach alone is not enough though; it will require a long-term commitment to this surrogate relationship

---

[17] Ibid., 97.

[18] Coons, Jr. and Harned, "Irregular Warfare Is Warfare," 99.

[19] Theresa Reinold, "State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11," *The American Journal of International Law* 105, no. 2 (April 2011): 4–5, doi:10.5305/amerjintelaw.105.2.0244.

[20] Coons, Jr. and Harned, "Irregular Warfare Is Warfare," 99.

[21] Eric T. Olson, "A Balanced Approach to Irregular Warfare," *The Journal of International Security Affairs*, no. 16 (2009): 3.

to make any lasting change, change that will over time contribute to the stability of a region, deny safe-havens for insurgents, and deter the future development of irregular opposition forces.[22]

Irregular warfare, by all indications, will become the standard and not the exception for the types of conflicts that the U.S. will face in the foreseeable future. Responding to an irregular threat with conventional forces will not provide the proper force structure or tools for success against an irregular opponent. The U.S. has identified and begun modifications to doctrine and force structure development to position itself to succeed in an IW conflict, but that work is not complete. Current efforts continue to be based on the tried and true tactics and techniques that were established and honed during the IW campaigns in Vietnam. In order to succeed against the irregular combatant of today we need to be able to evolve from the old mantra "hearts and minds," to a more 21st century centric mantra of social media and networks. By combining the historical principals of IW, such as by, with, and through, with the modern constructs like social media and complex networks, the U.S. can position itself for continued success in the population centric irregular warfare domain.

B. UNCONVENTIONAL WARFARE

Since its inception, U.S. Army Special Forces has been recognized as the nation's preeminent unconventional warfare (UW) force. Unfortunately, the lexicon of terms utilized by practitioners and non-practitioners alike to describe what exactly UW is has become confusing. However, two themes have remained consistent through multiple UW definition revisions; UW is conducted through, with, or by a surrogate force and the surrogate force is irregular in nature.[23] Unconventional warfare is not the inverse of conventional warfare. Conventional warfare seeks to employ general purpose forces (GPF) to defeat an adversary's armed forces, destroy an adversary's military capability,

[22] Ibid., 5.

[23] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*, 1–2.

and coerce, through force, an adversary's government.[24] UW can be employed against state or non-state actors and may or may not involve direct military confrontation.[25]

Just as UW is not conventional warfare, it is also not irregular warfare. As previously discussed, IW seeks to influence relevant populations and may employ the full range of military and other capabilities to do so.[26] Whereas UW also seeks to influence relevant populations, IW does not require that operations be conducted by, with, or through irregular forces. UW may be conducted within an IW campaign and as a method for conducting IW, but because UW is used to support insurgencies, resistance movements, and conventional military operations, by, through, or with surrogate forces, it is precluded from being categorized as solely an IW activity.[27]

Last, unconventional warfare is also not asymmetric warfare, unrestricted warfare, or fourth generation warfare (4GW). While it is useful to characterize UW as asymmetric in its application of techniques and activities to coerce, disrupt, or overthrow a government, the term asymmetric warfare refers more to the disparity between two opponents' strengths, sizes, capabilities, rather than the employment of irregular forces. Furthermore, there is no approved definition the use of the term "asymmetric warfare." Similarly, 4GW and unrestricted warfare also lack an accepted DOD definition and associated doctrine. While both propose there is a new era that has been entered into with respect to the way in which war is conducted, the later advocates for less restrictions and greater breadth of tools and capabilities with which to prosecute war; ultimately none directly address the central idea that UW is conducted by, with, or through surrogate forces of an irregular nature.[28]

---

[24] U.S. Special Operations Command and U.S. Marine Corps, "Irregular Warfare Joint Operating Concept."

[25] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*, 1–4.

[26] U.S. Special Operations Command and U.S. Marine Corps, "Irregular Warfare Joint Operating Concept."

[27] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*, 1–7.

[28] Ibid., J-3 – J-4.

As the U.S. continues to be the dominant military power, nation-states and non-state actors will continue to develop methods with which to avoid direct military conflict. Similarly the U.S. should maintain a measured response to counter such developments. Unconventional Warfare remains beneficial to the U.S. as a response because it provides a capability to cope with situations where strategic interests exist, but an optimal solution, in terms of the application of conventional military force, does not.[29] This is not to suggest that the definition of UW should not be further refined, nor does it advocate that doctrine not be revised and updated to acknowledge the vast technological accomplishments that have occurred since the idea of UW was first advanced. On the contrary, UW theory and doctrine should be focused on the development of capabilities that capitalize on the current operating environment in order to remain relevant, particularly if theories advancing the notion of 4GW and unrestricted warfare gain traction with our adversaries.

C. CYBER WARFARE

The conceptual framework for cyber warfare will be examined in the context of cyber policy, cyber strategy, and asymmetric warfare. Marine Corps General James E Cartwright, former vice chairman of the Joint Chiefs of Staff, provides this definition for cyber operations: "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[30] There is little about cyber warfare that is standardized and because of the nature of cyberspace what is known is in a near constant state of change. This section will provide a point of departure in our understanding of cyber warfare as we expand on the concept of UCW.

Cyber policy is having trouble keeping up with the changing times; gone are the days when the most significant threat in cyberspace was isolated hackers. Today, cyber policy must contend with sophisticated state actors, and a myriad of non-state actors

[29] Basilici and Simmons, "Transformation," 17.

[30] Cartwright, *Joint Terminology for Cyberspace Operations*, 8.

consisting of transnational crime organizations, "hacktivists," and patriotic hackers.[31] There is a great deal of reluctance to implement any type of systematic cyber policy because

> the government does not own the Internet, other major elements of cyberspace, or most of the critical infrastructures that depend on the Internet, and because there are strong incentives for many groups to resist measures that would help secure the Internet.[32]

The tendency for policy makers is to focus cyber warfare policy on historical precedents of historical warfare domains generally resulting in policy constrained by historical "attributes of military operations, such as mass, speed, synchronization, fires, command-and-control, and hierarchy, at the expense of other ways, such as engineering, as a way of creating or preventing effects."[33] In an unconventional warfare scenario, it would be possible to exploit the overall reluctance to adopt a global cyber policy, and in doing so neutralize opponents who rely on networked systems for operations or, possibly, to leverage this dependence in an asymmetric manner thus leaving their militaries less capable than if they had never adopted networked systems.[34]

Libicki, in "Cyberspace is not a Warfighting Domain," proposed that because of the factors of economy, certainty, and risk, cyberspace should be the preferred means of accomplishing one's desired effects in war.[35] To accomplish ones ends, cyber strategy should exploit the capabilities of the targeted opponent's systems. When one's opponent is vulnerable within cyberspace, then the opponents overall dependence on networks and systems should be the governing factor when determining whether to employ cyber as an operational means.[36] The concept of cyber power revolves around the low barriers to

---

[31] Terrence K. Kelly and Jeffrey Allen Hunker, "Cyber Policy," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 1.

[32] Ibid., 216.

[33] Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8 (2013 2012): 328.

[34] Ibid., 330.

[35] Ibid., 324.

[36] Ibid., 323.

entry and relatively limited cost of exerting influences on many facets of a society, from war to commerce. Ideally cyber means will be employed where one can create "preferred outcomes *within* cyberspace or cyber instruments can be used to produce preferred outcomes in other domains *outside* cyberspace."[37] As an adjunct to unconventional warfare, the strategic employment of cyber operations can achieve soft power in cyber space through agenda framing, attraction or persuasion.[38] In addition, in an unconventional warfare scenario, the strategic employment of cyber operations can achieve hard power to organize a distributed denial of service attack by using cyber militias to attack target's systems, or to insert malicious code designed to disrupt systems, or to steal intellectual property.[39]

The most capable adversary that one may encounter is the one that can attack your weaknesses from a position of relative strength without you knowing the attack is coming. Cyberwar has the potential to be the latest asymmetrical warfighting arena where a less powerful, or inferior force, may hope to gain parity and contest successfully with a much larger and stronger adversary. Clarke and Knake point out four key asymmetries that highlight the U.S.'s susceptibility to cyber-attacks: higher dependency on cyber enabled systems than any potential adversary, dispersal of essential systems in the private sector, the individual and collective political power of those private sector actors to prevent or dilute government regulation, and lastly the U.S. military's reliance on information sharing at all levels with the vulnerabilities to cyber-attack associated with these practices.[40] With ever increasing constraints on military budgets, the impetus is on military thinkers to create and employ capabilities to defeat the opponents they face, rather than choosing their opponents based on their current capabilities.[41] Our adversaries

---

[37] Joseph S. Nye, *Cyber Power* (Belfer Center for Science and International Affairs: Harvard Kennedy School, May 2010), 4, http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522626.

[38] Ibid., 5.

[39] Ibid., 6.

[40] Richard A Clarke, Cyber War (HarperCollins, 2011), 226–227.

[41] Charles Billo and Welton Chang, *Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States* (Hanover, NH: Dartmouth College, December 2004), 30, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.

recognize the significant role that cyber operations can play in offsetting an opponent's military superiority and see cyber operations as a cost effective means of conducting asymmetric warfare.[42] Nye points out that:

> Cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by small states using asymmetrical warfare; it is unlikely to be a game changer in power transitions. On the other hand, while leaving governments the strongest actors, the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century.[43]

Significant to the special operations community is the stated or implied opportunity to accomplish cyber effects via a proxy force, laying the foundation for future research on uses of a cyber-militia as a resistance force.

[42] Ibid., 29.

[43] Nye, *Cyber Power*, 19.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LEGAL, ETHICAL, AND ATTRIBUTION ASPECTS OF UNCONVENTIONAL CYBER WARFARE

This chapter will provide an examination of the legal, ethical, and attribution considerations and how they may apply to UCW. Particular consideration will be paid to how UCW could be viewed by the international community and how it may fit into current and future international law. While presented as subtopics it should be noted that each of these areas of consideration are interrelated and interdependent and should not be considered in a standalone manner. In this chapter we contend that there is an existing construct applicable to warfare and even though UCW is a new approach it should be governed by the existing legal, ethical and attribution considerations as applied to current conflicts.

A. LEGAL CONSIDERATIONS

With the ever increasing reliance on computers and networks for day to day operations, both in the civilian and military sectors, it has become increasingly important to gain a legal understanding of how cyber operations will be viewed in terms of international law. It is widely recognized that attacks within the cyber realm can be of strategic, operational, and tactical importance. Cyber operations have been demonstrated to be effective at accomplishing military objectives with similar effects as psychological operation, electronic warfare operation (EW), or kinetic attacks.[44] The very facet of networks that makes them such an integral piece of day to day operations is also the decisive feature that makes them a desirable target for cyber operations.[45] This in turn creates an attractive asymmetrical threat, whereby a weaker power can compete with a stronger power, via a means that negates the power base of its opponent, by employing a low-risk and low-cost option to achieve its goals.[46] In *The Law of Cyber Attack*, the

[44] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Information, 1999, 891, http://papers.ssrn.com/abstract=1603800.

[45] Ibid., 893.

[46] Ibid., 897.

authors propose the following distinctions for cyber operations: cyber-crime (only non-state actors, violation of criminal law), cyber-attack (objective to undermine function of computer network, must have political or national security purpose), and cyberwar (objective to undermine function of computer network, must have political or national security purpose, equivalent to armed attack or occurring during armed conflict).[47] In a UCW scenario, cyber operations would often be conducted by non-state actors opposed to the State's sovereign authority. The tendency may be to categorize these actions as cyber-crime, but due to the actions being in support of a political position, or in opposition to a nation's security, these acts would be governed by the same rules that govern cyber-attack.[48]

There is an ongoing debate as to whether cyberspace requires its own body of law or if instead existing law applies to cyberspace, whence it is a matter of identifying existing legal principles that can be effectively applied to the "person, place, object or type of activity in question."[49] Cyber-attacks, under certain conditions, may be considered a use of force, and therefore prohibited within the UN Charter, with the exceptions of self-defense, and UN Security Council mandate.[50] Cyber-attacks that have a clear kinetic parallel are easily categorized based on this precept. Controversy arises when discussing state responsibility for acts committed by non-state actors, in our case a resistance or proxy force, and also acts that do not result in injury or damage.[51] The issue of non-state actors is addressed by citing the International Court of Justice Nicaragua case that found that funding guerrillas who are conducting armed opposition against a state did not constitute an armed attack, but that arming and training them did; a decision that also suggested the consequences of an action need not be immediate to rise to the

[47] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100 (2012): 817.

[48] Ibid., 815.

[49] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *The Harvard International Law Journal Online* 54 (December 12, 2012): 17.

[50] Ibid., 18–19.

[51] Ibid.

level of a use of force.[52] These experts found that a cyber-attack would not have to include immediate consequences in the physical world and that arming a proxy force with the means of conducting cyber operations against a state would be consistent with an armed attack, but providing them with a safe haven would not.[53] If states desire to bypass the use of force constraint, highlighting the challenge of distinction in cyber warfare today, they may hide their involvement in cyber-attacks by permitting civilians as irregular armed forces to carry out cyber-attacks on their behalf.[54] Regardless of a state's ability to disguise its involvement in a cyber-attack via a proxy force, if the attack in question can be attributed to forces under its direction or control, then the state is legally responsible for the actions of its proxy.[55]

B. ETHICAL CONSIDERATIONS

The ethics concerning UCW can be incorporated into existing discussions on *jus in bello*, commonly referred to as the moral principles governing conduct in war, and need not be broken out into a unique area for consideration. The prima facie ethical question would be: can computers be used as weapons? Similar to the argument that objects with the capability to cause harm or death are not all categorized as weapons, the argument can be made that the intent of employment of a tool, in this case a computer, to create foreseeably harmful consequences is the means by which computers earn weapons status and the employment of them against an adversary may be considered a use of force.[56] In support of the use of cyber weapons, Denning and Strawser argue that it is "ethically obligatory" to use cyber weapons in place of kinetic weapons as long as the

---

[52] Ibid., 20.

[53] Ibid.

[54] Hathaway et al., "The Law of Cyber-Attack," 41.

[55] Harold Hongju Koh, "International Law in Cyberspace" (Remarks|Remarks presented at the USCYBERCOM Inter-Agency Legal Conference, FT Meade, MD, September 18, 2012), 4, http://www.state.gov/s/l/releases/remarks/197924.htm.

[56] William J. Bayles, "Moral and Ethical Considerations for Computer Network Attack As a Means of National Power in Time of War" (U.S. Army War College, 2000), 9.

action is just and there is no significant loss of capability.[57] Citing as advantages, these experts observe that, all other things being equal, cyber weapons are less risky to military personal because of the operational distance that can be achieved with their employment, and because cyber weapons can deliver kinetically equivalent military objectives without necessarily resulting in loss of life to one's adversary, nor to innocents and non-combatants.[58] Drawing on their example of manned verses unmanned aircraft, the parallel exists, in the case of a fully justified war, to achieve the same effects using a cyber means, without impacting the actor's ability to fight justly, and then because of their associated lower risk and cost to conduct, militaries are obligated to employ cyber means.[59] Furthermore, these experts would contend that in the case of a just war, the just fighter will bear an even larger burden with regard to the tenets of proportionality and necessity, thus requiring them to accomplish their ends with the means that uses the least amount of force and would incur the least amount of risk.[60]

Rowe, in his paper "Ethics of Cyberwar Attacks," posits that two key factors of cyber-attacks can be employed to mitigate the associated collateral damage: targeting precision and repair mechanisms.[61] Target precision provides the means whereby attacks are limited not only by the specificity of the target machines, but also a more granular level of specific critical software aspects on these machines.[62] The use of repair mechanisms allows for implementation of attack vectors that are easily reversible, either by doing no real harm, perhaps only making code segments unavailable for specific periods, or by providing a cyber-antidote to a neutral third party to be held until the end

[57] Dorothy E. Denning and Bradley J. Strawser, "Moral Cyber Weapons: The Duty to Employ Cyber Attacks," in *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo (Springer, 2012), 87.

[58] Ibid., 88.

[59] Ibid., 87.

[60] Ibid., 89.

[61] Neil C. Rowe, "Ethics of Cyber War Attacks," in *Cyber Warfare and Cyber Terrorism*, ed. Lech Janczewski and Andrew M. Colarik (Idea Group Inc (IGI), 2008), 107.

[62] Ibid.

of hostilities.[63] As Denning and Strawser point out, reversibility would be of immense value for stability and reconstruction operations and would allow for critical infrastructure to be targeted and restored within hours rather than the days, weeks, and months that would be associated with like infrastructure targeted by kinetic weapons.[64] This will be further elaborated upon in Chapter VI, when we present the way forward for UCW.

The case for the morality of cyber weapons is not without detractors. Rowe cites the difficulties associated with identifying attackers and targets in cyber, the high cost/low reusability of cyber weapons, and the secrecy associated with conducting cyber-attacks as why their use is ethically questionable.[65] He goes on to posit that since the ethics of using cyber weapons is questionable, states should enact an ethical cyber policy by doing one of three things: 1) pledge to never employ cyber weapons, 2) pledge to not use cyber weapons as a first strike capability, or 3) pledge to only use cyber weapons in response to cyber weapons.[66] Adopting Rowe's proposal to never employ cyber weapons would effectively concede cyberspace to the multitudes of state and non-state actors that are currently conducting cyber activities today, often with no regard for legal or ethical constraints. A better course of action would be to conduct operations in cyberspace within the precepts of *jus ad bellum* and *jus in bello*, against legitimate military targets whereby employing cyber means would achieve the desired effects but with less risk and collateral damage than the same effects might be achieved by a kinetic means.[67] Likewise, his proposal to not employ cyber weapons as a first strike option could give rise to the employment of harmful kinetic first strike options that may cause unnecessary civilian casualties and unintended collateral damage, both of which may have been avoided with the employment of an equally just but discriminate cyber means.[68] Lastly,

---

[63] Ibid., 108.

[64] Denning and Strawser, "Moral Cyber Weapons," 91.

[65] Rowe, "Ethics of Cyber War Attacks," 108.

[66] Ibid.

[67] Denning and Strawser, "Moral Cyber Weapons," 93.

[68] Ibid., 97.

his third proposal to only use cyber weapons in response to cyber can be countered with the same arguments used against the prior two proposals; chiefly when the means are currently employed across the spectrum of cyberspace, it is ethically and morally incumbent upon those with the capability, against legitimate military targets, to employ just cyber means which would achieve the same effects as just kinetic means, but with less risk and collateral damage.[69] These arguments are the basis for our position that UCW is a more ethically responsible means of achieving effects than traditional UW.

It is essential for the sponsor forming and controlling cyber militias to understand the legal and ethical considerations of employing civilians in a cyber-attack role. Civilian cyber warriors, a facet of UCW operations employing resistance or proxy forces, can be subject to that state's domestic criminal laws, which is not the case if the same actions were undertaken by a member of an opposing military force.[70] Additionally, these civilian cyber warriors, and their military cohorts, may be attacked with any legal means, wherever they may be found, and the associated collateral may not be deemed excessive due to the threat posed by the cyber warrior.[71] These are just some of the concerns that must be taken into consideration when planning to use proxy forces to conduct UCW.

As presented above, employment of cyber weapons is a contentious issue that will be made even more so by the employment of proxy cyber militias during unconventional warfare. However, the current legal and ethical framework for conducting a just war is as applicable for this type of employment of forces as it has been for the employment of kinetic weapons since its inception. The advantage to examining these issues within the existing legal and ethical framework is that when employing a cyber means to accomplish a just military objective, the desired effect may be accomplished with more precision, less collateral damage, and with a keen eye on leveraging the target for future operations. Until such time as there is a kinetic means that can be employed to the same

---

[69] Ibid., 93.

[70] Charles Dunlap, "The Intersection of Law and Ethics in Cyberwar: Some Reflections," *Air & Space Journal*, January 1, 2012, 6.

[71] Ibid., 6–7.

effect and reversed in the same timeframe, it would be a difficult argument to not employ the cyber means, all other things being equal.

C. ATTRIBUTION

The simplest definition for cyber attribution is "determining the identity or location of an attacker or an attacker's intermediary"[72] Cyber attribution also should consider identification of intermediaries, whether they are willing or unwilling, and the traceability of the attack, starting from the target and tracing backwards to the attacker.[73] In addition, it should consider sponsors of attacks, especially in cases where the sponsors are nation states, but are not directly involved in the attacks themselves. Attribution is inherently limited by the capability of attackers to time-offset their attacks while simultaneously routing these attacks through intermediaries in many jurisdictions, some benign and some hostile, further complicating the attribution effort.[74]

Technology allows for the near complete anonymity of actors in the cyber domain and severely hampers attribution efforts.[75] Typical computer networks are not designed with attribution in mind. In some instances the networks' own capabilities unintentionally complicate the act of attribution because of the ease by which information, such as sender addresses can be "spoofed.[76] While possible to improve the attribution process via technological features like logging, tracing, and unique communication keys, these options alone may not be sufficient to provide attribution in cases of extreme action.[77] Attribution means beyond the information infrastructure will be required to meet the

---

[72] David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* (Defense Technical Information Center, 2003), 1, http://handle.dtic.mil/100.2/ADA468859.

[73] Jeffery Hunker, Bob Hutchinson, and Jonathan Margulies, "Role and Challenges for Sufficient Cyber-attack Attribution" (Institute for Information Infrastructure Protection, 2008), 5, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

[74] Wheeler and Larsen, *Techniques for Cyber Attack Attribution*, 53.

[75] Stephen J. Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains," in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 2010, 16.

[76] Wheeler and Larsen, *Techniques for Cyber Attack Attribution*, 5.

[77] Hunker, Hutchinson, and Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," 11.

standard of sufficiency, especially if the objective is to determine not only the attackers, but their sponsors.[78]

The risk of nation states using attribution techniques against its own citizenry to suppress independence and civil liberties is a concern that has led to the development of technologies that provide anonymity and to the rejection of policies that prohibit all anonymous activity.[79] Hunker, Hutchinson, and Marguiles propose the creation of an acceptable and sufficient means of attribution without destroying non-attribution.[80] They contend that most states will emphasize maintaining their strategic flexibility and would accept a system that guarantees attribution in the case of offensive or defensive employment of cyber weapons by nation states.[81] We contend that states would prefer to maintain the capability to conduct their own operations in cyberspace in a clandestine manner, and therefore may not be willing to accept a system that guarantees attribution, assuming such guarantees were even possible.

Without adequate attribution there would be no basis for taking action against cyber-attackers or their sponsors, thus setting the conditions for a successful anonymously sponsored UCW campaign. Offensive operations, such as computer network attack, could be employed in a UCW scenario with high confidence that the sponsor of such attacks could remain anonymous if so desired. The overall difficulty with attribution provides for the perfect opportunity to conduct a covert UCW campaign that gives the resistance force flexibility and the resistance sponsor anonymity.

---

[78] Ibid.

[79] Wheeler and Larsen, *Techniques for Cyber Attack Attribution*, 50–51.

[80] Hunker, Hutchinson, and Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," 4.

[81] Ibid.

IV. CASE EXAMINATION

This section will examine three cases relevant to UCW. The first two, the Russo-Georgian conflict and the Syrian conflict, will be conducted in three parts: the word, the messenger and the deed. The word portion will examine the underlying message that was the unifying theme for the movement, what the movement's stated or unstated goals might be, and the events that led to the movement's creation. The messenger portion will examine the means and methods that were employed to spread the word, how the movement conducted their recruiting, and then how they managed their day to day operations. Lastly the deed portion will delve into the tactics, techniques and effects of the movement's actions, at both an operational level and a strategic level. The approach for the third case on Tunisia's revolution will vary because it exemplifies third party, non-state actors, working on behalf of a resistance movement. This case will examine the events that set the conditions for success and posit that the existence of dissident and diaspora media, cyber activists, Anonymous, and coordinated cyber operations in support of revolutionaries in Tunisia were able to effect socio-political change within that country.

A. CASE 1: THE RUSSO-GEORGIAN WAR: CYBER MILITIA IN SUPPORT OF CONVENTIONAL OPERATIONS

Cyber-attacks, in support of conventional military operations have a great deal of potential to be force multipliers on today's complex battle fields. Imagine a simultaneous attack in cyber space and in the physical realm, designed to cripple a country's ability to communicate, both internally and externally, and making it virtually unable to defend against a military assault by conventional forces. In 2008, that very scenario was carried out in the Russo-Georgian conflict with Russian conventional operations supported and its success enhanced by a carefully coordinated cyber strike, via a surrogate force, that was able to render the Georgian Republic incapable of defending itself in either the cyber or physical domain.

What was the popular message used to create to movement that spawned the surrogate force? How was the surrogate force recruited and empowered to carry out the cyber-attacks? What are the odds that this type of an attack would be successful? How likely is it that given the near simultaneity of the assaults that they were not coordinated and orchestrated by the attacking state? These are some of the questions that have been asked and examined following the ground and cyber conflict between Georgia and Russia in 2008. In this case, we will examine this conflict in terms of how the narrative that was the genesis for the conflict was used to organize and empower a surrogate force, and then the actions and impact of the surrogate force.

The conflict between Georgia and Russia in 2008 on the surface would appear to be the result of longstanding animosity between neighbors; however, the conflict was much more complicated and nuanced. Though the principal players in the conflict were these two nations, the actual conflict was a proxy for longstanding animosity at the local, regional, and international level. At the local level, this conflict has its roots in the ethnic strife rampant in the Soviet satellite states after the collapse of the Soviet Union. The Georgian regions of South Ossetia and Abkhazia initially sought more autonomy within the Georgian Republic, but supported by their Russian neighbors and their 1992 blanket offer of Russian citizenship for former citizens of the Soviet Union their demands were escalated from autonomy to complete independence.[82] Though this conflict has gone through a number of cycles prior to the conflict in 2008, the movement began to pick up speed with the declaration of independence by Kosovo in February of 2005. These factors lead to a major push by the Russian Republic of North Ossetia to call for unification with the breakaway Georgian province of South Ossetia.[83] This conflict also served as a proxy for the ongoing friction between NATO and Russia with regard to NATO expansion into former Soviet satellite states; the level of economic and political support for the breakaway Georgian provinces was seen to increase when the NATO backed Kosovo

[82] Andreas Hagen, "The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict" (The Armed Forces Communications and Electronics Association, May 24, 2012), 3, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

[83] "Russia's N.Ossetia Wants Unification with Georgia's S.Ossetia," Russian News Agency, *RIA Novosti*, May 20, 2008, http://en.ria.ru/world/20080520/107888655.html.

independence was declared and when Georgia was accepted for membership in that organization.[84] The conflict escalated from words to actions on August 7, 2008 when Georgian troops responded to bombardments by South Ossetian forces by entering the South Ossetian capital, to which the Russian military launched an overwhelming response in the physical domain, while patriotic Russian hackers launched attacks in cyber space to oppose the Georgian invasion.[85]

1. THE WORD

An interesting facet of this conflict were the actions of a proxy cyber militia to carry out a series of attacks which served to destabilize and degrade the Georgian Republics current operations, indirectly supporting the goals of Russia to destroy the republic's international stature and value to NATO. These cyber-attacks were the result of a long-term process of creating the proper atmosphere and conditions, all closely integrated with the messaging in support of Abkhazia and South Ossetia, backed by Russian forces, and their plans to solidify the breakaway regions in support of a "step-by-step" independence effort.[86] To add legitimacy to its involvement, Russia played on its close economic ties to the region and took steps to solidify its position by offering Russian citizenship to any former Soviet Union citizens, thus paving the way for future intercession on behalf of these Russian citizens.[87] Within the cyber domain this objective would require a long-term program to not only identify "hacktivists" that were friendly to the South Ossetian / Russian cause but to identify the means and methods of bringing the force of the cyber militia to bear. The message was designed to appeal to Russian nationalist supporters both within and outside of Russia, focusing on encouraging self-mobilization of the local Internet users by spreading "For our motherland, brothers!" or "Your country is calling you!" hacktivist messages across web forums.[88] The Russians

---

[84] Christian Lowe, "Russia Tightens Ties with Georgian Rebel Areas," *Reuters*, April 16, 2008, http://www.reuters.com/article/2008/04/16/us-russia-georgia-breakaway-idUSL164428920080416.

[85] Hagen, "Russo-Georgia War," 5.

[86] Lowe, "Russia Tightens Ties with Georgian Rebel Areas."

[87] Hagen, "Russo-Georgia War," 3.

[88] Dancho Danchev, "Coordinated Russia vs Georgia Cyber Attack in Progress."

also sought to enhance their position in the global energy markets, using the pretext of supporting the breakaway regions as means of degrading the legitimacy of the Georgian government and directly threatening their role as a competing source of energy.[89] To bring the conflict to a personal level, a messaging campaign was run concurrently that equated the president of the Georgian Republic, Mikheil Saakashvili, to Adolf Hitler.[90] Leading up to the actual conflict members of the cyber militia attempted to influence international public opinion regarding the struggle by manipulating non-scientific online polls on international news sites in an attempt to justify future Russia's actions as a peacekeeping intervention.[91] The effects of this campaign was the establishment of a nationalist Russian movement, the legitimization of their social, political, and economic ties with the breakaway regions, a favorable picture in the world press, and a blanket of villainy applied to the Georgian Republic and its leaders.

2. THE MESSENGER

As with most wars, this one began as a war of words. The message was initially disseminated to the target audience using traditional methods such as print journalism, but transitioned to chat rooms and web blogs as the call to action gained momentum. While the outcome being sought was clearly in favor of Russian interests, the Russian government took great pains to separate the message from the messenger. While not able to directly attribute the actions of the cyber militias to official government sanction, Project Grey Goose, an open source intelligence initiative to examine this conflict, hypothesized as to the true origins of the cyber-attack after examining the registration and hosting of the site stopgeorgia.ru, the site carrying the majority of the coordination, targeting, and specific hacking tools for this attack. Project Grey Goose was able to establish a geographic proximity, not a direct connection, between this site and the

---

[89] David Hollis, "Cyberwar Case Study Georgia 2008," Military, *Small Wars Journal*, 2011, 4, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[90] Kim Hart, "Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar," News, *Washington Post*, August 14, 2008, 2, http://articles.washingtonpost.com/2008-08-14/news/36876288_1_georgia-s-Internet-web-sites-cyberattacks.

[91] Hagen, "Russo-Georgia War," 10.

Russian GRU (equivalent to the U.S. NSA).[92] To further isolate the source of the messaging for the conflict they presented circumstantial evidence of connections between the Russian government and Russian youth organizations, including Nashi and United Russia, via a Russian media report "that has provided new evidence pointing to how the Russian government sponsors and pays leaders of Russian youth organizations to engage in Information Operations up to and including hacking to silence or suppress opposition groups."[93] The overall goal of the Russian government may have been to, either directly or indirectly, insure that there existed a focused cyber militia that understood their opponents center of gravity, and that the methods and techniques were identified and in place to employ these forces against a target and at a time of their choosing.[94] In the end, while there is no direct connection between the Russian government and the attacks, there is enough evidence to make it unlikely the Russians would be able to achieve the success that they were able to without direct coordination with the civilian nationalists militias that they were able to organize, equip, and employ as a proxy force without having to directly intercede or act in order to achieve its objectives.

3. THE DEED

It appears that that the attack preparation had been going on for some time and that online forums were used to coordinate the attacks providing target lists and details about target Georgian websites.[95] The overall objective of the attacks was to deny and disrupt information flows within Georgia, hoping that the isolation from information would serve to demoralize and disorient both the citizens and the leadership of Georgia.[96] The warning shots for conflict escalation may have been heard as early as July 20, with a

---

[92] "Project Grey Goose Phase II Report," Scribd, 15–19, accessed August 13, 2013, http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.

[93] Ibid., 21–22.

[94] Hollis, "Cyberwar Case Study Georgia 2008," 5.

[95] Brian Krebs, "Security Fix - Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," News, *Washington Post*, October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

[96] Hagen, "Russo-Georgia War," 6.

series of distributed denial of service attacks (DDoS) that were able to effectively shut down some Georgian websites.[97]

From an operational perspective, Russian hacker forums, websites, and chat rooms were planning and anticipating these attacks for several weeks, leading to reconnaissance and probing attacks that gradually increased in scope and complexity as the onset of the cyber and physical conflict drew closer.[98] Perhaps anticipating a retaliatory strike in response to the cyber-attacks on Georgia, the Russian-supported hacker militia also targeted their counterparts in the Georgian hacker community.[99] The principle command and control node for these attacks appears to have been a Russian hacker forum StopGeorgia.ru where there was an established hacker hierarchy that coordinated the targeting, training, and employment of the exploits used to attack the Georgian websites.[100] The attacks and tools had the same characteristics as those employed in the past by the Russian Business Network (RBN); indeed, in some cases the attackers used tools and actual botnets known to be under RBN's control. Further, the attacks appeared to have been staged and activated just prior to the launch of the Russian ground offensive.[101] A series of DDoS attacks against Georgian web-sites started a day before the ground campaign between Georgian and Russian military units engaged in physical conflict in South Ossetia. Logs of these attacks trace at least a portion of them back to servers located on the networks of Russian state-operated firms Rostelecom and Comstar.[102] The attackers accomplished their goals without the required volume of traffic to overload a service by targeting vulnerability in a built in feature of MySQL that

---

[97] John Markoff, "Before the Gunfire, Cyberattacks," *York Times*, August 13, 2008, sec. Technology, 1, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[98] Hollis, "Cyberwar Case Study Georgia 2008," 4.

[99] Ibid., 3.

[100] Krebs, "Security Fix - Report," 1.

[101] Markoff, "Before the Gunfire, Cyberattacks," 2.

[102] John Leyden, "Bear Prints Found on Georgian Cyber-Attacks," News, *The Register*, August 14, 2008, http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

allowed the attackers to overload the backend database servers that supported the websites.[103]

Three other programs known to have been used were used to overload servers with traffic, while a fourth was intended to add functionality to websites, but was altered to overload the computing capability of servers by requesting non-existent web pages.[104] This level of organization and planning allowed for ordinary Russian citizens to attack the Georgian government websites with the aid of programs distributed through friendly sites.[105] The emergence of sites like StopGeorgia.ru within hours of the ground conflict, the pre-existence of a detailed target list with known vulnerabilities, and the support of a large cyber militia prepared to execute the attacks shows a level of detail and planning that many believe would not be expected without coordination and instruction from the forces that were to conduct the ground assault.[106] Reports estimate a total of 54 websites in Georgia related to communications, finance, and the government, sites whose denial of availability would be beneficial to the overall Russian military campaign, were attacked by cyber militia elements within Russia that disrupted communication between the Georgian government and its citizens as well as the outside world.[107]

The immediate response was for the Georgian government to relocate its websites to hosting locations in the U.S. to work around the DDoS attacks, so that these government sites might be able to resume their role communicating and providing guidance internally and externally in this time of crisis.[108] Another, more potent, reason for the choice to relocate government web services to the U.S. may have been to deter further cyber-attacks against the sites hosted on U.S. soil to avoid the unintended

---

[103] Krebs, "Security Fix - Report," 2.

[104] Jeremy Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime," Technology, *Computerworld*, August 17, 2009, 2, http://www.computerworld.com/s/article/9136719 /Georgia_cyberattacks_linked_to_Russian_organized_crime?pageNumber=1.

[105] Joseph Menn, "Expert: Cyber-Attacks on Georgia websites Tied to Mob, Russian Government," LA Times, August 13, 2008, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

[106] Krebs, "Security Fix - Report," 2.

[107] Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime," 2.

[108] Dancho Danchev, "Coordinated Russia vs Georgia Cyber Attack in Progress," 1–9.

consequences of bringing the U.S. into the conflict.[109] While the impact of the cyber-attacks was devastating to the Georgian government's ability to respond to the Russian invasion, it could have been worse; destructive cyber-attacks against crucial infrastructure, accessible over the Internet were not carried out, leading some to believe that predetermined limits were in place on the cyber-attacks just as they were on the ground attacks.[110]

Attacks by the Russian cyber militia were integral to the effort to deny and degrade the Georgian government's ability to convey vital information, both internally and externally. Additionally, the overwhelming effects in the physical domain, including the ground invasion, naval blockade, and bombing around the oil pipeline, allowed the Russians to achieve their strategic objective of demonstrating the inability of the Georgian government to defend its sovereign territory in both the physical domain and cyberspace.[111] The benefit of the unofficial cyber militia in this conflict is undeniable. Using unskilled cyber partisans with simple cyber tools, these forces were able to decisively deny and disrupt key elements of Georgian government communication and infrastructure, and may have been able to do more.[112]

It appears that within the international community countries like China and Russia have identified the value of such cyber militias, whereas countries like the United State have yet to realize their potential.[113] The key to the success of this operation was the detailed efforts that went into enumerating the target environment, the identification of targets and vulnerabilities, the pre-packaging of malicious payloads, and the coordinated exploitation.[114] This operation was targeted in nature, based on the desired effects, and focused on isolating the key areas that the Russian military intended to attack. This had

---

[109] Ward Carroll, "Cyber War 2.0 — Russia v. Georgia," Defense Tech, 1, accessed December 17, 2013, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/.

[110] Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime," 2.

[111] Hollis, "Cyberwar Case Study Georgia 2008."

[112] Hagen, "Russo-Georgia War," 19.

[113] Ibid.

[114] Hollis, "Cyberwar Case Study Georgia 2008," 6.

the subsequent effect of providing indicators of impending attacks on key centers of gravity, hindering opposition response, denying command and control elements that are actively engaged in the conflict, and in a broader sense to create a sense of national helplessness because to the psychological effects of isolation.[115]

The Russo-Georgian conflict may not be the first incidence of a combination of attacks in the physical domain and cyberspace, but it is an excellent example of conducting a cyber-attack via a proxy force, the hallmark of unconventional warfare, in support of the larger strategic and operational objectives of a conventional force. The attacks by the cyber militia were critical to destabilizing the government of the Republic of Georgia, denying it access to its critical communications infrastructure, and allowing its opponents to control the perception of the conflict leading up to and during the actual conflict on the ground. While there is no direct attribution to the Russian government for the cyber-attacks, based on the complexity and coordination evident from the attacks, evidence indicates something more robust than an ad hoc community of nationalist hackers being involved. The Russians were able to leverage their significant advantage in kinetic forces and benefit from the actions of the cyber militia to decisively defeat the Georgians. The lessons to take away from this case, and for future research, include the benefits of both the murky attribution situation and of the simultaneous employment of cyber and kinetic weapons.

B. CASE 2: SYRIAN ELECTRONIC ARMY: CYBER MILITIA IN SUPPORT OF THE STATE

In this case we will examine the Syrian Electronic Army (SEA) and its role in the ongoing conflict between pro-Assad forces and opposition forces in Syria. We will examine the narrative that was the genesis of the conflict, how this narrative was employed to organize and empower a surrogate force, and then the actions and impact of the surrogate force in the conflict. This case will demonstrate how the Syrian Electronic Army employed cyber means as a surrogate force to support the Assad regime and its effort to resist internal and external forces seeking regime change. Some of the questions

[115] Ibid.

we seek to answer are: What was the popular message used to create the movement that spawned the surrogate force? How was the surrogate force recruited and empowered to carry out the cyber-attacks? What are the methods employed and the targets that this force attacked and to what effect? We will look at the available data and determine how the practices and effects might be leveraged for future SOF operations using cyber warfare in support of unconventional warfare.

1. THE WORD

With the rise of the networked society, the days of combatant forces conducting operations in the physical world alone has gone the way of the cavalry. This has been especially apparent with the Arab Spring popular resistance movements in the Middle East and North Africa, where protestors have exploited the asymmetric capabilities afforded to a weaker combatant by conducting operations in cyberspace against the states. While this has characterized the Syrian uprising as well, that conflict has also given rise to an open and organized pro-government cyber militia that is actively targeting internal and external opposition to the Assad regime.[116] This militia, which calls itself the Syrian Electronic Army (SEA), claims that it was launched in May of 2011 and is comprised of "a group of young people who love their country and have decided to fight back electronically against those who have attacked Syrian websites and those who are hostile to Syria."[117]

SEA repeatedly asserts that it is not an officially sanctioned organization, rather just an ad hoc group of enthusiasts that strike back against those who are attempting to destabilize Syria via cyber space.[118] In a speech on June 20, 2011, President Bashar al-Assad lauded the SEA as a "real army" operating in a virtual world. While SEA welcomed these comments, it also took great pains to reiterate that it was not affiliated

[116] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 1.

[117] Ibid.

[118] Ibid.

with any government organization.[119] Nevertheless, the SEA has taken a decidedly pro-regime stance, urging passive and active resistance against both forces inside Syria that are opposing the state as well as supporting cyber-attacks on individuals, groups, and web organizations that are seen as opposing the Assad regime.[120] This is a significant expansion of the scope of most cyber resistance movements, moving from defending one's own position to actively attacking not just people and organizations that oppose you, but in some cases the companies that produce software, for example Microsoft or mobile phone application developers, that is employed by those the movement opposes.[121]

The SEA was founded as a means for young Syrian computer enthusiasts to provide support in what they perceived as the ever increasing opposition to the Syrian government.[122] The group, whose lineage can be traced back to the Syrian Computer Society, an organization once headed by current Syrian President al-Assad, first emerged as an entity on Facebook in response to the dissident movement in Syria gaining momentum.[123] The group has an interesting relationship with Facebook; whenever a page has been identified as associated with the SEA, Facebook then moves to shut it down, triggering the migration of the organization to a new page in a perpetual cycle (see Figure 2).[124]

---

[119] Information Warfare Monitor, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets," June 25, 2011, 1, http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/.

[120] Sarah Fowler, "Who Is the Syrian Electronic Army?," *BBC*, April 25, 2013, 1, http://www.bbc.co.uk/news/world-middle-east-22287326.

[121] Information Warfare Monitor, "Syrian Electronic Army," 3.

[122] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 1.

[123] Ibid.

[124] Ibid., 2.

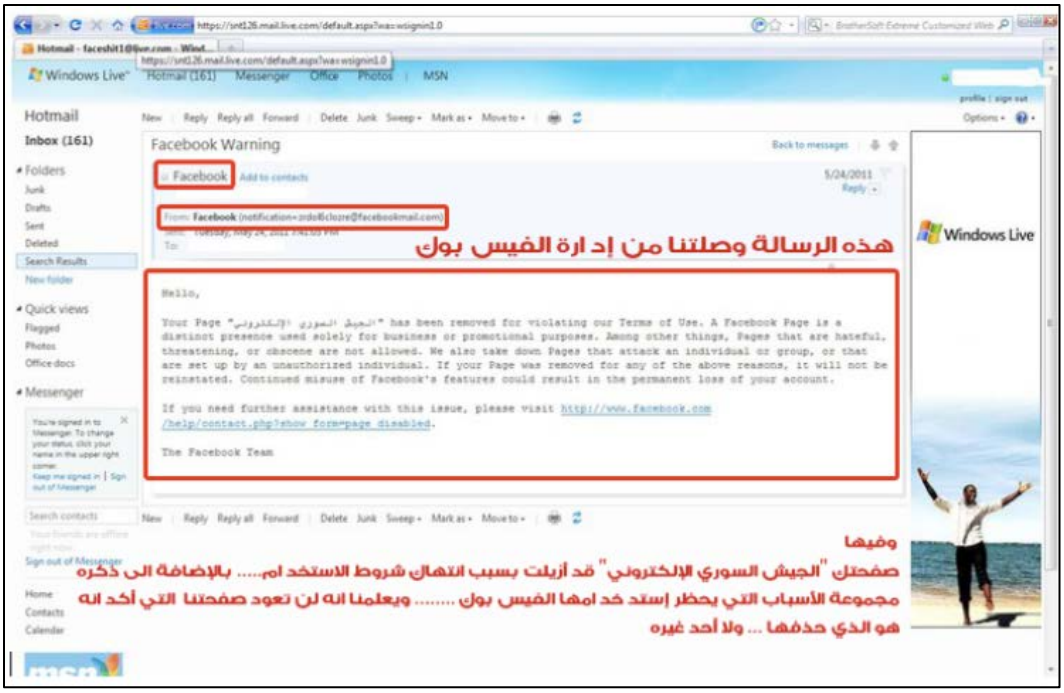

Figure 2. Screenshot of an alleged Facebook message sent to the Syrian Electronic Army notifying them of their page removal.[125]

There has been rising criticism within Syria for the perceived unfair practice of censoring SEA pages by Facebook without justification or notice, a practice that is not applied to Syrian opposition forces.[126] There appears to be an uneasy truce between the SEA and Facebook, as the SEA has been able to maintain an unpublicized page with the same information, and have more than eleven thousand members, since May 26, 2011.[127] This organization also maintains a presence on Twitter and YouTube that hosts before and after videos of targets, the reasons particular sites were targeted, and the messages that were left on the targets sites.[128]

[125] Ibid., 3.

[126] Ibid., 2.

[127] Ibid., 3.

[128] Ibid.

2. THE MESSENGER

The SEA began its early recruiting and organizing via Facebook pages and has been supported by a group calling itself "Syrian Hacker School" that is a repository for cyber tools, recruitment, training, and tactics, techniques and procedures (TTPs) for attacking vulnerable websites.[129] Then, with heavy reliance on social media platforms such as Facebook and Twitter, it organized and managed multiple spamming campaigns, as well as denial of service attacks, against targets they deemed as hostile to the Assad regime.[130] The group employs its own website to provide the latest details, both in English and Arabic. It offers accounts and screen captures of its latest success, as well as media clips from news outlets about its activities, allowing the organization to tout its successes, as a means to bolster support and to warn against opposition.[131]

While the Assad regime is afforded plausible deniability by its distance from the organization with regard to international opinion and international law, there is some evidence that there are close, if hidden, ties between the two groups. The SEA's original key members have all been replaced by a new organization that functions like the hacking collective Anonymous; this change is commonly believed to have resulted because of a leak of information deemed critical by the regime attributed to the SEA that put the group at odds with its benefactors.[132] Once this change of leadership happened, the Facebook accounts and hacker aliases that were being tracked for SEA disappeared and were replaced by a far less organized group of hackers that assumed the mantle of the SEA.[133] In addition to loose connections with the Syrian government, there are some equally vague connections between the SEA and Iranian hackers. While not definitive, they could

---

[129] Information Warfare Monitor, "Syrian Electronic Army," 2.

[130] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 3.

[131] Fowler, "Who Is the Syrian Electronic Army?," 2.

[132] Nicole Perlroth, "Hunting for Syrian Hackers' Chain of Command," Newspaper, *New York Times*, May 17, 2013, 2–3, http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html.

[133] Ibid., 3.

be indicative of collaboration between the two, but most likely are just an indicator of exploiting the ease of access afforded by the lack of security on the targeted sites.[134]

The SEA has received a tremendous amount of attention from the Syrian media, with articles ranging from those in support of the SEA, to those critical of Facebook for oppressing its sites.[135] This has led to the SEA creating its own internal library of select regional and international media coverage, with selective translation being employed to present the organization in a positive light and to exclude any sections critical of the SEA or the regime.[136]

3. THE DEED

When examining the deeds of the SEA, we will look at significant activities conducted in support of its goals, how it was able to accomplish these actions, and the effects that resulted from their actions. The primary objective of the SEA is the defacement of Syrian opposition websites, usually run by groups or individuals, via attack tools made available on the group's Facebook pages.[137] The exact vector being employed for their attacks is not known, only that it is referred to as a "widely available program" indicating that the SEA is not exploiting an unknown vulnerability via a "zero-day" or new method, but rather using an existing vector targeting a known vulnerability to accomplish their objective.[138] As of May 2011, the SEA claimed to have defaced over 50 websites, replacing the existing pages with temporary pages touting pro-regime messages of "truth," but not outright destroying the targeted websites (see Figure 3).[139]

---

[134] Information Warfare Monitor, "Syrian Electronic Army," 4.

[135] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 11.

[136] Ibid.

[137] Ibid., 3.

[138] Ibid.

[139] Ibid.

Figure 3. Syrian Electronic Army Facebook page announces that over 50 websites have been attacked, and that it did not destroy content of any of the websites.[140]

The second area of focus for the SEA is Western websites, to include government, media, groups, and individuals that it perceives as being either anti-Syria / Assad or as supporting the Syrian opposition (see Figure 4).[141]

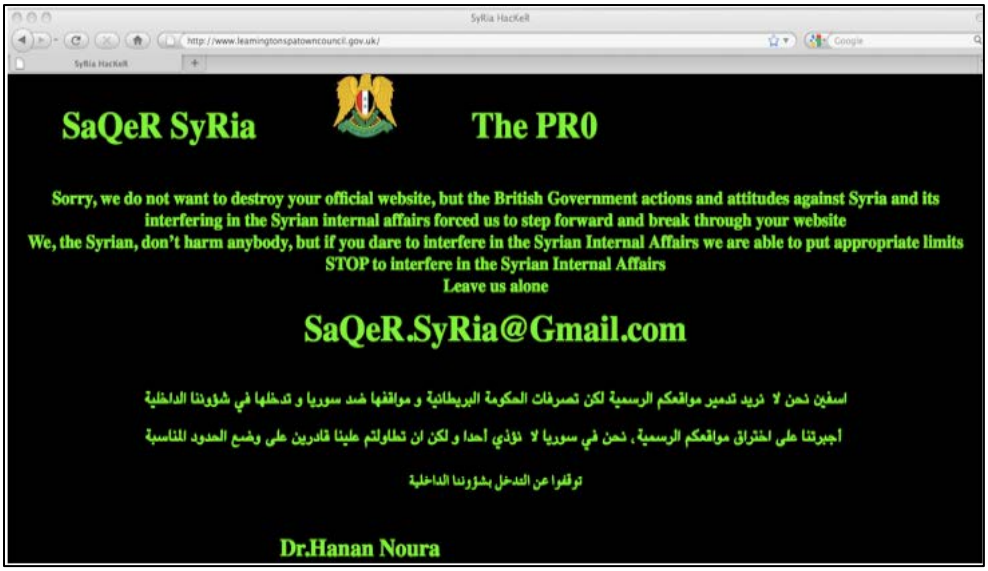

Figure 4. Screenshot of defaced website of Royal Leamington Spa Town Council at http://www.leamingtonspatowncouncil.gov.uk.[142]

[140] Ibid., 4.

[141] Fowler, "Who Is the Syrian Electronic Army?," 1.

[142] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 5.

Of note is that some of the Western websites have been targeted by the SEA not because of any outright activity by the site in question, but rather because of the actions of the countries within which the sites reside, presumably because the SEA was not able to target these offending countries directly.[143] Other theories as to why these sites were targeted include cases of mistaken identity, lack of understanding of the foreign countries language, pure mistakes, or because the targets were perceived as "soft" and therefore easy to exploit.[144] The SEA was able to conduct mass defacements via exploiting a single vulnerability on a shared webserver, where the redirect tag was injected into the target database rather than requiring the attackers to upload the SEA page on the target site (see Figure 5).[145]

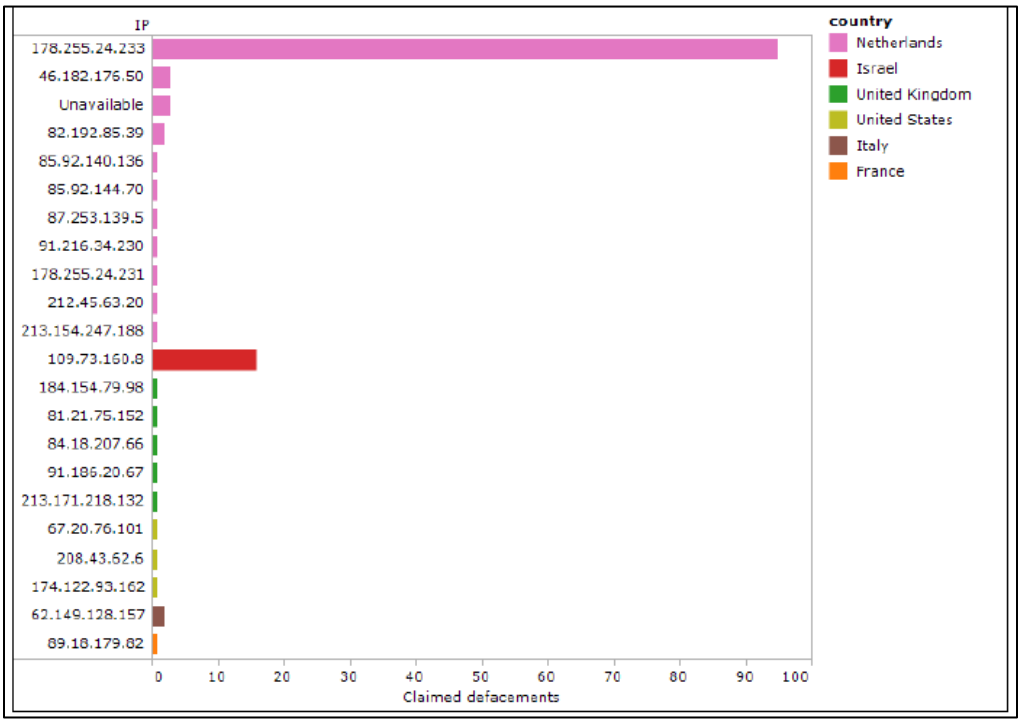

Figure 5. Claimed defacements by IP and country, May 16–June 19, 2011.

[143] Ibid.

[144] Ibid.

[145] Information Warfare Monitor, "Syrian Electronic Army," 3.

The SEA has been prolific in its attacks against Israeli government and tourist websites; however these sites were not targeted for any specific anti-Syria acts, but rather for the more traditional approach of attempts to "cleanse the web from Israeli websites that promote hatred towards the Palestinian people" (see Figure 6).[146]

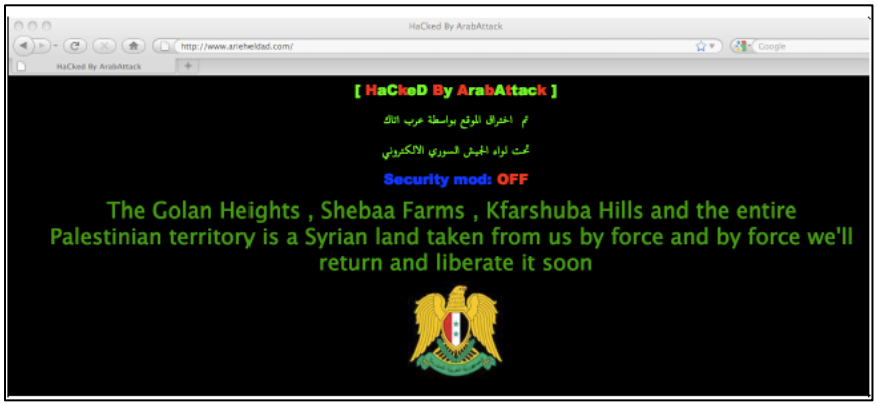

Figure 6. Screenshot of defaced website of Israeli Member of Knesset Arieh Eldad.[147]

These sites appeared to have been exploited via an HTML re-direct injection, but the underlying purpose for these attacks appears to not be a response to an anti-Assad or opposition position, but rather as a means of garnering media attention for the SEA, as was evidenced by the controlled manner in which the exploits were announced and publicized.[148] The SEA has also maintained a steady information campaign via posting repetitive comments on prominent public figures Facebook pages, both as spam attacks and to draw attention to itself and to protest the target's perceived support of the revolution in Syria (see Figure 7).[149]

[146] Ibid., 5.

[147] Ibid.

[148] Ibid., 6.

[149] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 7–8.

Figure 7. Syrian Electronic Army documents its "virtual demonstration" on U.S. President Barack Obama[150]

Recalling the definition we will use for unconventional cyber warfare (UCW) (to achieve military objectives or effects in or through cyberspace by, with, or through irregular forces in support of a resistance movement, an insurgency, or conventional military operations) the SEA provides a contemporary framework for employment of a cyber-militia in support of the State. The SEA organized, trained, equipped and mobilized in cyberspace, using social media both as its base of operations and its preferred battlefield. Arguments could be made that the SEA's effectiveness against internal threats was due to the support of the State-run media and network. Their ability to accomplish objectives against external targets demonstrates the low barrier to entry and the ease in which one can fight in cyberspace. While the SEA's targeting was not always optimal, it demonstrated that one need not employ cutting edge, or original threat

[150] Ibid., 8.

vectors to be successful contesting in cyber space. With the inherent vulnerabilities present in most software and hardware, target enumeration is one option to determine where to attack. However, these vulnerabilities make it possible to attack across a broad spectrum of cyberspace, in a version of cyber recon by fire. Either approach allows adversaries to identify vulnerabilities and exploit those vulnerabilities without the need for highly sophisticated forces. These existing vulnerabilities, the difficulty with attribution in cyberspace, and the low cost and technology threshold for cyber-attacks make this an ideal area to contest as part of a UCW campaign.

C. CASE 3: ANONYMOUS – NON-STATE ACTORS AS CYBER MILITIAS

Tunisia's president, Zine el-Abidine Ben Ali, had been in control for nearly 23 years, yet Tunisia was "the first nation in the Arab world to have its leader removed through a popular uprising of its citizens or, more precisely, 'netizens' thanks to Tunisia's modern communications infrastructure, pervasive Internet, and mobile phone network."[151] Although the use of information and communication technologies (ICTs) and social media has been credited with much of the success of the Jasmine Revolution and subsequent movements associated with the "Arab Spring," it does little to explain why these tools were effective.

1. BACKGROUND

Tunisia's secular government maintained close diplomatic relations with Europe and the U.S. The population experienced greater prosperity, better educational opportunities, and the women enjoyed more freedoms than in other Arab countries. Throughout Ben Ali's reign Tunisia had remained extremely stable, with no terrorism to speak of. However, Tunisia was not without its problems.[152] The Tunisian people were exposed to greater economic disparity, a growing demographic youth bulge, overt

[151] Jeffrey Carr, "In Tunisia, Cyberwar Precedes Revolution," *Forbes*, January 15, 2011, http://www.forbes.com/sites/jeffreycarr/2011/01/15/in-tunisia-cyberwar-precedes-revolution/.

[152] Naseema Noor, "Tunisia: The Revolution That Started It All | International Affairs Review," *International Affairs Review*, January 31, 2011, http://www.iar-gwu.org/node/257.

nepotism, and extensive government corruption all as a result of the Ben Ali regime's policies.

Tunisia's unemployment rate was between 13 and 16 percent.[153] Although this was greater than Egypt's, Libya's, and Algeria's unemployment rates at the time, Tunisia had experienced very little instability in comparison.[154] However, the unemployment rate of university graduates in Sidi Bouzid, where the Jasmine Revolution began, was between 25 and 30 percent.[155] The youth bulge, combined with greater accessibility to higher education, created a growing number of youths either unemployed or underemployed for the jobs available in the Tunisian economy. Corruption, and an increasing cost of living coupled with unemployment, and an underemployed workforce had already resulted in uprisings within the Gafsa mining basin in 2008.

Ben Ali had pledged to bring democracy and human rights to Tunisia early in his reign. Instead, he used the threat of radical Islamic movements to install and bolster his internal security apparatus, manipulate electoral processes, and co-opt officials. He was viewed as an authoritarian, but he was able to stabilize the country and bring tourism and investors into the country while keeping the Islamists out.[156] He had been so effective at controlling the country that there was no visible opposition to his regime at the time of the revolution. The regime participated in the censoring of media outlets, blocking the formation of civil organizations, and detaining and torturing thousands of dissidents.[157]

---

153 Christopher Alexander, "Tunisia's Protest Wave: Where It Comes from and What It Means," Blog, *Foreign Policy Blogs*, January 3, 2011, http://mideastafrica.foreignpolicy.com/posts/2011/01/02/tunisia_s_protest_wave_where_it_comes_from_and_what_it_means_for_ben_ali.

154 "Tunisia Unemployment Rate | Actual Value | Historical Data | Forecast," accessed March 10, 2014, http://www.tradingeconomics.com/tunisia/unemployment-rate; "Egypt Unemployment Rate | Actual Value | Historical Data | Forecast," *Trading Economics*, accessed March 10, 2014, http://www.tradingeconomics.com/egypt/unemployment-rate; "Libya Unemployment Rate | Actual Value | Historical Data | Forecast," *Trading Economics*, accessed March 10, 2014, http://www.tradingeconomics.com/libya/unemployment-rate; "Algeria Unemployment Rate | Actual Value | Historical Data | Forecast," *Trading Economics*, accessed March 10, 2014, http://www.tradingeconomics.com/algeria/unemployment-rate.

155 Alexander, "Tunisia's Protest Wave."

156 Ibid.

157 Noor, "Tunisia: The Revolution That Started It All | International Affairs Review."

However, his attempts to control Tunisia became less creative and more transparent as the growth of Facebook, Twitter, and the blogosphere helped to inform the population of news that was otherwise censored.[158]

Dissidents and political conspirators, who had long advanced the notion of nepotism and corruption within the Ben Ali regime, had managed to garner little international attention until candid dispatches from Robert Godec, the U.S. Ambassador to Tunisia, were revealed detailing the opulent lifestyle members of the Ben Ali family enjoyed along with the rampant corruption present within the regime.[159] The extent to which the leaking of U.S. State Department cables outlining the corruption and nepotism within the regime incited the revolution is debatable. However, it is undeniable the information within those documents had a psychological effect on the citizens of Tunisia. No longer were exiled bloggers and activists telling their story, but the U.S., a strong ally, appeared to share their concern.[160]

The Tunisian people were highly connected despite Ben Ali spending the greater part of 23 years constructing a pervasive state security apparatus that existed in both the virtual and physical space. Tunisia had a well-developed mobile phone and Internet infrastructure with nearly nine out of 10 Tunisians owning a mobile phone. Of those, 84 percent accessed the Internet at home through the state run ISP, the Tunisian Internet Agency. An additional 75 percent utilized the Internet at work and 24 percent relied on access to the Internet through public cafes.[161] In 2011, Tunisia, though one of Africa's smallest countries, had the fourth largest number of Facebook users on the continent

---

158 Alexander, "Tunisia's Protest Wave."

159 Nate Anderson, "Tweeting Tyrants Out of Tunisia: Global Internet at Its Best," *WIRED*, accessed March 7, 2014, http://www.wired.com/threatlevel/2011/01/tunisia/.

160 Sami Gharbia, "Chelsea Manning and the Arab Spring," *Nawaat*, February 24, 2014, http://nawaat.org/portail/2014/02/28/chelsea-manning-and-the-arab-spring/; Narnia Bohler-Muller and Charl Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent," *Africa Institute of South Africa, Policy Brief* 46 (2011): 1–8.

161 Brett Van Niekerk, Kiru Pillay, and Manoj Maharaj, "Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," *International Journal of Communications* 5 (2011): 1406–16.

along with the highest Internet penetration rate of any other African nation, 56.8 percent.[162]

However, penetration and connectivity had not equated to a free exchange of ideas or information. In the summer of 2010, digital activist, Global Voices and Readwriteweb contributor, Slim Amamou published a story exposing the Tunisian government's capabilities. Amamou outlined the Ben Ali regime's cyber capabilities including employing an estimated 600 cyber warriors and sophisticated DNS spoofing techniques utilized to obtain the username and passwords of Tunisians.[163] These techniques would later be put to wider use to target dissidents and activists as the intensity of the uprising spread and the regime clung desperately to power.

2. CHAIN OF EVENTS

Mohamed Bouazizi's suicide protest is credited as being the catalyst for the revolution in Sidi Bouzid, Tunisia. His actions on December 17, 2010, were in response to his frustration toward police actions taken against him, his inability to pay the bribe to recover his produce cart, and his governor's refusal to hear his complaint.[164] For weeks friends and residents in Sidi Bouzid staged demonstrations that led to the popular uprising resulting in the toppling of the Ben Ali regime.[165] Despite the undeniable impact of the images and news of Bouazizi's plight, which resulted in numerous copycat protests by individuals throughout the Middle East and Europe, it is necessary to begin our examination several months earlier in order to ascertain the impact of information and communication technologies (ICTs), and later Anonymous, within this revolution.

---

[162] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent."

[163] Fabrice Epelboin, "Revolution 2.0: Rebooting Tunisia," *ReadWriteWeb*, January 14, 2011, http://readwrite.com/2011/01/14/revolution_20_rebooting_tunisia; Yves Gonzalez-Quijano, "False Promises? The Social Media and Arab Political Change," *Media and Arab Transition*, 2013, 60–63.

[164] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent"; Noor, "Tunisia: The Revolution That Started It All | International Affairs Review."

[165] *Mohammed Bouazizi. A Tunisian Martyr*, 2011, http://www.youtube.com/watch?v=jHw_auqod6Y&feature=youtube_gdata_player.

Sami Ben Gharbia, a self-described Tunisian campaigner, blogger, writer, freedom of expression advocate, founding director of the advocacy arm of Global Voices, co-founder of nawaat.org, co-founder of the Arab Techies Collective, and co-organizer of the Arab Bloggers Conference, claims that PVT Manning's release of U.S. secrets to WikiLeaks had also played a part in starting the revolution.[166] Gharbia's exposure to those secrets began in October 2010. According to Gharbia, "This is what we were looking for during the last decade of strategizing and theorizing about citizen dissent media, diaspora media, exiled media, and digital activism: the ability to inform and transform. This was momentum."[167] Gharbia contacted associates with whom he had worked on building anti-censorship strategies and campaigns and training non-violent protest movements. They decided to publish TuniLeaks on 28 November 2010 to coincide with the release by WikiLeaks.[168]

The TuniLeak documents were to be released on google.appspot to enable Gharbia and his associates to change the IP addresses and negate the need for complex circumvention tools as Ben Ali's regime would inevitably blocked them. Al Jazeera also released the "Palestine Papers" around this time.[169] Once public, the documents were spread by a variety of means: as pdf. on Scribd, file sharing services, torrents, and on Facebook as images (spread further by Slacktivists). They were later passed on by CDs, thumb drives, and hard copies. Activists also began crowdsourcing the translation of many of the documents.[170]

The Ben Ali regime began to take action in an attempt to restore order as the demonstrations and protests spread. It undertook an enormous effort to begin phishing and spear phishing to gain control of activist's email and Facebook accounts in order to

---

[166] Gharbia, "Chelsea Manning and the Arab Spring."

[167] Ibid.

[168] Ibid.

[169] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent." 5.

[170] Gharbia, "Chelsea Manning and the Arab Spring."

delete content, accounts, and followers.[171] It also began blocking many of the websites involved with either spreading the leaked information or that were assisting the protestors to mobilize.[172] This prompted The Committee to Protect Journalists to send an open letter to the Tunisian government after learning local and international websites carrying news of the demonstrations in Tunisia had been blocked.[173] Growing frustrated, the Ben Ali regime eventually resorted to blocking social media sites and the Google App Engine IPs.[174] This evoked a response that Ethan Zuckerman has referred to as the "cute cat theory." The nearly 3.6 million Internet users of Tunisia, seeking only to use the Internet to "share pictures of cute cats," were affected by the Tunisian regime's attempt to censor the Internet. The result was a population previously politically uninterested in the ongoing protests that was transformed into one that mobilized against the censorship.[175] What occurred next drew the ire of the hacker group Anonymous. Fresh off of attacks in support of Operation Payback to protest anti-piracy companies, Anonymous had then taken aim at PayPal, MasterCard, and others as they withdrew support to WikiLeaks in the wake of the release of secret U.S. State Department cables. Anonymous' next logical target became the Ben Ali regime that had blocked access to the WikiLeaks website. #OPTUNISIA "began when one Anon began spamming the forum, drawing support from activists around the world."[176]

Generally, Anonymous' motivation for action revolves around the central theme of freedom of information. Although this was not always the case, the group appears to have undergone some type of cognitive liberation around 2008 when the Church of Scientology attempted to censor leaked videos and information that was meant for its

---

[171] Yasmine Ryan, "Tunisia's Bitter Cyberwar - Features - Al Jazeera English," News, *Al Jazeera*, January 6, 2011, http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html.

[172] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent."

[173] Anderson, "Tweeting Tyrants Out of Tunisia."

[174] Carr, "In Tunisia, Cyberwar Precedes Revolution"; Gharbia, "Chelsea Manning and the Arab Spring."

[175] *Ethan Zuckerman- Cute Cats and the Arab Spring: When Social Media Meet Social Change*, 2011, http://www.youtube.com/watch?v=tkDFVz_VL_I&feature=youtube_gdata_player.

[176] Ryan, "Tunisia's Bitter Cyberwar - Features - Al Jazeera English."

membership only. The resulting attacks by Anonymous were characterized by one participant as not much more than "ultra coordinated motherfuckary" until Mark Bunker, an outspoken critic of the church, began to call for greater political action from the group.[177] On February 10, 2008, Anonymous left the Internet and approximately 6,000 people showed up to protest at Church of Scientology locations around the world.[178]

As Anonymous mobilized on 4chan for Operation Payback in September 2010, targets were chosen and voted on, individuals worked collectively on documents to outline who were and who were not to be targeted by the group, and activists utilized Internet Relay Chat (IRC) to better coordinate their actions. It appeared that a greater social/global consciousness within Anonymous had begun to emerge along with the principles that would govern how members should act.[179]

On January 2, 2011, Anonymous launched #OPTUNISIA.[180] Anonymous members carried out DDoS attacks upon initiating #OPTUNISIA stating, "this is a warning to the Tunisian government. Any organization involved in censorship will be targeted and will not be released until the Tunisian government hears the claim for freedom to its people."[181] It managed to disable eight websites to include those of the president, prime minister, several ministries, and the stock exchange with the initial attack. Tunisia's state run ISP was also targeted.[182] Its efforts did not stop there. A call for greater activism on the part of Anonymous began as greater numbers of Tunisians came into contact with the members of Anonymous on the web. Anonymous funneled out

[177] Gabriella Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance," *The New Significance*, May 9, 2011, http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/.

[178] Ibid.

[179] Ibid.

[180] Ibid.

[181] Carr, "In Tunisia, Cyberwar Precedes Revolution."

[182] Ryan, "Tunisia's Bitter Cyberwar - Features - Al Jazeera English."

videos of street protests and regime violence, provided resources to Tunisian activists to secure their online activity, and even created packets for use by the Tunisian activists.[183]

As support to the protestors continued, so too did the regime's attempts to deny the opposition freedom of maneuver in the physical and virtual space. On January 6, 2011, Anonymous reported to Al Jazeera that its own site was under DDoS attack, but vowed to continue to DDoS that DNS server until after that day's strike by the labor and lawyer unions.[184] The regime continued to inject additional javascript into websites in order to obtain passwords and usernames of protestors, political activists, reporters, and bloggers. On January 7, 2011, Reporters Without Borders confirmed five cases of bloggers and online activists being arrested by the regime.[185] One of those detained was Global Voices and ReadWriteWeb France contributor, Slim Amamou.[186] The Electronic Frontier Foundation published a "greasemonkey" script on January 11, 2011, to strip away the additional coding, which had been emplaced by the regime, from websites for activist activities.[187] In one last effort to retain power, Ben Ali announced an end to all net censorship and released all the remaining bloggers from custody on January 13, 2011. The following day, January 14, 2011, Ben Ali left the country.[188]

Would all this have been possible without Anonymous, the Internet, mobile phones, traditional media, and social media? Rim Nour, a hacktivist who personally participated in the Jasmine Revolution, seems to believe so. Nour stated that, "the 2010 Tunisian revolution was not a Wikileaks or Facebook or (a) Twitter revolution, but an uprising fundamentally powered by people and the socio-political and economic conditions of their lives."[189] Nour goes on to acknowledge the importance of the role

---

[183] Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance";" Ryan, "Tunisia's Bitter Cyberwar - Features - Al Jazeera English."

[184] Ryan, "Tunisia's Bitter Cyberwar - Features - Al Jazeera English."

[185] Anderson, "Tweeting Tyrants Out of Tunisia."

[186] Gonzalez-Quijano, "False Promises? The Social Media and Arab Political Change."

[187] Anderson, "Tweeting Tyrants Out of Tunisia."

[188] Epelboin, "Revolution 2.0."

[189] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent.,"5.

ICTs and the traditional media played in the revolution, but maintains the revolution "would have happened without social media, but not as fast."[190] Clay Shirky and Malcolm Gladwell have further supported the notion that social media tools are by themselves ineffective due to the state's increasing ability to monitor them and that weak ties created amongst casual participants on social media cannot bring about any useful action.[191]

The uprisings in the Gafsa mining basin occurred only two years prior, in the cities of Redeyef, Moularès, M'dhila, and Metlaoui, and shared many of the same concerns that mobilized people for the Jasmine Revolution. There was a large economic gap between the region and the rest of the country, massive unemployment, underemployment, corruption, nepotism, and perceived social injustices just as there was Sidi Bouzid. The unrest in Gafsa served as a catalyst for a variety people and civil society organizations to begin to coalesce; connecting "bread and butter" grievances to larger rule of law concerns.[192] However, the protestors in the Gafsa mining basin were ultimately unsuccessful because they were unable to move beyond a local protest movement and resist the Ben Ali regime's repressive response.[193] What differs in the instance of the Jasmine Revolution were the several external influences present, such as TuniLeaks, WikiLeaks, Anonymous, diaspora and dissident media, social media, and ICTs, that were all leveraged to alter the scale of the conflict.

[190] Ibid., 5.

[191] Ibid.

[192] Eric Gobe, "The Gafsa Mining Basin between Riots and a Social Movement: Meaning and Significance of a Protest Movement in Ben Ali's Tunisia," January 20, 2011, http://halshs.archives-ouvertes.fr/halshs-00557826/; Alexander, "Tunisia's Protest Wave."

[193] Gobe, be, Gafsa Mining Basin between Riots and a Social Movement.e

3. CONCLUSION

Does this case further perpetuate the "False Promise" myth that argues as Internet activism gains visibility in public spaces it becomes a part of the larger political game and that due to the political naiveté of the activists involved they are relegated to subordinate roles by the more politically astute?[194] The Union of Unemployed Graduates from Tunis University managed to enlist the assistance of trade union leaders in Redeyef to support the continued mobilization of protestors. However, it was these leaders from Redeyef who formed the core of the negotiating committee and marginalized the younger, more inexperienced organizers from the Union of Unemployed Graduates in an attempt to secure their own interests within the bureaucracy.[195] Conversely, the Internet activism and protests that played out in the events leading up to and during the Jasmine Revolution demonstrate that although the Internet activists were just as vulnerable to being subjugated by the more politically shrewd, the "False Promise" myth may be just that, a myth. Activists may avoid falling victim to the "False Promise" if they understand the role of information warfare and the supporting technologies to further their objectives.

The Jasmine Revolution offers four primary lessons for conducting cyber operations in support of revolutionary movements: 1) It establishes the importance of information and communication technologies (ICTs), 2) external support via cyber means, 3) the usefulness of the narrative to attract vital external support, and 4) the value of recognizable dissident and diaspora media with an established reputation to compliment the movement's physical operations, counter a regime's attempts to isolate and subdue the revolution, both virtually and physically, and affect the ouster of a regime. These tactics were used to varying degrees throughout the "Arab Spring." The diffusion of these techniques to other movements illustrates the importance of understanding why the tools of information warfare worked in one instance but not in another.

---

[194] Gonzalez-Quijano, "False Promises? The Social Media and Arab Political Change."

[195] Gobe, behe Gafsa Mining Basin between Riots and a Social Movement.m

As a dimension of socio-political activism, ICTs provided an "immediacy of audience access" that enabled the movement to disseminate information in order to alter the perceptions and the will of both the local and international communities, provide the ability to coordinate and mobilize, and conduct psychological and command and control warfare against the regime.[196] In an interview with a British journalist, Ben Ali's propaganda minister, Oussama Romdhani, "confessed that 'TuniLeaks was the coup de grace, the thing that broke the Ben Ali system'. The regime never understood that blocking websites doesn't block information."[197] The actions of the regime toward the ICTs, specifically the Internet, demonstrated the importance of Ethan Zuckerman's cute cat theory and how embedding the movement within benign spaces on the web can protect it from coercive measures taken by the regime.

Anonymous referred to its interventions in Tunisia, and subsequent operations, as "new activism."[198] This illustrated potential of technology to influence the socio-political climate has emboldened its users. Some have claimed that "Anonymous has proven to be a mature political entity" and has grown into a sort of "global consciousness."[199] Anonymous appears to have remained more pragmatic with its approach and understands the limitations of its capabilities based upon statements contained within software packets provided to Tunisian activists:

> (T)his is your revolution, you must hit the streets or you will lose, always stay safe, once you got (sic) arrested you cannot do anything for yourself or your people. Your government is watching you[200]

The multi-modal warfare exhibited during this movement of DDoS attacks in support of protests and demonstrations, supplying news, video, and images to media and

---

[196] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent";" Van Niekerk, Pillay, and Maharaj, "Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," 14.

[197] Gharbia, "Chelsea Manning and the Arab Spring."

[198] Bohler-Muller and Van der Merwe, "The Potential of Social Media to Influence Socio-Political Change on the African Continent."

[199] Epelboin, "Revolution 2.0."

[200] Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance."

international organizations beyond the country's borders, and delivering the knowledge and resources to activists in order to remain beyond the regime's reach in cyberspace demonstrate how vital external cyber support is.

In Tunisia, the establishment of external cyber support occurred mostly by chance. Anonymous' initial intervention was under the premise of protesting the regime's censorship policy. However, the interaction between the Tunisian activists and Anonymous point to how the role of Anonymous evolved as their collective consciousness grew to become more aware of the plight of the Tunisian citizens. In Egypt, Anonymous attacked Morsy for his "lack of care about the core values of democracy…"[201] Anonymous targeted the Algerian government in response to human rights violations and repression of its citizens.[202] The ability of movements, through the frame alignment process, to garner greater support from Anonymous suggests that it is beneficial to analyze what messages could be used in order to attract groups such as Anonymous to provide the necessary external support to movements in authoritarian countries. It is also worth mentioning that cyber activism presents many people a way to engage in political action that previously did not exist.[203]

Last, it is important to recognize the value of established dissident and diaspora media with a proven reputation. Bloggers, reporters, and activists with a known penchant for reporting the truth can assist in gathering information and disseminating news to international media outlets, garnering external support as an intermediary, and, with a large audience, can influence the direction of the movement. A new Twitter handle or Facebook page would likely not have the same impact of an already established blogger or activist might have. Such was the case with Slim Amamou, "Slim was at the crossroad of a movement that could be mobilized and ready to fight in just a click."[204] Slim was a recognized personality who had been in public opposition to the Ben Ali regime for some

---

[201] Anderson, "Anonymous Threatens Morsy with Cyberwarfare."

[202] "List of Targets of Arrested Computer Hackers," *Phys.org*, March 6, 2012, http://phys.org/news/2012-03-hackers.html.

[203] Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance."

[204] Epelboin, "Revolution 2.0."

time prior to the revolution and was eventually detained during the uprising. Upon his release, he was appointed to the interim government. Although he later resigned, Slim's experience points to the importance of a movement having individuals that can influence the movement before, during, and after the regime has been overthrown.[205]

[205] Gonzalez-Quijano, "False Promises? The Social Media and Arab Political Change," 62.

THIS PAGE INTENTIONALLY LEFT BLANK

V. UNCONVENTIONAL CYBER WARFARE: A THEORETICAL FRAMEWORK

As stated earlier, the aim of this thesis is to assist planners in determining whether and how cyber warfare can support a UW campaign. In this chapter, we will first offer observations and recommendations regarding conditions that may be favorable to employing UCW. Then, utilizing FM 3-05-130 as a reference, along with the seven phases of unconventional warfare contained therein, we will provide a means to categorize and exercise lessons learned from the case studies involving Russia, Syria, and Tunisia to develop a UCW theoretical framework. Doing so will highlight the applicability of UCW to support or counter insurgencies, resistance movements, and conventional military operations.

A. WHEN TO EMPLOY UCW

This section will discuss characteristics that may assist planners in identifying opportunities to further demonstrate the potential of UCW. It complements the following section, which will discuss the employment of UCW within the framework of current, traditional UW phases.

The following charts are used to identify the most connected / highest penetrated societies by ICTs as well as those countries that are most censored. The assumption is that a society with high level of Internet and mobile phone penetration is also highly connected and reliant on ICTs. Logically, it would seem that a highly connected yet highly repressive or closed society would be especially suitable to utilize UCW in support of U.S. strategic interests due to the difficult environment the U.S. would face in conducting a traditional UW campaign.

Table 1 depicts the top 20 countries of mobile phones per 100 people. Table 2 lists the top 20 countries by number of Internet users per 100 people.

Rank	Country or region	Number of mobile phones	Population	Phones per 100 citizens
64	Panama	6,900,000	3,405,813	202.5
47	Hong Kong	13,264,896	7,008,900[57]	187.9
39	Saudi Arabia	46,000,000	27,137,000	169.5
61	Lithuania	4,940,000	2,955,986[67]	167.1
05	Russia	256,116,000	142,905,200[10]	155.5
59	Estonia	1,982,000	1,340,602	147.8
15	Italy	88,580,000	60,090,400	147.4
54	Singapore	8.063,000	5,312,400	143.5
25	Argentina	56,725,200	40,134,425	141.34
52	Bulgaria	10,655,000	7,600,000	140.2
50	United Arab Emirates	11,540,040	8,264,070	139.6
04	Brazil	273,583,000	201,032,714[10]	136.45
38	Australia	30,200,000[47]	22,700,000[48]	133.0
11	Germany	107,000,000	81,882,342	130.1
13	Iran	96,165,000	73,973,000	130
53	Israel	9,319,000	7,310,000	127.5
46	Portugal	13,400,000	10,562,178	126.87
55	Denmark	7,000,000	5,543,819	126.2
22	Ukraine	57,505,555	45,579,904	126.0
26	Poland	47,153,200	38,186,860[36]	123.48

Table 1. Top 20 countries of mobile phones per 100 people[206]

[206] "List of Countries by Number of Mobile Phones in Use," *Wikipedia, the Free Encyclopedia*, April 23, 2014, http://en.wikipedia.org/w/index.php?title=List_of_countries_by_number_of_mobile_phones_in_use&oldid=605471188.

Country name	2009	2010	2011	2012
Iceland	93.0	93.4	94.8	96.2
Norway	92.1	93.4	94.0	95.0
Sweden	91.0	90.0	94.0	94.0
Netherlands	89.6	90.7	92.3	93.0
Denmark	86.8	88.7	90.0	93.0
Luxembourg	87.3	90.6	90.9	92.0
Bermuda	83.3	84.2	88.3	91.3
Finland	82.5	86.9	89.4	91.0
New Zealand	79.7	83.0	86.0	89.5
Liechtenstein	75.0	80.0	85.0	89.4
Qatar	53.1	81.6	86.2	88.1
Bahrain	53.0	55.0	77.0	88.0
United Kingdom	83.6	85.0	86.8	87.0
Monaco	70.1	75.0	80.3	87.0
Canada	80.3	80.3	83.0	86.8
Andorra	78.5	81.0	81.0	86.4
Faeroe Islands	75.2	75.2	80.7	85.3
Switzerland	81.3	83.9	85.2	85.2
United Arab Emirates	64.0	68.0	78.0	85.0
Korea, Rep.	81.6	83.7	83.8	84.1

Table 2. Top 20 countries by number of Internet users per 100 people[207]

Citing sources from FreedomHouse.org and the Committee to Protect Journalists, we have identified some of the most repressive countries in the world. These are shown in Table 3 (the "PR" stands for political rights and "CL" for civil liberties, with 1 being the best score and 7 the worst) and Table 4.

207 "Internet Users (per 100 People)," Non-Profit, *The World Bank*, 2012, http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?order=wbapi_data_value_2012%20wbapi_data_value%20wbapi_data_value-last&sort=desc&display=default.

Country	PR	CL	Combined Average Rating	Freedom Status
Belarus	7	6	6.5	Not Free
Burma	7	6 ▲	6.5	Not Free
Chad	7	6	6.5	Not Free
China	7	6	6.5	Not Free
Cuba	7	6	6.5	Not Free
Equatorial Guinea	7	7	7	Not Free
Eritrea	7	7	7	Not Free
Laos	7	6	6.5	Not Free
Libya	7	6 ▲	6.5	Not Free
North Korea	7	7	7	Not Free
Saudi Arabia	7	7 ▼	7	Not Free
Somalia	7	7	7	Not Free
Sudan	7	7	7	Not Free
Syria	7	7 ▼	7	Not Free
Turkmenistan	7	7	7	Not Free
Uzbekistan	7	7	7	Not Free

Table 3. The most repressive countries in the world[208]

Table 4. Map of the Top 10 most censored countries[209]

[208] "Worst of the Worst 2012: The World's Most Repressive Societies," Independent Watchdog, *Freedom House*, 2012, http://www.freedomhouse.org/report/special-reports/worst-worst-2012-worlds-most-repressive-societies#.U2v5-vldViM.

After cross-referencing the proceeding charts for countries that are both highly connected and highly repressive we find that only Saudi Arabia and Iran meet both criteria set forth by the assumptions. However, what is not mentioned are other contributing factors that would facilitate successful UCW efforts: the numbers of dissident and diaspora media and bloggers capable of influencing, transmitting, or otherwise assisting in a UCW campaign, underlying inter and intrastate tensions, and existing grievances between the population and government. Kirk Duncan provides additional thoughts on which environments may be more favorable than others to achieve success in UCW in his thesis, "Assessing the use of Social Media in Revolutionary Environment."[210]

While the initial assumptions and data only provide us with two countries that meet the criteria for both high rates of mobile phone and Internet penetration as well as a highly repressive regime, Iran and Saudi Arabia, we feel that this is misleading. If we examine the data related to the countries in our case studies, namely Syria, Russia, Georgia, and Tunisia, it becomes apparent that there are opportunities for the use of UCW regardless of how connected or closed a society is. According to worldbank.org, in 2007 Georgia's Internet penetration rate was slightly above eight percent and in 2008 had only risen to 10 percent.[211] Despite this, the case of Russia versus Georgia demonstrates that cyber-attacks against even a minimally connected country can have dramatic effects, especially when supported by conventional military operations and limited strategic objectives. Freedomhouse.org reported that in 2009 Tunisia's Internet penetration rate was around 34 percent.[212] This figure seems counterintuitive and fails to address a number of things including the preexisting physical networks from the Gafsa Mining Basin uprisings, growing internal grievances, smart phone penetration, and external

---

[209] "10 Most Censored Countries," *Committee to Protect Journalists*, accessed April 25, 2014, http://cpj.org/reports/2012/05/10-most-censored-countries.php.

[210] Kirk A. Duncan, "Assessing the Use of Social Media in a Revolutionary Environment" (Naval Postgraduate School, 2013), http://calhoun.nps.edu/public/handle/10945/34660.

[211] "Internet Users (per 100 People)."

[212] "Freedom on the Net: Tunisia," Independent Watchdog, *Freedom House*, 2011, http://www.freedomhouse.org/report/freedom-net/2011/tunisia#.U2murcepqwM.

support from Anonymous received by the revolutionaries during the uprising. Lastly, internetworldstats.com reports Syria has a nearly 23 percent Internet penetration rate.[213] Assad's ability to remain in power and counter the numerous factions that are pitted against him with the assistance of the SEA again demonstrates that the number of Internet users within the target country is not the only factor to consider when deciding whether or not to conduct a UCW campaign.

Given the relatively low percentage of connectivity within each of these countries allows us to conclude that the penetration rates of ICTs are not as important as one may have previously thought. Rather, other factors including social media platform use, government censorship and surveillance protocols, circumvention tools, narratives, key influencers, grievances, target selection, etc., all play a role in determining how and when to apply UCW in pursuit of U.S. objectives.

B. UCW FRAMEWORK

Before discussing the seven phases, we discuss three overarching concerns that are evident throughout the analysis of the case studies, UCW, and the 7 phases of UW. These concerns are risk, cost, and flexibility. Addressing these first will provide background for their mention within the phases to which they apply.

The topic of risk encompasses the domains of political risk, risk to mission, and risk to men; UCW seeks to mitigate all these. Reducing the ability of target governments to attribute UW operations, via cyber, to the U.S. can lessen the associated political risk involved with its application. Political risk is further mitigated by the target government's inability to attribute cyber activity with any relative certainty. This decreases the likelihood of retribution, avoids international legal issues involving the violation of States' sovereignty, and further reduces potential political damage incurred by an unpopular or unsuccessful operation. These factors may increase the attractiveness of

[213] Internet World Stats, "Internet World Stats: Usage and Population Statistics, Internet Users in the Middle East and the World - June 30, 2012," *Internet World Stats: Usage and Population Statistics*, June 30, 2012, http://www.internetworldstats.com/stats5.htm.

U.S. assistance to an insurgency that might otherwise be resistant to U.S. aid, providing a greater level of deniability to the supported movement.

We also judge that the application of UCW can greatly reduce the risk to mission. UCW may be applied across the spectrum from soft power to hard power by providing planners and operators with the ability to turn on and off support, increase or decrease aid, precision target, tailor effects to the operational requirement, and reduce the exposure of operators to the target regime. The applicability of UCW across the spectrum enables planners to provide solutions and responses that are measured and scalable to achieve U.S. strategic interests and objectives, which may not be achievable through traditional methods alone.

The preferred application of UCW to conventional UW is apparent when discussing its advantages with respect to the risk associated to personnel. The application and conduct of UCW provides operators the distance necessary to eliminate or greatly reduce life-threatening risk, as previously discussed in the ethical use of UCW. However, the use of UCW not only reduces risk to U.S. personnel but also to resistance and insurgent forces operating against the target regime by providing a layer of anonymity in cyberspace. Similarly, UCW can mitigate risks to the target in the form of minimizing collateral damage, civilian risk, risk to U.S. forces, and risk to proxy forces supporting conventional military operations. These reduced risks may also result in reduced costs and increased stability during transition.

UCW, with its low associated costs, may become even more appealing in the future to decision makers as the U.S. enters into an era of greater fiscal constraints. Here, cost refers to the monetary assistance required to support an unconventional warfare operation as well as the cost of reconstruction efforts provided to countries that have been the target of traditional conventional military operations (CMO). For years, planners have assumed that support to insurgencies called for the U.S. to provide guns and money to achieve desired end states. We argue that not only does UCW reduce the reliance and need to supply guns and money to a resistance, but the traditional logistics tail associated with an unconventional warfare operation is also greatly reduced with the application of UCW.

Lastly, UCW provides planners and operators flexibility in terms of measured responses and applications. Cyber may enable simultaneous operations to occur throughout the UWOA, ranging from overt to covert or clandestine, with anonymity provided by operating in the virtual as opposed to the physical space. Multiple supporting operations may be occurring within the UWOA spanning the spectrum from overt to clandestine, offering the operator the ability to choose to apply hard or soft power as the mission dictates, yet retain ample flexibility by remaining compartmentalized. Cyber also enables operations to be conducted as broadly, as narrowly, or as specialized as required by the mission.

The following sections will discuss the seven phases of unconventional warfare, what is commonly expected to occur during these phases, where we see UCW's application to each phase either to augment a UW campaign or as a standalone option, and draw upon relevant examples from the previously described case studies.

1. PREPARATION

Three general processes occur during the traditional Preparation Phase, Phase 1: intelligence preparation of the environment (IPOE), war planning, and shaping operations. Phase 1 can occur globally and continuously in order to set conditions favorable for the conduct of UW. All elements of national power, diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL), can be used in addition to preparation of the environment (PE) activities to further shape the environment locally, regionally, and globally.[214] Utilizing UCW, cyber capabilities may enable operators to conduct PE remotely, continuously, and globally from the micro to macro level without attribution, or without violating physically the sovereignty of the target state. In an effort to provide methods of employment to planners considering the use of UCW, we propose three approaches that draw on similarities found in the preceding case studies as suggestions for possible use in future operations.

[214] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*.

The first approach suggests that we build the infrastructure to be used for future operations. This method is similar to the one utilized in the case of Russia versus Georgia where the emergence of sites like StopGeorgia.ru occurred within hours of the ground conflict and the existence of a predetermined target list that detailed the known vulnerabilities allowed a large cyber militia to remain hidden until the specific moment they were called on to execute the intended attacks.[215] The next tactic would be to utilize an already existing organization complete with organic infrastructure and personnel that may be repurposed to support operations. This approach draws on similarities from the Syrian Electronic Army case study. The SEA traces its lineage back to the Syrian Computer Society, and as a cyber-militia, began conducting operations in support of the state's government when the dissident movement in Syria began gaining momentum.[216] Lastly, we advocate for an approach that would require identifying, infiltrating, and/or influencing an existing organization and infrastructure that exists with limited purpose but is malleable enough for the formation of new goals and purposes that would be in line with U.S. objectives. Or, in the most likely case, the goal, or purpose, of the group may be re-tasked, influenced, or otherwise morphed to meet the demands of the fluid UW environment. Similar actions occurred with Anonymous as their original reason for involvement in Tunisia began in response to Ben Ali's censorship of WikiLeaks, but transformed to supplying active assistance to the resistance and coordinating attacks in the virtual space to aid in demonstrations in the physical space as it came into contact with greater numbers of Tunisian activists.[217]

2. INITIAL CONTACT

Initial contact, or Phase 2, occurs when a pilot team makes physical contact with a resistance element within the unconventional warfare operational area (UWOA). The pilot team then assesses the viability of conducting UW within the UWOA, the

---

[215] Krebs, "Security Fix - Report," 2.

[216] Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East," 1.

[217] Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance."

compatibility of U.S. and local interests and objectives, as well as arranges for the reception of initial assistance and ARSOF units.[218]

Initial contact conducted within the construct of a UCW campaign offers several advantages including the previously discussed ethical, fiscal, and political reasons favoring the use of cyber in UW. Phase 2 operations conducted within the unconventional cyber warfare operational area (UCWOA) favors operators by providing an inherent clandestine and covert capability central to the facet of non-attribution associated with operating in cyberspace. This fundamental characteristic of cyber lends itself to two important notions regarding the assessment of the feasibility to conduct UW within the UWOA.

First, the compatibility of U.S. and local interests and objectives may align more closely within the UCWOA as the apparent lack of sponsorship or attribution may create a more politically feasible climate for insurgent or resistance leaders to act in a manner that is more favorable to U.S. strategic interests and objectives than may otherwise permit with the presence of actual forces operating within the UWOA.

Conversely, initial contact within the UCWOA may allow the U.S. to determine more quickly and accurately that an insurgent or resistance leader is less likely, or more resistant, to act in the interest of U.S. strategic objectives thus enabling the U.S. to back out of negotiations and withdraw support with less exposure and risk than may be feasible with the presence of U.S. forces on the ground in the UWOA. This would also enable the U.S. to begin assessing other leaders more rapidly to counter any movement gaining momentum that does not align with U.S. strategic interests.

Second, the technical capabilities and competencies of the resistance or insurgent forces may be assessed to a greater degree than in a traditional phase 2 operations. Doing so may lead to a higher degree of assurance that operations within the UCWOA are feasible, thus affording the U.S. a greater chance of achieving its goals and objectives.

[218] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*.

These concepts were apparent within each case study to a varying degree; significant is that during this phase each case shows how the command and control of the cyber militias had as thorough of an understanding of the effects that they could wield via their forces as they did of their opponent's capabilities that they wanted to mitigate. Although Egypt is not part of the case studies, the aftermath of its revolution has proven to be an example where a better assessment of who, or which groups, aligned more closely with U.S. strategic interests would have been beneficial and could have been conducted within the cyber realm. Egypt represented an opportunity to identify other groups that may have served to counter the Muslim Brotherhood and also align more closely with U.S. interests.

3. INFILTRATION

Infiltration, or Phase 3, simply denotes the phase of the campaign in which ARSOF units infiltrate the UWOA and, the unit, or units, merely linkup with the pilot team and the irregular force. If they are unable to contact the irregular force, they continue the area assessment begun by the pilot team in order to confirm or deny their findings.[219] Traditional UW Phase 3 entails risk of discovery and compromise to the UW practitioner.

Cyber's speed and control favor the use of UCW within the infiltration phase. The presence of existing cyber infrastructure and personnel can enable infiltrations to be initiated and performed quickly, allowing the application of force, the Employment Phase, to occur much earlier than in a traditional UW effort. This was apparent in the case studies as the Russians sought to exploit tools and actual botnets known to be under the control of the Russian Business Network (RBN) to quickly bring cyber forces to bear to coincide with the launch of the Russian ground offensive.[220]

Cyberspace also affords a degree of control not normally experienced in traditional UW as operations can be initiated and aborted with relative ease and with

[219] Ibid.

[220] Markoff, "Before the Gunfire, Cyberattacks," 2.

minimal risk. During the Russian/Georgian conflict malicious packets were pre-packaged as malicious payloads, employing easy to follow instructions and simple attack tools, which allowed unskilled cyber partisans to conduct coordinated exploitation across the broad spectrum of the cyber domain.[221]

4. ORGANIZATION

Organization, or Phase 4, encompasses the development of a capable, irregular force, to include an auxiliary, underground, guerrilla force, and area command structure.[222] For practitioners operating within the traditional UW framework, Phase 4 demands a majority of attention given the complexity of organizing disparate groups to accomplish specific objectives as well as balancing the inherent constraints of risks, costs, and time.

The advantages of cyber within Phase 4 include greater flexibility in terms of developing organizations that are required to accomplish specific objectives and the clandestine method in which these organizations may be built. As noted in the discussion of Phase 1, UCW is not bound by the traditional UW organizational structures and although it may be useful to think of diaspora media and dissident bloggers as an underground and auxiliary, hackers and hacktivists as a guerrilla force, and influential persons within cyberspace as area commanders, it is not necessary, nor always conducive to thinking in an unconventional manner, to do so.

In a UCW environment planners may choose to develop one or more of the previously described UCW models to meet the needs of the mission. UCW permits the development of organizations and their infrastructure simultaneously, in a compartmented manner, well beyond the normal scrutiny of a target regime, or for that matter the participants or potential participants. Planners and operators overcome the constraints inherent with traditional UW by operating in near anonymous and non-attributable ways to maintain freedom of action.

---

[221] Hollis, "Cyberwar Case Study Georgia 2008," 6.

[222] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*.

5. BUILDUP

Buildup, or Phase 5, involves the expansion of the organization and its capabilities. The focus during this phase is on recruitment, training, and targets appropriate to the actual requirements of the mission.[223] To accomplish these tasks within a UCW campaign operators may leverage cyber capabilities to develop multiple, redundant, compartmented organizations that provide durability to the ongoing UW effort.

A way to grow the organization is through recruitment. Arguably, with cyber the barriers to entry into a resistance movement are much lower. The Tunisian Revolution witnessed the growth of the presence of Anonymous, as it provided a discrete micro-protest possibility to many that otherwise was previously unavailable.[224] To utilize this platform of protest enables those who otherwise wouldn't participate an opportunity to do so. However, as groups grow during this phase, the possibility of being infiltrated remains, just as it does in traditional UW.

Operating outside the bounds of traditional time and space constraints allows for the development of redundant organizations maximizing cyberspace's inherent compartmentalization. The insurgent or resistance organization may become layered as a result of the redundancy and provide an organic level of durability to the UW effort. Creating redundancy in the organization serves to mitigate the effectiveness of COIN efforts undertaken by the target regime. The groups within the organization may quickly be re-tasked or repurposed to meet the challenges of the dynamic UW environment. Additionally, existing infrastructure may also be leveraged to mitigate the exploits of any COIN effort. This was apparent in the Tunisian experience as activists disseminated information via pdf. on Scribd, file sharing services, on torrents, and on Facebook as images, and also began crowdsourcing the translation of many of the documents.[225]

---

[223] Ibid.

[224] Coleman, "Anonymous — From the Lulz to Collective Action | The New Significance."

[225] Gharbia, "Chelsea Manning and the Arab Spring."

Lastly, there is an existing asymmetric component within cyber. The size of these groups is scalable to the mission; the requirement no longer exists to get big in order to win.

6. EMPLOYMENT

Within the traditional UW campaign the Employment Phase, or Phase 6, involves irregular forces operating in a combat or hostile environment. ARSOF units ought to ensure that the effects of the activities continue to support the goals of the theater commander as these operations increase in scope and size.[226] Cyber may be easily tied to supporting conventional military operations (CMO) or major combat operations (MCO). Just as cyber was instrumental in setting conditions for Russia's kinetic strike into Georgia, cyber may also be used to support protests and demonstrations as was the case in Tunisia. Upon commencement of Phase 6 planners and operators need to be mindful of employing constraints in preparation for transition whether they are supporting kinetic or non-kinetic operations.

7. TRANSITION

Transition, Phase 7, is typically the most difficult and sensitive phase of any UW effort. Transition may not necessarily require demobilization, but may require some type of stability operations.[227] As discussed earlier, cyber provides a high level of control that enables operators to turn off the effects of operations, thus returning disrupted services to normal operations. However, it may prove to be far more difficult to turn off the cyber militia that carried out the attacks. This is highlighted by the events surrounding the Arab Spring when at the conclusion of Ben Ali's reign in Tunisia, Anonymous continued to assist in revolutions throughout the Middle East and elsewhere. Further analysis may be warranted to determine the optimal model to organize, build, employ and transition for UCW operations.

---

[226] Department of the Army, *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*.

[227] Ibid.

C. CONCLUSION

UCW is not always the appropriate means to accomplish ones objective, however because of the flexibility and the ability to achieve results in environments that have limited connectivity, it is a viable option in many cases. Just as with traditional UW, the phases of UCW do not have to occur in order, may occur simultaneously, and depending on the mission requirement, may not occur at all. For example, as the resistance movement in Tunisia gained momentum, a large and effective organization developed that required only 'logistical support' via technical means in order to continue to be organized and employed against the regime, thereby bypassing the organization phase. The phases may also occur out of sequence, as the case of Russia v. Georgia illustrates the buildup of organization and infrastructure prior to populating the cyber militia with actual cyber guerrillas. Phases may also receive varying degrees of emphasis.[228] UCW allows for the greatest amount of flexibility, lowest cost, lowest inherent risk, and highest degree of control, all things being equal, and stands as a viable option to traditional UW options.

[228] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Our thesis has demonstrated that cyber is often times a means to an end, but it may also be the means with the least amount of inherent cost, risk, and the greatest opportunity to accomplish one's goals. Cyber means have the same ethical and legal constraints as their kinetic equivalent; however, because of the lesser risk, cost, and associated damage, they present a more palatable option than kinetic ones, all things being equal. During the examination of UCW we identified three approaches to creating or repurposing a cyber-militia. Each of these provides advantages and disadvantages, and none are a complete standalone solution. During the course of future research into the topic of UCW, it would be beneficial to determine when and under what conditions each approach can be leveraged to maximize opportunities for success.

As demonstrated by the case examinations and the proposed framework, UCW can enable a force the opportunity to exploit inherent weaknesses in cyberspace to support their operational objectives. UCW can be used as a means to an end by supporting concurrent major combat operations or to support ends directly in a standalone fashion. The speed, flexibility, low cost, and low-risk nature of UCW make it an appealing possibility that should be added to the formal lexicon of options within the realm of irregular and unconventional warfare.

As previously stated, similar to traditional UW, the phases of UCW do not have to occur in order, may occur simultaneously, and depending on the mission requirement, may not occur at all. The phases may also occur out of sequence to facilitate the buildup of organization and infrastructure prior to populating the cyber militia with actual cyber guerrillas. Phases may also receive varying degrees of emphasis, depending on the mission requirements, available infrastructure, and the amount of preparation to the cyber battlefield that has been conducted prior to UCW operation. UCW allows for the greatest amount of flexibility, lowest cost, lowest inherent risk, and highest degree of control, all things being equal, and stands as a viable option to traditional UW options.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"10 Most Censored Countries." *Committee to Protect Journalists*. Accessed April 25, 2014. http://cpj.org/reports/2012/05/10-most-censored-countries.php.

Alexander, Christopher. "Tunisia's Protest Wave: Where It Comes from and What It Means." Blog. *Foreign Policy Blogs*, January 3, 2011. http://mideastafrica.foreignpolicy.com/posts/2011/01/02/tunisia_s_protest_wave_where_it_comes_from_and_what_it_means_for_ben_ali.

"Algeria Unemployment Rate | Actual Value | Historical Data | Forecast." *Trading Economics*. Accessed March 10, 2014. http://www.tradingeconomics.com/algeria/unemployment-rate.

Anderson, Nate. "Tweeting Tyrants Out of Tunisia: Global Internet at Its Best." *WIRED*. Accessed March 7, 2014. http://www.wired.com/threatlevel/2011/01/tunisia/.

Anderson, Sulome. "Anonymous Threatens Morsy with Cyberwarfare." *Foreign Policy*, November 28, 2012. http://blog.foreignpolicy.com/posts/2012/11/28/anonymous_threatens_morsy_with_cyberattacks.

Basilici, Steven P., and Jeremy Simmons. "Transformation: A Bold Case for Unconventional Warfare." Monterey, CA: Naval Postgraduate School, 2004.

Bayles, William J. "Moral and Ethical Considerations for Computer Network Attack As a Means of National Power in Time of War." U.S. Army War College, 2000.

Billo, Charles, and Welton Chang. *Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States*. Hanover, NH: Dartmouth College, December 2004. http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.

Bohler-Muller, Narnia, and Charl Van der Merwe. "The Potential of Social Media to Influence Socio-Political Change on the African Continent." *Africa Institute of South Africa, Policy Brief* 46 (2011): 1–8.

Carr, Jeffrey. "In Tunisia, Cyberwar Precedes Revolution." *Forbes*, January 15, 2011. http://www.forbes.com/sites/jeffreycarr/2011/01/15/in-tunisia-cyberwar-precedes-revolution/.

Carroll, Ward. "Cyber War 2.0 — Russia v. Georgia." *Defense Tech*. Accessed December 17, 2013. http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/.

Cartwright, James E. *Joint Terminology for Cyberspace Operations.* JCS Memorandum, November 2010. http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint Terminology for Cyberspace Operations.pdf.

Clancy, James, and Chuck Crossett. “Measuring Effectiveness in Irregular Warfare.” *Parameters* 37, no. 2 (June 22, 2007): 13.

Clarke, Richard A. *Cyber War*. New York, NY: HarperCollins, 2011.

Coleman, Gabriella. “Anonymous — From the Lulz to Collective Action | The New Significance.” *The New Significance*, May 9, 2011. http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/.

Coons, Jr., Kenneth C., and Glenn M. Harned. “Irregular Warfare Is Warfare.” *Joint Force Quarterly* 1st Quarter 2009, no. 52 (2009): 97–103.

Dancho Danchev. “Coordinated Russia vs Georgia Cyber Attack in Progress.” Security. *ZDNet*, August 11, 2008. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

Denning, Dorothy E., and Bradley J. Strawser. “Moral Cyber Weapons: The Duty to Employ Cyber Attacks.” In *The Ethics of Information Warfare*, edited by Luciano Floridi and Mariarosaria Taddeo, 85–103. Springer, 2012.

Department of the Army. *FM 3-05.130, Army Special Operations Forces Unconventional Warfare*. Washington, D.C.: Headquarters, Department of the Army, 2008. http://orfeu-marketing.com/data/documents/A9R7039.pdf.

Duncan, Kirk A. “Assessing the Use of Social Media in a Revolutionary Environment.” Naval Postgraduate School, 2013. http://calhoun.nps.edu/public/handle/10945/34660.

Dunlap, Charles. “The Intersection of Law and Ethics in Cyberwar: Some Reflections.” *Air & Space Journal*, January 1, 2012, 1–17.

“Egypt Unemployment Rate | Actual Value | Historical Data | Forecast.” *Trading Economics*. Accessed March 10, 2014. http://www.tradingeconomics.com/egypt/unemployment-rate.

Epelboin, Fabrice. “Revolution 2.0: Rebooting Tunisia.” *ReadWriteWeb*, January 14, 2011. http://readwrite.com/2011/01/14/revolution_20_rebooting_tunisia.

Ethan Zuckerman- Cute Cats and the Arab Spring: When Social Media Meet Social Change, 2011. http://www.youtube.com/watch?v=tkDFVz_VL_I&feature=youtube_gdata_player.

Fowler, Sarah. “Who Is the Syrian Electronic Army?” *BBC*, April 25, 2013. http://www.bbc.co.uk/news/world-middle-east-22287326.

"Freedom on the Net: Tunisia." Independent Watchdog. *Freedom House*, 2011. http://www.freedomhouse.org/report/freedom-net/2011/tunisia#.U2murcepqwM.

Gharbia, Sami. "Chelsea Manning and the Arab Spring." *Nawaat*, February 24, 2014. http://nawaat.org/portail/2014/02/28/chelsea-manning-and-the-arab-spring/.

Gobe, Eric. "The Gafsa Mining Basin between Riots and a Social Movement: Meaning and Significance of a Protest Movement in Ben Ali's Tunisia," January 20, 2011. http://halshs.archives-ouvertes.fr/halshs-00557826/.

Gonzalez-Quijano, Yves. "False Promises? The Social Media and Arab Political Change." *Media and Arab Transition*, 2013, 60–63.

Hagen, Andreas. "The Russo-Georgian War (2008): The Role of the Cyber Attacks in the Conflict." The Armed Forces Communications and Electronics Association, May 24, 2012. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Hart, Kim. "Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar." News. *Washington Post*, August 14, 2008. http://articles.washingtonpost.com /2008-08-14/news/36876288_1_georgia-s-Internet-web-sites-cyberattacks.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, and Haley Nix. "The Law of Cyber-Attack." *California Law Review* 100 (2012): 817.

Hollis, David. "Cyberwar Case Study Georgia 2008." Military. *Small Wars Journal*, 2011. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Hunker, Jeffery, Bob Hutchinson, and Jonathan Margulies. "Role and Challenges for Sufficient Cyber-Attack Attribution." Institute for Information Infrastructure Protection, 2008. http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

Information Warfare Monitor. "Syrian Electronic Army: Disruptive Attacks and Hyped Targets," June 25, 2011. http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/.

"Internet Users (per 100 People)." Non-Profit. *The World Bank*, 2012. http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?order=wbapi_data_value_2012%20wbapi_data_value%20wbapi_data_value-last&sort=desc&display=default.

Internet World Stats. "Internet World Stats: Usage and Population Statistics, Internet Users in the Middle East and the World - June 30, 2012." *Internet World Stats: Usage and Population Statistics*, June 30, 2012. http://www.internetworldstats.com/stats5.htm.

Kelly, Terrence K., and Jeffrey Allen Hunker. “Cyber Policy.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 211–43.

Kirk, Jeremy. “Georgia Cyberattacks Linked to Russian Organized Crime.” Technology. *Computerworld*, August 17, 2009. http://www.computerworld.com/s/article/9136719/Georgia_cyberattacks_linked_to_Russian_organized_crime?pageNumber=1.

Koh, Harold Hongju. “International Law in Cyberspace.” Remarks|Remarks presented at the USCYBERCOM Inter-Agency Legal Conference, FT Meade, MD, September 18, 2012. http://www.state.gov/s/l/releases/remarks/197924.htm.

Krebs, Brian. “Security Fix - Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.” News. *Washington Post*, October 16, 2008. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

Leyden, John. “Bear Prints Found on Georgian Cyber-Attacks.” News. *The Register*, August 14, 2008. http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

Libicki, Martin C. “Cyberspace Is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8 (2013 2012): 321.

“Libya Unemployment Rate | Actual Value | Historical Data | Forecast.” *Trading Economics*. Accessed March 10, 2014. http://www.tradingeconomics.com/libya/unemployment-rate.

“List of Countries by Number of Mobile Phones in Use.” *Wikipedia, the Free Encyclopedia*, April 23, 2014. http://en.wikipedia.org/w/index.php?title=List_of_countries_by_number_of_mobile_phones_in_use&oldid=605471188.

“List of Targets of Arrested Computer Hackers.” *Phys.org*, March 6, 2012. http://phys.org/news/2012-03-hackers.html.

Lowe, Christian. “Russia Tightens Ties with Georgian Rebel Areas.” *Reuters*. April 16, 2008. http://www.reuters.com/article/2008/04/16/us-russia-georgia-breakaway-idUSL164428920080416.

Lukasik, Stephen J. “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.” In *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 2010.

Markoff, John. “Before the Gunfire, Cyberattacks.” *New York Times*, August 13, 2008, sec. Technology. http://www.nytimes.com/2008/08/13/technology/13cyber.html.

Menn, Joseph. “Expert: Cyber-Attacks on Georgia websites Tied to Mob, Russian Government.” *LA Times*, August 13, 2008. http://latimesblogs.latimes.com /technology/2008/08/experts-debate.html.

Mohammed Bouazizi. A Tunisian Martyr., 2011. http://www.youtube.com/watch?v=jHw_auqod6Y&feature=youtube_gdata_player.

Noman, Helmi. “The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army.” *Infowar Monitor: Tracking Cyberpower*, May 30, 2011. http://www.infowar-monitor.net/2011/05/7349/.

Noor, Naseema. “Tunisia: The Revolution That Started It All | International Affairs Review.” *International Affairs Review*, January 31, 2011. http://www.iar-gwu.org/node/257.

Nye, Jr., Joseph S. *Cyber Power*. Belfer Center for Science and International Affairs: Harvard Kennedy School, May 2010. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522626.

Olson, Eric T. “A Balanced Approach to Irregular Warfare.” *The Journal of International Security Affairs*, no. 16 (2009): 7.

Perlroth, Nicole. “Hunting for Syrian Hackers’ Chain of Command.” Newspaper. *The New York Times*, May 17, 2013. http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html.

“Project Grey Goose Phase II Report.” *Scribd*. Accessed August 13, 2013. http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.

Reinold, Theresa. “State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11.” *The American Journal of International Law* 105, no. 2 (April 2011): 244–86. doi:10.5305/amerjintelaw.105.2.0244.

Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. doi:10.1080/01402390.2011.608939.

Rowe, Neil C. “Ethics of Cyber War Attacks.” In *Cyber Warfare and Cyber Terrorism*, edited by Lech Janczewski and Andrew M. Colarik, 105–11. Idea Group Inc (IGI), 2008.

“Russia’s N.Ossetia Wants Unification with Georgia’s S.Ossetia.” Russian News Agency. *RIA Novosti*, May 20, 2008. http://en.ria.ru/world/20080520/107888655.html.

Ryan, Yasmine. “Tunisia’s Bitter Cyberwar - Features - Al Jazeera English.” News. *Al Jazeera*, January 6, 2011. http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html.

Schmitt, Michael N. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. Information, 1999. http://papers.ssrn.com/abstract=1603800.

Schmitt, Michael N. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *The Harvard International Law Journal Online* 54 (December 12, 2012): 13–37.

“Tunisia Unemployment Rate | Actual Value | Historical Data | Forecast.” Accessed March 10, 2014. http://www.tradingeconomics.com/tunisia/unemployment-rate.

U.S. Special Operations Command, and U.S. Marine Corps. “Irregular Warfare Joint Operating Concept.” Department of Defense, September 11, 2007. http://www.au.af.mil/au/awc/awcgate/dod/iw_joc.pdf.

Van Niekerk, Brett, Kiru Pillay, and Manoj Maharaj. “Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective.” *International Journal of Communications* 5 (2011): 1406–16.

Wheeler, David A., and Gregory N. Larsen. *Techniques for Cyber Attack Attribution*. Defense Technical Information Center, 2003. http://handle.dtic.mil/100.2/ADA468859.

“Worst of the Worst 2012: The World’s Most Repressive Societies.” Independent Watchdog. *Freedom House*, 2012. http://www.freedomhouse.org/report/special-reports/worst-worst-2012-worlds-most-repressive-societies#.U2v5-vldViM.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California