NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ASSESSING THE USE OF SOCIAL MEDIA IN A REVOLUTIONARY ENVIRONMENT

by

Kirk A. Duncan

June 2013

Thesis Advisor:	Dorothy Denning
Second Reader:	Gordon McCormick

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE ASSESSING THE USE OF SOCIAL MEDIA IN A REVOLUTIONARY ENVIRONMENT	5. FUNDING NUMBERS
6. AUTHOR(S) Kirk A. Duncan	
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) N/A	**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 Approved for public release, distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

Social media garnered much attention from the Arab Spring uprisings where activists took advantage of computer and mobile phone technologies to organize the collective actions of thousands of citizens. The influence and power of social media are only likely to increase. According to *eMarketer* (2012), by 2014, over one-fourth of the world's population will be using social media technology. However, military planning has not fully harnessed this powerful tool. In trying to understand how this technology should be utilized by special operations forces (SOF), this thesis examines the role that social media plays in various forms of conflict across the globe. Specifically, this research assesses and identifies what types of social media should be used to support a range of special operations objectives, from strategic influence to disruption, coercions, and regime overthrow. Additionally, a social media assessment methodology is provided that can be used by strategists to evaluate the most appropriate use of social media technology to support special operations.

14. SUBJECT TERMS Social Media, Social Media Technology, Social Media in Unconventional Warfare, Unconventional Warfare, UW, Special Forces, Special Operations Forces, SOF, ARSOF, Core Activities, Arab Spring, Revolution, Egyptian Revolution, Revolutionary Warfare, Insurgent, Insurgency, Tunisia, Egypt, Political Process Model, Social Movement, Social Movement Theory, SMT, Social Networks, Facebook, Twitter, Disrupt, Coerce, Deter, Overthrow, Defeat, Regime Change, Insurgent Warfare, Counterterrorism, CT, Counter-Insurgency, COIN, Information Operations, IO, Internet, Bluetooth, Social Media Assessment Tool, Social Media Assessment Methodology, Mobile Phones, Cell Phones, SMS, Text Message, Censorship, Censorship Tools, Surveillance, Filters, Circumvention Tools, Proxy, Augmented Reality, CIA, FBI, Crowdsourcing, Open Source Intelligence, OSINT, Narrative, Passive Mobilization, Consensus Mobilization, Recruitment, Activism, Active Mobilization, Action Mobilization, Military Information Support Operations, MISO	15. NUMBER OF PAGES 175
	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

ASSESSING THE USE OF SOCIAL MEDIA IN A REVOLUTIONARY ENVIRONMENT

Kirk A. Duncan
Major, United States Army
B.A., Benedictine College, 2001
M.B.A., American Military University, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2013

Author: Kirk A. Duncan

Approved by: Dorothy Denning
Thesis Advisor

Gordon McCormick
Second Reader

Doowan Lee
Third Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Social media garnered much attention from the Arab Spring uprisings where activists took advantage of computer and mobile phone technologies to organize the collective actions of thousands of citizens. The influence and power of social media are only likely to increase. According to *eMarketer* (2012), by 2014, over one-fourth of the world's population will be using social media technology. However, military planning has not fully harnessed this powerful tool. In trying to understand how this technology should be utilized by special operations forces (SOF), this thesis examines the role that social media plays in various forms of conflict across the globe. Specifically, this research assesses and identifies what types of social media should be used to support a range of special operations objectives, from strategic influence to disruption, coercions, and regime overthrow. Additionally, a social media assessment methodology is provided that can be used by strategists to evaluate the most appropriate use of social media technology to support special operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARSOF	Army Special Operations Forces
ASD [SO/LIC]	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
CSCC	Center for Strategic Counterterrorism Communications
CIA	Central Intelligence Agency
CA	Civil Affairs
CAO	Civil Affairs Operations
CCV	Client/Customer/Visitor
CGI	Common Gateway Interface
COIN	Counter-Insurgency
CP	Counter-Proliferation
CT	Counter-Terrorism
DPP	Democratic Progressive Party
DoD	Department of Defense
DOT	Digital Outreach Team
DA	Direct Action
DDOS	Distributed Denial of Service
DNS	Domain Name Server
XMPP	Extensible Messaging and Presence Protocol
FBI	Federal Bureau of Investigation
FTP	File Transport Protocol
FID	Foreign Internal Defense
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol with Secure Sockets Layer
IO	Information Operations
IIS	Interagency/Intergovernmental Support
IXPs	Internet Exchange Points
IP	Internet Protocol
ISPs	Internet Service Providers
JAM	Jaish al-Mahdi

JRTN	Jaysh Rijal al-Tariqa al-Naqshbandia
LAN	Local Area Network
MISO	Military Information Support Operations
MSO	Military Support Operations
NPS	Naval Postgraduate School
NAPs	Network Access Points
OAKOC	Observation, Avenues of Approach, Key Terrain, Obstacles, Cover and Concealment
OEV	Operation Earnest Voice
ODA	Operational Detachment—Alpha
PACE	Primary, Alternate, Contingency, Emergency
POP	Points of Presence
RTP	Real-time Transport Protocol
SSH	Secure Shell Tunnels
SFA	Security Force Assistance
SIP	Session Initiation Protocol
SMS	Short Messaging Services
SMTP	Simple Mail Transport Protocol
SF	Special Forces
SFISC	Special Forces Intelligence Sergeant Course
NDC	Special Forces Network Development Course
SOF	Special Operations Forces
SR	Special Reconnaissance
TTPs	Tactics, Techniques, and Procedures
TCP	Transmission Control Protocol
SWCS	U.S. Army John F. Kennedy Special Warfare Center and School
UW	Unconventional Warfare
UWODC	Unconventional Warfare Operational Design Course
USD(P)	Undersecretary of Defense for Policy
URL	Uniform Resource Locator
USSOCOM	United States Special Operations Command

VPNs	Virtual Private Networks
VoIP	Voice-Over Internet Protocol
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to extend my deepest thanks to my thesis advising team. Dr. Denning is a professional in every sense of the term. Her mentorship, guidance, and common-sense advice were invaluable to this work. Dr. McCormick's assistance in developing the overall focus for this thesis was critical. He provided the basic direction from which to tackle this challenging topic. Professor Lee worked tirelessly to help me during the entire writing process. His contributions are sprinkled throughout this thesis. He continually challenged and motivated me to do my best. Thanks, also, to the entire Defense Analysis Department. The leadership, faculty, and staff provide amazing support to the department's students. Finally, and most importantly, thank you to my family for their constant support for everything that I do. Most especially, I want to thank my wife, Becky, whose patience, love, and encouragement know no bounds.

—De Oppresso Liber

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. GENERAL AREA OF RESEARCH

What role did social media play during the revolutionary uprisings and regime changes in Tunisia, Egypt, Libya, and Yemen, commonly referred to as the Arab Spring? Collectively, these four countries experienced relatively rapid regime change, and one of the common factors in each was the citizenry's use of social media as an organizing tool and communications platform. Taken together, the individual outcomes of each country affected by the Arab Spring seemed to indicate a causal relationship between the use of social media as a tool of protest, and the ability to overthrow a regime. Additionally, extensive use of anecdotal evidence by various authors has been offered as proof that the use of social media within the context of revolutionary struggle favors the insurgent movement. However, upon closer examination, it is evident that social media is a neutral technology. It can be used in both an offensive and defensive manner by those fighting the revolution, and those in power trying to put the revolution down.

B. STATEMENT OF PURPOSE AND SCOPE

A lot of research, time, and effort have been devoted to examining the use of social media during the Arab Spring, and in social movements in general. Some argue that social media was a direct cause of the various regime changes that happened across North Africa and the Middle East. Others take the view that these various regime changes would have occurred without the use of social media. Still others take a middle ground approach, arguing that while social media did not play a central role in causing the revolutions, it did significantly increase the speed in which the revolutions occurred.[1] What is missing in the current literature regarding social media is a way to systematically assess the strengths and weaknesses of each side's social media capabilities.

[1] For a thorough bibliography of the Arab Spring Uprising, see the Project on Middle East Political Science web site at http://pomeps.org/category/academic-works/arabuprisings/.

Certainly, oppressive regimes have learned from the situations in Tunisia, Egypt, Libya, and Yemen. Thus, it is important for the United States to develop an organizing framework from which to evaluate the future utility of social media in executing unconventional warfare (UW), as it can be assumed that dictatorial leaders will be more prepared to counter social media sparked uprisings in the future. The purpose of this thesis is to provide that framework.

This thesis will develop a social media assessment methodology that can be used by strategists to evaluate the social media environment in a given country or situation. By building an organizing framework with which to view social media as a tool for both the state and counter-state to utilize, strategists will be able to make better judgments in terms of how social media should be used (if at all) in trying to achieve U.S. objectives. More specifically, this exploration of social media in conflict will be focused primarily on UW.

C. BACKGROUND

For a social movement to emerge, a significant portion of a disenfranchised population must experience a transformation of consciousness.[2] For an insurgency to emerge, three sets of factors must meld in a way that favors the insurgents. Initially, expanded political opportunities must emerge and combine with existing indigenous networks within the minority community. These expanded opportunities provide the insurgent movement the structural potential to act in a collective manner. This potential is transformed into kinetic activity by the critically important intervening process of cognitive liberation. Cognitive liberation entails framing the community's perceived situation in life as unjust, intolerable, and mutable in order to mobilize a large group. Thus, all three factors are necessary but alone insufficient causes for the emergence of an insurgent movement.[3] This process is graphically depicted in Figure 1.

---

[2] Doug McAdam, *Political Process and the Development of Black Insurgency, 1930–1970*, 2nd ed. (Chicago, IL: University of Chicago Press, 1999), 51.

[3] Ibid., 51.

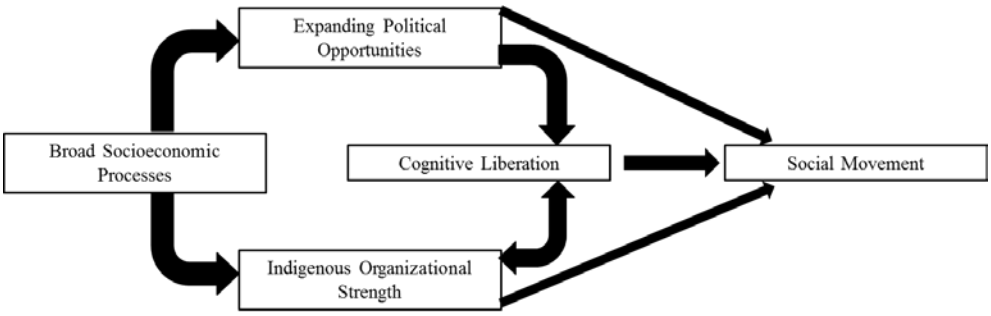

Figure 1. The Political Model of Social Movements[4]

Also, a quick examination of revolutionary history shows that movements that are threatening to governments, and the governments themselves, will utilize all available tools of information dissemination either to fight or counter the revolution. Examples include the Bolshevik revolution of 1917 and the Iranian revolution in 1979. The Bolsheviks made great use of the postal service and the telegraph. Those behind the revolution in Iran used tape recorders to smuggle in sermons recorded by the Ayatollah in Paris.[5]

The unfolding events of Tunisia and Egypt provided a more recent example that demonstrates the competitive nature of the technological environment, in this case the social media environment. A Twitter hashtag, #sidibouzid, helped spark the first protests that turned into flash mobs in Tunisia. Additionally, Facebook pages were beginning to populate the Internet in protest of the Zine el-Abidine Ben Ali dictatorship. Attempting to stifle the voices of dissent, the Tunisian government began to hack into and delete the Facebook accounts of the activists. In response, Tunisian social media users reached out to the greater "hacktivist" community and asked for help. The hacker group Anonymous took up the cause and blocked the president's official website, the local stock exchange, and key ministry's websites. Additionally, the group provided a cyber-war survival guide to the citizens of Tunisia. This guide provided leaked wiki-leaks documents showing the

[4] McAdam, *Political Process*, 51.

[5] Evgeny Morozov, interview by Marwan Bishara, IITrends, http://www.iitrends.com/2011/03/video-social-networks-social-revolution.html (acccessed November 12, 2012).

corruption of the Ben Ali regime. The guide also provided tips for running from the police, and using proxy websites to regain access to Facebook and Twitter.[6]

The Tunisian government countered these activities by executing a phishing operation that was used to steal the user name and passwords of citizens' email, Twitter, and Facebook accounts in order to spy and silence online dissent.[7] Eventually, the people of Tunisia won this competition and were able to oust Ben Ali. The successful revolution in Tunisia broke the fear factor in Egypt and provided the accelerant needed to fuel the Egyptian people into collective action.

Egyptians began to share tips on topics such as self-defense and nonviolent resistance. Egyptian activists also began to make plans to circumvent existing police barricades, which were designed to prevent protestors from reaching Cairo's Tahrir Square. On the other side, Egyptian President Hosni Mubarak had also learned from the events in Tunisia. In an effort to stop the January 25, 2011 protests from gaining momentum, the Egyptian government shut down the country's Internet. Outside supporters responded by providing proxy sites that would allow Egyptians to circumvent the government's block of the Internet. Additionally, journalists inside Egypt started to send "tweets" via text messages to their friends outside of Egypt. These friends would then turn the text message back into a tweet and send the tweet out via Twitter. In response, the Egyptian government began to arrest and imprison journalists in the country.[8]

In light of the Arab Spring and the literature on social media's use in conflict, this thesis argues that while social media is not a direct cause of revolution, it certainly helps

---

[6] Al Jazeera English, "Empire," http://www.aljazeera.com/programmes/empire/2011/02/201121614532116986.html (accessed January 9, 2013).

[7] Yasmine Ryan, "Tunisia's Bitter Cyber War,"*Aljazeera*, January 6, 2011, http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html (accessed January 11, 2013).

[8] Ibid.

to facilitate them. Additionally, social media technology differs from previous generations' communication technology in that social media operates in a "super-sonic" manner, with the ability to reach so many, so quickly.[9]

D. RESEARCH QUESTIONS

The primary research question addressed by this thesis is: How can one analyze and assess the social media environment in the context of a revolutionary environment? To address this question, the thesis also investigates several secondary questions, including:

1. What are each side's opening advantages and vulnerabilities in the social media environment?
2. What are the critical factors or variables that contribute to an entity's relative social media capabilities?
3. What are the options available to each side in its utilization of social media within a competitive environment?
4. What are the advantages and disadvantages of either using or not using social media in revolutionary movements?
5. What are the specific effects that can be achieved by the state and by insurgent groups by using social media?

E. CENTRAL CLAIM

The central claim of this thesis is that social media can be an effective tool in achieving strategic goals of the U.S. within a UW campaign, and that they may play an important role in future U.S. UW campaigns. However, the appropriate use of social media depends on the specific situation on the ground. Just as there is no one-size-fits-all approach to military strategy in general, there is no set strategy in the utilization of social media. 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 social media. For instance, one set of conditions on the ground, such as the ones found in Egypt, may mean that

[9] Carl Bernstein, interview by Marwan Bishara, IITrends, http://www.iitrends.com/2011/03/video-social-networks-social-revolution.html (acccessed November 12, 2012).

social media could be used in an effort to overthrow a regime. On the other hand, in Syria for example, social media may only be used to help disrupt or coerce the government to reform certain policies. To help strategists determine whether and how social media can support a UW campaign in a given country or situation, this thesis will develop a social media assessment methodology that can be used to evaluate a social media environment.

F. LITERATURE REVIEW

One of the key debates within the literature is the extent to which social media conditions or facilitates the likelihood of revolution. On one hand, social media is portrayed as the single most significant causal factor of revolution. On the other, the role of social media is more nuanced as one of many tools of information sharing. In other words, other conditions must be in place for social media to have a significant impact on social revolution.[10] Representing the former, journalist Andrew Sullivan declared in 2009, "the revolution (in Iran) will be Twittered!" Sullivan's comments came as several thousand social media users in Iran attempted to mobilize the citizens in that country to move towards regime change. However, as the next several months played out, there was no revolution in Iran. Since Sullivan's famous remarks were made, several prominent journalists have argued that social media, in and of itself, can be a primary cause of revolutionary changes. Arguably the most prominent supporter of the political power of social media in social movements is author Clay Shirky. In his article, "The Power of Social Media," he opens with what he describes as the first major use of social media to affect political change.[11]

According to Shirky, some seven million text messages were sent during the week that Philippine President Joseph Estrada was on trial, facing possible impeachment. When several news sources revealed that Estrada loyalists in the Philippine Congress had voted to set aside key evidence against the sitting president, a citizen initiated protest was organized. In response to the simple text message, "Go to EDSA, Wear blk," over one

[10] Doowan Lee, "A Social Movement Approach to Unconventional Warfare," *Special Warfare Magazine* 27, no.1 (2013).

[11] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs* 90, no. 1(2011): 28–41.

million people descended on downtown Manila. Eventually, the country's legislators gave in to the crowd's pressure, re-introduced the damning evidence against Estrada, and on January 20, 2001, Estrada was finished as president. Using this example, and several others, Shirky's primary argument is that the United States should continue to push for and support unrestricted access to the Internet and to social media for every person in the world. Internet freedom, Shirky states, facilitates advances in civil society in the long run, and helps to prevent abuses of power in the short term. Social media accomplishes these objectives by exponentially increasing the spread of information, the type and numbers of speeches by ordinary citizens, and the spread of group coordination.[12] Shirky provides a caveat to his arguments by stating that ultimately social media's effect is limited when a government is willing to turn its guns on its own citizenry as was done to the Green Movement in Iran, and to the Red Shirt protestors in Thailand. Stated simply, killing is often an effective way to maintain the status quo. Other authors argue that future revolutions will not be tweeted.

The two most prominent opponents to the argument that social media matters in the context of revolutionary movements are Malcolm Gladwell and Evgeny Morozov. Gladwell opens his article, "Small Change; Why the Revolution Will not be Tweeted," with an example of a social movement spread without the use of social media. This social revolution started in Greensboro, North Carolina in 1960, and centered on a local Woolworth's refusal to serve a cup of coffee to a black college student. Starting in that one store, in that one city, Gladwell describes the rapid spread of other protests throughout the South that eventually numbered over 70,000 protesters, saw thousands arrested, and sparked the decade-long civil-rights war.[13] Gladwell states that successful social movements are centered on an individual's *strong ties* to one another. Examples provided include the participants in the Freedom Summer movement in the United States, the Red Brigades in Italy, and the mujahideen in Afghanistan. The argument here is that

[12] Shirky, "The Political Power of Social Media," 29.

[13] Malcolm Gladwell, "Small Change: Why the Revolution will not be Tweeted," *The New Yorker*, http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all (accessed August 20, 2012).

people join movements primarily because they have a close friend or relative who is already in the social movement, this connection representing a strong tie.

With the use of social media, however, the connections between users is centered on *weak ties*.[14] Although there are many powerful connections that can be the result of these weak ties—new ideas and innovations, interdisciplinary collaboration, or the ability to seamlessly match sellers to buyers,—weak ties seldom lead to high-risk activism. In this argument, Gladwell states that it is easy to get lots of people with whom one has weak ties to do something on one's behalf, given that the task does not ask too much of others. Thus, Gladwell draws a sharp distinction between a Facebook friend and a *real* friend. Additionally, Gladwell argues that although social media is a great way to build a network structure, networks are not effective at accomplishing certain tasks. Because networks do not have a central leadership structure, there is difficulty reaching any kind of consensus, and no way to set an agreed upon goal. Networks cannot think strategically, and are chronically at risk of constant conflict and error. According to Gladwell, giving everyone an equal voice is not necessarily a good thing. Thus, social media makes it easier for activists to express themselves, but harder to convert the ability to express ideas into tangible action that results in something that is impactful. Morozov shares much of the same views on social media that Gladwell does.

In his book, *The Dark Side of Internet Freedom,* Morozov argues that rather than a force for positive change, having unlimited access to the Internet and social media actually results in an increased ability for repressive regimes to suppress free speech, increase the effectiveness of surveillance, increase the spread of propaganda, and help to pacify citizens with mindless, digital entertainment.[15] Thus, the U.S. must stop viewing social media as inherently liberating but more as a neutral technology. In fact, Morozov

---

[14] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (1973):1360–1380, http://sociology.stanford.edu/people/mgranovetter/documents/granstrengthweakties.pdf (accessed May 15, 2013).

[15] Evgeny Morozov, *The Net Delusion* (New York: PublicAffairs, 2011).

states that social media and the Internet may actually favor the state, especially dictatorial regimes that are willing to use excessive amounts of violence against their own people to stay in power.

The truth may lie somewhere in the middle of these two opposite views. The research done in this thesis clearly shows that people simply having access to the Internet and social media is not enough to allow them to cause a sustained revolution. However, it also indicates that social media technology, if used in smart, creative ways, can facilitate and accelerate the pace and growth of an insurgency. Therefore, social media is an inherently neutral tool. The side that uses this tool most effectively will gain a significant advantage in determining the ultimate victor in a conflict.

G. THESIS STRUCTURE

This thesis contains five chapters and three appendices. The first chapter introduced the general area of research, the purpose, some background information (to include a description of the Political Process Model of social movements), the hypothesis and research questions, and concluded with a literature review. Chapter II opens by applying the military acronym OAKOC to social media as a way of better understanding this competitive environment. The chapter provides some technical background information which describes how the Internet and social media platforms actually work. It introduces a conceptual model that is designed to facilitate the understanding of the competitive landscape of social media. The second chapter concludes with a description of the technologies and means that governments use to censor and conduct surveillance within the social media environment, and a description of the technologies dissidents use to avoid being censored and kept under digital surveillance.

Chapter III provides an overview of how certain social media platforms and technologies have been used to assist in the execution of various types of operations, in different types of warfare. More specifically, the focus of this chapter centers on the use of social media to support insurgent warfare, counterterrorism (CT), and counter-insurgency (COIN) to achieve a range of desired end-states ranging from disruption to

overthrowing/defeating a ruling regime or a major insurgent group The chapter concludes with a discussion of future trends in using social media in conflict.

Chapter IV starts with an outline of twelve key factors that should be taken into account by military planners in assessing the most appropriate use of social media technology in conflict. More specifically, the chapter primarily focuses on assessing the best use of social media technologies in support of an UW campaign. The second part of the chapter identifies the various overarching ways in which social media can be used in conflict. This menu of options is ranked based on the relevant amount of risk a person would face in using social media in a particular way. Finally, this chapter identifies and discusses the limitations and potential misuses of social media technology in revolutionary warfare, that is, both the conditions in which social media should not be used and the objectives that social media should not attempt to accomplish.

Chapter V is the concluding chapter and provides recommendations for the authorities, training and education, and the doctrine needed to maximize the potential of social media in support of military operations. Please note that a thorough reading of the technical discussions in Chapter II is not essential to the remainder of the thesis. Chapters III, IV, and V were written to be used as stand-alone products.

II. THE INTERNET AND SOCIAL MEDIA: AN INTRODUCTION

One of the United States' special operation forces' imperatives is to understand the operational environment. According to Army doctrine, "Special operations cannot shape the operational environment without first gaining a clear understanding of the theater of operations."[16] At a more elementary level, Infantry second lieutenants are taught to evaluate the environment they will be operating in by using an acronym to describe the physical terrain. This acronym is OAKOC. It stands for observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment.[17] By studying each of these aspects of the physical terrain in which missions will be conducted, good platoon leaders can visualize how to best navigate within their area of operations. In a similar manner, they must understand the social media environment in order to operate within this virtual domain. Applying OAKOC to the various aspects of social media throughout this chapter will add a familiar framework to the descriptions of each part of this online environment. First, the thesis will examine the social media environment from a broad perspective.

To begin to understand the social media environment, it is important to first establish social media's taxonomy. Most broadly categorized, social media falls under the communications media umbrella. Examples of other technologies that belong to this category include platforms such as television, radio, the Internet, print media and any other tools used to communicate. Narrowing the taxonomy further, social media falls largely within a sub-component of the Internet, namely the World Wide Web. Still further, social media is part of Web 2.0 technology. Web 2.0 is defined as "a set of applications and technologies that allows users to create, edit, and distribute content;

---

[16] Department of the Army, *Army Doctrine Publication 3-05, Special Operations* (Washington, D.C.: Department of the Army, 2012), 13, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_05.pdf (accessed March 12, 2013).

[17] Department of the Army, *Army Field Manual 3-21.8, The Infantry Rifle Platoon and Squad*. (Washington, DC: Department of the Army, 2008), 1-45, https://rdl.train.army.mil/catalog/view/100.ATSC/04183AF4-34EB-47F0-BCEE-29C93432DA49-1274564010088/3-21.8/toc.htm (accessed March 12, 2013).

share preferences, bookmarks, and online personas; participate in virtual lives; and build online communities.[18] In addition to Internet-enabled social media platforms, social media also includes mobile phones as well as other handheld devices (the iPod Touch 5th Generation, for example). With social media's taxonomy complete, the social media environment itself will be examined.

At the most basic level, the social media environment relies on the Internet and various pieces of hardware and software to operate. Satellites and cellular phone towers also facilitate the use of social media. In the context of social media's use during a period of conflict, the primary context of this thesis, the social media environment should be examined by looking at the technologies that are used by a state for the purposes of censoring, monitoring, locating, and keeping surveillance on dissidents. Conversely, the technologies that those in rebellion use to circumvent state activities and remain anonymous should be examined.

This chapter will provide a basic overview of how the Internet operates, the hardware and software that is needed to run the social media environment, the technologies used to censor, monitor, and keep surveillance on social media users, and the technologies used to avoid detection and remain anonymous while using social media. Additionally, this chapter will provide a graphical model for visualizing the social media environment and framing the subsequent chapters. Graphically depicting the competition space is important as war practitioners seek to understand how to articulate intent in using social media technology during periods of conflict. This chapter will conclude with some additional points to consider when examining the social media environment, including a discussion on the future of the social media environment.

To begin to apply the OAKOC framework to the social media environment, the thesis will begin with the most important aspect of analyzing any environment, identifying the key terrain. In the majority of military conflicts, from antiquity to the modern conflict currently waging in Afghanistan, the expression "control the high

[18] Kenneth Laudon and Carol Traver, *E-Commerce: Business, Technology, Society*, 7th ed. (Upper Saddle River, NJ: Prentice Hall, 2011), 18.

ground" is used by commanders to identify the key physical terrain in their operating environments. Identifying the high ground is a fairly simple task, yet can be overlooked in the heat of battle. Similarly, the single most critical consideration in examining social media is also simple, but can be overlooked in the heat of the moment. This critical factor is connectivity to the Internet and/or to cellular phone towers. To begin the discussion of the Internet, the key terrain of the social media environment, it is important to understand how this communications platform actually functions.

A. THE INTERNET—KEY TERRAIN

The most basic task of the Internet is to facilitate the movement of digital information from an origin to a specified destination, using the most suitable path available and the most appropriate mode of transportation.[19] A primary question is how this is accomplished?

The Internet is a network of networks connected by devices called routers. Routers are responsible for managing the flow of information between networks. They work by forwarding data to another router closer to the end destination for a data request. The networks comprising the Internet are owned and operated by organizations called Internet Service Providers (ISPs). Smaller, regional ISPs typically buy Internet access from very large national or multinational ISPs. These ISPs have various Points of Presence (POP) in each region in which they operate. Each connected computer that links to a specific POP network is then connected to the backbone.[20] Individual Internet users connect to the Internet either directly through an ISP or through an organization's internal network (e.g., a local area network or LAN), which in turn is connected to an ISP.

The Internet backbone is comprised of major networking equipment and global data connections comprised of fiber-optic cables and satellite links. The backbone owners connect to each other at major hubs known as Network Access Points (NAPs) or Internet

[19] Ronald Deibert et al., "Circumvention Tools," (2011), http://howtobypassinternetcensorship.org/files/bypassing-censorship.pdf (accessed February 11, 2013).

[20] Ibid.

Exchange Points (IXPs).[21] These backbone connections are what enable Internet users in countries around the world to communicate with one another. Finally, the routers that connect internal networks to the Internet or that connect local or national networks to the global Internet are sometimes referred to as gateways. It is important to understand all of these points of connection because Internet traffic can be censored, monitored, or otherwise controlled at any number of these routers and gateway connections.[22] Figure 2 is a very simplified graphical depiction of the major components of the Internet.

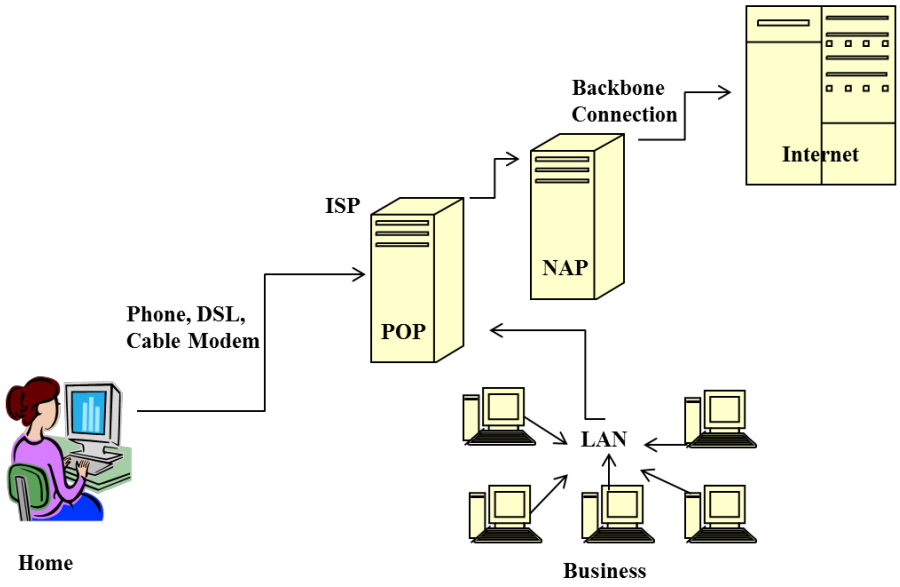

Figure 2. How the Internet Works[23]

All of the connections made to the Internet use some type of standard or protocol. These protocols allow one Internet-connected computer to find and transmit data to another Internet-connected computer. The most basic protocol is called the Internet Protocol or IP. This protocol is responsible for routing all data, which is assembled into

[21] Laudon and Traver, *E-Commerce*, 145–147.

[22] Deibert et al., "Circumvention Tools."

[23] Jeff Tyson, "How Internet Infrastructure Works," How Stuff Works, http://computer.howstuffworks.com/internet/basics/internet-infrastructure1.htm (accessed February 8, 2013).

packets, through the Internet. Another important protocol is the Transmission Control Protocol (TCP). This protocol sets up a reliable connection with a remote device that ensures packet delivery. The TCP uses IP to transmit and route the data it sends.

In order to connect to the Internet, a device needs a numeric IP address. While some addresses are static, others are assigned dynamically at the time of connection. The IP addresses assigned to Internet servers that host Websites and email are static, although they can be changed. For the most part, users need not be concerned with IP addresses. Instead of having to memorize a long stream of numbers (the actual IP address), the Domain Name Server (DNS) system matches numbers like 216.92.171.152 to names such as www.witness.org.[24]

The information that one sends through the Internet can take many forms. Examples include Web pages, email, pictures or video, a database, a secure text file, a software program, and many others. To handle these various information forms, a variety of specific protocols have been developed. The Hypertext Transfer Protocol (HTTP) supports Web traffic. Simple Mail Transport Protocol (SMTP) handles emails. Extensible Messaging and Presence Protocol (XMPP) is designed for routing instant messaging. File Transport Protocol (FTP) accommodates file sharing. Peer-to-peer file sharing can be done through the Bit Torrent protocol. Other protocols include Voice-Over Internet Protocol (VoIP), Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) among others. All of these protocols use IP, and many use TCP as well. A brief summary of how information flows across the Internet via the Web allows the thesis to bring the entire discussion into focus.

Suppose a person wants to visit the website www.witness.org. To do so, the user would type that website name into a Web browser and hit enter. The Internet-connected device would send this domain name to a DNS server. The DNS server would return a message that contains the IP address for this website, currently 216.92.171.152. The Web browser would then send a digital request to that IP address using TCP (which will use

[24] Deibert et al., "Circumvention Tools."

IP) asking to set up a connection. This request would get sent through a serious of routers. Each router would send the request to another router that is closer to the final destination until the specific machine is reached. This machine would then acknowledge the TCP request. Once the connection is established, the browser would send an HTTP request to the Web server requesting the page at the Web address. The HTTP request will use TCP, which in turn will use IP, to transmit the request over the established connection. The Web server in turn would use HTTP to send the requested page back to the browser for display on the user's monitor. The route that the information from the website actually goes through is different from the original path. Each stop along the way is known as a "hop" and the number of hops between a user and a website is typically between five and 30.[25]

All of this information is important in the utilization of social media in support of UW. Having a basic understanding of how the Internet operates will facilitate a better understanding of the technologies that support the social media environment and the technologies used to exploit its various capabilities by both states and those that oppose states. Having this understanding facilitates a special operations forces (SOF) operator's ability to evade state monitoring and censorship. Additionally, this knowledge will help in understanding where vulnerabilities are in terms of the Internet.

If a planner is aware of where an individual insurgent's Internet connections are most vulnerable along this massive chain of interconnected machines, and where connectivity is needed most, he or she will be better able to apply resources and develop plans to maintain Internet connectivity for those whose objectives align with the planner's objectives. Several examples of innovative and creative ways to gain control of Internet connectivity will crystallize this discussion.

One of the U.S. State Department's primary objectives under Secretary Hillary Clinton was to ensure that repressed peoples around the world had digital connectivity to

[25] Deibert et al., "Circumvention Tools."

the rest of the world.[26] To that effort, the U.S. government has been developing a small package of hardware and software that can be employed stealthily in almost any environment. The concept, known informally as the "Internet in a suitcase," can provide wireless communications over a large area which facilitates connectivity to the global Internet.[27] A graphic representation of the basic concept is shown in Figure 2. Basically, the system uses mesh network technology that can transform simple devices such as cell phones and laptops into a vast wireless network, without the need for a centralized hub.[28] Thus, a text message, email, or picture could hop along individual, modified cell phones and computers, with each machine acting as its own small cell tower, thus bypassing a government's state controlled infrastructure. This asset has the potential to enable activists in countries like Iran, Syria, and North Korea, for example, to be able to communicate outside of their government's control.

[26] James Glanz and John Markoff, "U.S. Underwrites Internet Detour Around Censors," *The New York Times*, June 12, 2011, http://www.nytimes.com/2011/06/12/world/12internet.html?pagewanted=all&_r=0.

[27] Ibid.

[28] Ibid.

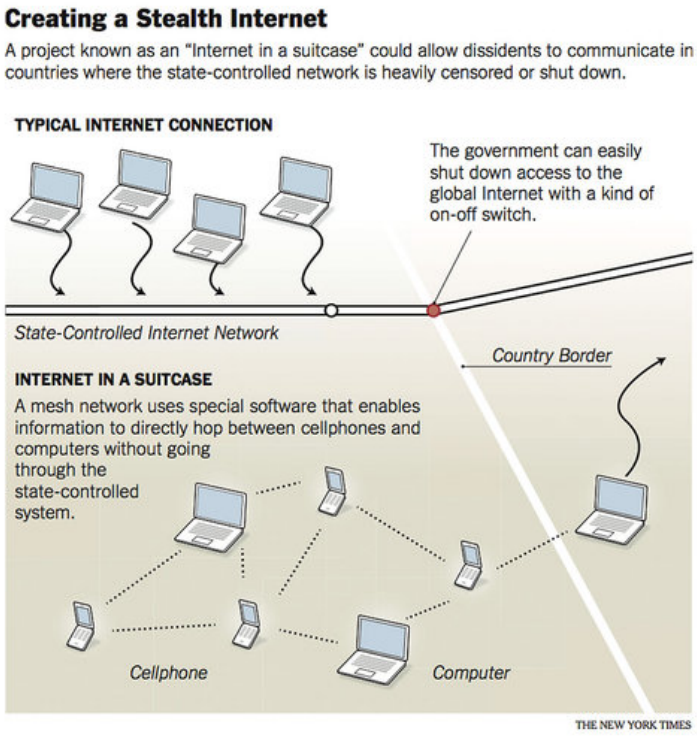

Figure 3. The Internet Suitcase[29]

Another key characteristic of a system like the Internet in a suitcase, that is important to highlight, is that it operates on a completely different pathway from what the government and general citizenry are using. This makes stealthy Internet connectivity hardware and software different from traditional circumvention tools (which will be discussed in depth later in this chapter). Traditional circumvention tools, such as proxy websites, while operating on the global Internet, are usually accessed through state-controlled ISPs. Internet provided by stealthy technology avoids these state-controlled ISPs. A second example of an emerging means of controlling social media's key terrain is Bluetooth technology.

Traditionally, Bluetooth technology is used to facilitate a headset communicating wirelessly with a cell phone, or for an iPod to play music wirelessly through a stereo. However, technology that is being partially funded by the U.S. State Department will

[29] Glanz and Markoff, "U.S. Underwrites Internet Detour."

allow dissidents to make slight software modifications to their cell phones that will open up new communication capabilities. This new technology would, for example, allow a video of a protester being beaten by state police to jump from cell phone to cell phone automatically within a network of trusted insurgents.[30] As the circle of trust within the insurgent group widened and more people were brought into the movement, the dissemination of such information would increase as well.

With an explanation of how the Internet functions and a discussion of the importance of Internet connectivity complete, the thesis will discuss how social media platforms actually operate. Understanding how these sites function is important, because individual social media sites, such as Facebook and Twitter, represent avenues of approach within the social media environment. These avenues of approach, which can also be conceptualized as the various options available to navigate the social media environment, allow individuals to connect with the people and information that will help facilitate an insurgent group's desired end state.

B. SOCIAL MEDIA PLATFORMS—AVENUES OF APPROACH

A major social network website, such as Facebook or Twitter, requires a combination of powerful software and hardware. Despite different functionalities provided by each social media platform, there are many similarities in how each platform functions. First, most social networks use open-source software.[31] In fact, nearly all of the operating systems behind sites such as Twitter, LinkedIn, and MySpace are Linux based (Facebook uses F5 Big-IP). Additionally, most social media sites use Apache Web server and MySQL as their database management system. In order to respond to millions of users' simultaneous demands on the platforms, social media sites predominately use software called Memcached to handle the massive data requirements of the various social

[30] Glanz and Markoff, "U.S. Underwrites Internet Detour."

[31] Steven Vaughan-Nichols, "How Social Networking Works," IT World, http://www.itworld.com/software/91803/how-social-networking-works (accessed November 12, 2012).

network applications.[32] In addition to the multitude of layered software applications, social network sites need massive amounts of computer hardware to operate.

The most extreme example of the type of hardware necessary to run a major social networking site is Facebook. The Silicon Valley based company uses over 30,000 servers to handle the hundreds of billions of page views the company serves up every month.[33] Each site uses high powered switches to connect each of their servers. Finally, enormous storage servers are built to store the petabytes (10^{15}bytes) of user data. Typically these data centers are located near major Internet NAPs so that they can be connected to the fastest Internet connections possible. With these massive systems costing hundreds of millions of dollars, most individuals will never be able to build a social network on this scale. However, by realizing and understanding that social networks are built on open-source (often free) software, individuals, including those working for revolutionary change, can easily and quickly start their own, fully functional social networks.

There are dozens of companies and software applications that allow individuals to start social network websites. Examples include Elgg, Lovd by Less, Drupal, and Pligg. Even easier to deploy is Ning. Ning is a simple, turn-key program that allows customers to have a social media website up and running in a matter of minutes. For as little as $49.00 a month (price as of March 31, 2013), individuals can host up to 10,000 members. Doubling the payment to $99.00 a month allows a website creator to host up to 100,000 members.[34] Ning's customizable templates include custom member profiles, a blog and forum feature, photo and video embeds, group pages, events, chat, and privacy options within the network. Additionally, the site can integrate seamlessly with other social media sites such as Facebook, Twitter, LinkedIn, Google Plus, and others. Ning sites are also optimized for mobile applications such as smartphones.[35]

---

[32] Vaughan-Nichols, "How Social Networking Works."

[33] Ibid.

[34] Ning.com, "14-Day Trial on all Plans," Ning.com, https://www.ning.com/pricing/ (accessed March 31, 2013).

[35] Ibid.

This easily created social network platform provides another potential option for those wishing to take advantage of the power of social media as a communications platform, yet allowing them to stay off the radar of oppressive regimes. With companies like Ning and others providing such a powerful, low cost social media option, the social media environment will continue to grow and evolve. These platforms can be viewed as a type of cover and concealment among the virtual operating environment. Following this overview of how the Internet and social media platforms function, the author refers to Figure 4 which is a model to facilitate the understanding of the competitive environment that is social media.

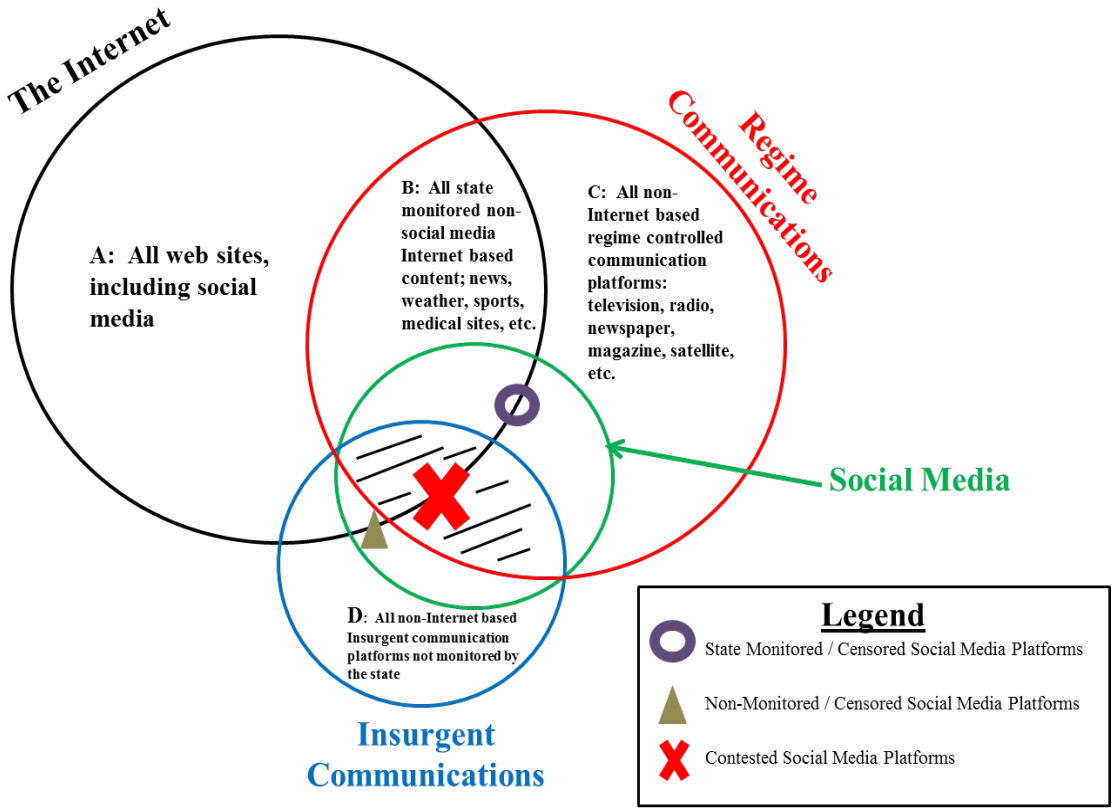

Figure 4. A Model of Select Communications Platforms

Just as military service members use maps to help visualize and understand the physical terrain in which they will operate, those working in the cyber domain will be aided in their understanding of the social media environment by studying a graphical

representation of that environment. Figure 4 is a model designed for that purpose. The model is comprised of seven basic parts. The three principle components are labeled with various symbols described in the legend. The four other components of the model are labeled "A" through "D" and a brief description of each is contained within the model itself.

Section A represents the Internet as a whole including social media and websites of both a political and non-political nature. Examples include business websites, financial websites, news websites, websites about sports, leisure activities, or the weather. Section B is a representation of Internet content, excluding social media sites, that is monitored, censored, or blocked by the ruling regime. Some of the same types of Web content included in Section A would be included in Section B. The difference, though, is that the content in Section B is of concern to the regime. If foxnews.com were blocked by the Iranian government, it would fall into Section B. Section C includes all regime controlled, non-Internet based communications platforms and channels. Examples include state run television programming, radio stations, magazines, and newspapers. Section D of the model represents all non-Internet based communications platforms that insurgents use either outside of the regime's control or not monitored by the state. Examples include underground newspapers, pirate radio stations, citizens band (CB) radio, and informational pamphlets. The three principle sections, represented by the symbols in the legend, are all social media based and form the heart of the model.

The triangle represents the social media platforms that are used by the insurgents, but which are not actively monitored by the state. Examples of social media sites that would fall into this section include Wael Ghonim's Facebook page, "We are all Khaled Said," and the website Goodreads.com. That Facebook page was a key website for the organization and mobilization of Egyptian citizens who wanted to protest against the Mubarak regime. Goodreads.com is a social networking website that is designed for book enthusiasts to discuss their favorite reads. Iranian dissidents used the site to discuss

problems with the Iranian regime. This website was not on the Regime's censored list until a story by the *Los Angeles Times* exposed how the Iranian dissidents were using the website.[36]

The example demonstrates how the model can change as Goodreads.com once fit into the triangle space (an unmonitored social media platform used by insurgents), but was pushed into the circle space (monitored/censored social media platforms). Another example of social media websites that insurgents could use that would not be monitored or censored are newly created sites that utilize turnkey solutions such as those provided by Ning mentioned above. However, the problem with using a new social media website is getting enough users so that information disseminated on the site gains widespread readership. An insurgent group could have the most powerful video content, yet if viewed by only a few people, it basically would have no power to influence others. The circle section represents social media that is actively monitored and censored (or blocked) by the state.

In Iran, popular social media websites such as Facebook and Twitter are blocked by the government. Thus, Facebook and Twitter are examples of social media sites that would fall into the area represented by the circle for the country of Iran. The last section of the model is represented by an X and is the social media space that is being censored by the state, but also being used by dissidents, and is thus contested. An example of contested social media space is the Chinese social media website Sina Weibo.

Sina Weibo is China's most popular micro-blogging site with over 500 million users. However, the Chinese government actively monitors the accounts of over 300,000 users who have at least 1,000 followers.[37] This influential group is closely watched, and if something posted on the Sina Weibo network is not approved by the Chinese

---

[36] Evgeny Morozov, "How Dictators Watch Us on the Web," *Prospect Magazine*, November 18, 2009, http://www.prospectmagazine.co.uk/magazine/how-dictators-watch-us-on-the-web (accessed November 21, 2012).

[37] The Economist, "Monitoring the Monitors," *The Economist*, July 10, 2012, http://www.economist.com/blogs/analects/2012/07/online-censorship (accessed November 20, 2012).

government, the comments are deleted from the network almost immediately.[38] So on one hand, China has banned social media sites like Facebook and Twitter, but on the other hand, China allows its citizens to use social media via sites like Sina Weibo. The caveat of course is that the Chinese government is very conscientious in monitoring the "approved" social media websites. Thus, the most active, popular users of social media in China play a cat and mouse game with the government censors, thereby making sites like Sina Weibo contested space in the social media model.

With this explanation of how social media sites actually function, and exploration of a model that represents the competitive environment, the author will discuss technologies used to control information on the Internet and social media websites. This information is summarized in Table 1. One important consideration is that all of these censorship tools are only necessary when the regime in question does not have jurisdiction over the website that is hosting the prohibited content. If the website host is located in the censoring regime's purview, the government can simply order the content removed. These tools come into play when the website is located outside of a regime's jurisdiction.

[38] Economist, "Monitoring the Monitors."

Internet Censorship Tools			
1. Social Filters: A citizens own self censorship; combined with political filters, it is a powerful tool			
2. Legal Filters: The laws and regulations a country imposes on its citizen's use of the Internet			
3. Technical Filters: The technical means a government uses to censor the Interenet; there are multiple examples			
Name of Filter	**How It Works**	**Advantages**	**Disadvantages**
IP Block Filters	Blocks the IP address of an individual computer or server making the machine inaccessible	Require very little computing power	Technique is very blunt; blocks entire addresses
		Can be used on all backbone connections in a country	Cannot block individual stories on a given web site
			If two individual web sites are co-hosted on the same IP address, both sites will be blocked
DNS Block Filters	Blocks the DNS names of offending web sites. A DNS name is the plain text name (google) of an IP address.	Unlike an IP Block filter, if two individual web sites are co-hosted on the same IP address, a DNS blocker can block one web site, but not the second	Typically involves "overblocking" like IP Block filters, as individual stories cannot be blocked
Keyword Block Filters	Examines content of data traffic, looking for a specific URL or offending keywords in emails, etc.	Much more precise compared to IP and Keyword block filters; can block msn.com/politics, while not blocking msn.com/sports for example	Very expensive to implement, must examine entire streams of digital content, not just short destination
			Can be bypassed with simple encrpytion
		Can be used on any data application; web pages, emails, IMs, etc	Cannot be used against non-text data
Search Results Removals	A government simply requests that search providers such as Google omit certain search results when specific words are phrases are searched for	Costs the requesting government nothing	Completely reliant on search companies in order for this to work
		If search provider agrees to censor search results, this technique can be very effective	Risk of public backlash if requests are made public
Internet Shut Downs	A government shuts off access to the Internet	Effective at preventing the use of social media	Causes world-wide backlash
			Can do more harm than good to the government in power

Table 1. Internet Censorship Tools

C. TECHNOLOGIES FOR CENSORING, MONITORING, AND LOCATING

In 1985, then U.S. Secretary of State George Shultz proposed a concept he called the dictator's dilemma. The idea was that totalitarian leaders must choose between allowing citizens to access and use newly developed communication technologies, thus accepting the potential these tools have to subvert their authority, or to block access to these platforms and suffer the inevitable economic slow-down.[39] The recent events in North Africa and the Middle East point to a digital dilemma which is forcing dictatorial leaders to make the same kind of choice outlined by Mr. Shultz.

As the world witnessed in Egypt, some leaders are willing to suffer economic and public relations damage to try to stop popular uprisings. In order to deter, prevent, and ultimately stop insurgent activity, governments utilize a variety of means to control content on the Internet. In particular, social media content and platforms are singled out for censorship. Before examining the particular techniques that are used to control

[39] Hal Roberts, Ethan Zuckerman, and John Palfrey, "2011 Circumvention Tool Evaluation," Berkman Center for Internet & Society at Harvard University, http://cyber.law.harvard.edu/publications/2011/2011_Circumvention_Tool_Evaluation (accessed November 10, 2012), 1.

information on the Internet, the thesis will discuss the basic points of connectivity that a government can manipulate in order to control the content that its citizens view when using the Internet. By building in features to control Internet connectivity, a government gains control of the key social media terrain.

D. CENSORING THE INTERNET—A GOVERNMENT'S ATTEMPT TO CONTROL KEY TERRAIN

A filter can operate on various Internet connection points. Examples include the actual client's machine which is requesting data, the server designated to return the requested data, or the network between the client and the server during either the initial request or during the response.[40] Client-side filtering is not a truly viable option, as it would require placing software inside every browser on every computer (easily circumvented by installing new browsers). Server side filtering can work, but it requires the hosting content owner to provide active support to the government's request that certain content on the Internet be filtered in their county.[41] Alternatively, the servers could be attacked using tactics such as a denial of service attack. The third place for filtering are locations such as routers and DNS servers that help deliver content to users. Because the majority of Internet data travels on a relatively small number of huge backbone data pipes (before being routed off onto small regional network pipes), filtering countries will typically input large lists of prohibited keywords onto those Internet routers that control the data flow on the backbone data pipes.[42] These routers then block data that contains the blacklisted keywords.

Ultimately, most filtering countries use a combination of social, legal, and technical filtering methods, which are described in detail below. The most aggressive Internet filtering countries, such as China, will use a combination of overlapping

---

[40] Hal Roberts, Ethan Zuckerman, and John Palfrey, "2007 Circumvention Landscape Report: Methods, Uses, and Tools," Berkman Center for Internet & Society at Harvard University, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2007_Circumvention_Landscape.pdf (accessed November 10, 2012), 10.

[41] Ibid., 11.

[42] Ibid., 11.

methods. The first two types, social and legal, are means by which the government tries to prevent its citizens from accessing certain Internet content. These types of filters can be considered the obstacles within the social media environment.

1. Social Filters—Obstacles

Although at first glance it seems counter-intuitive, the most powerful filters of Internet content are not powerful computers with technically advanced software, rather they are the citizenry's own self-imposed restraints in not trying to access forbidden information.[43] This social pressure prevents the vast majority of people living in countries that censor the Internet from going to websites or searching for information about topics that are forbidden. This unfortunate circumstance, combined with the effort and technical knowledge needed to use circumvention tools, is often all that is needed to prevent people from accessing information on the Internet. If social pressures fail, legal pressures serve as the next line of defense against a citizen's ability to freely surf the Web.

2. Legal Filters—Obstacles

Political pressure is normally applied through a country's laws and regulations. Although arrests for accessing restricted information on the Internet is not commonplace, the mere threat of being arrested for accessing certain websites or content on the Internet is often enough pressure to prevent people from trying. Additionally, in countries like China, businesses that provide Internet access are under close surveillance by government authorities. Still further, many Internet cafes in China are required to request and record an Internet user's credentials.[44] These additional obstacles make it more difficult for Internet café users to access information that the government does not approve of and helps the government keep known political dissidents under careful watch.

Technology such as radio, television, newspapers, and even the Internet itself, allows the government to communicate which types of information its citizens should

[43] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 9.

[44] Ibid, 9.

avoid. Putting this information out to the masses creates the first two types of filters, social and legal. Then, if these both fail, the technical filters (actual blocking) kick in to prevent individuals from accessing restricted content.[45]

3. Technical Filters—Observation and Fields of Fire

Technical filters represent the first letter in the OAKOC framework, observation and fields of fire. They allow a repressive government to "see" the social media environment. Whether it is setting up fake proxy sites, or actively monitoring social media users with over 1,000 followers, such as in China, the hardware and software used to monitor and censor Internet users gives the regime a means to observe where an insurgent might maneuver within this competitive landscape. These filters serve as the first and last lines of defense against unwanted information getting into the hands of citizens living in countries that want to control the information its citizenry reads. There are a multitude of technical filters, the most prominent of which are discussed in the following subsections.

a. IP Block Filters

The most straightforward and basic means of blocking traffic on a router (and thus the Internet) is to block the IP addresses (the number used to identify each specific machine on the Internet) of servers hosting the information that a government wants blocked.[46] Basically, once a machine's IP address is blocked, it becomes inaccessible. This method is simple, requires very little computer power, and can be used on a large scale. The drawback is that it blocks everything at a given site. Individual stories on a specific site cannot be blocked using this method. It is either "all or nothing." Still worse, some Web hosting firms actually combine hundreds of individual websites onto a single IP address. Therefore, when the offending website shares an IP address with

[45] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 10.

[46] Ibid., 11.

other websites, even completely unrelated ones, all of those websites will be blocked. This makes IP block filters the equivalent of a sledgehammer, as opposed to a surgical tool, when it comes to Internet filtering.

b. DNS Filters

The DNS filters block looking up specific domain names (google.com or foxnews.com, for example). To block specific name lookups, a government need only send a list of domain names to block to each DNS server operating in that particular country. Like IP filtering, DNS filters block entire domains. A specific news story on msn.com cannot be blocked without blocking the entire msn.com domain. However, if two sites are co-hosted by a server with the same IP address, DNS blocking can block one without blocking the other. So, msn.com could be blocked while foxnews.com could remain unblocked, even if both sites were hosted on the same IP address. This is one advantage of DNS filters over IP address blocking.[47] From the government's point of view, however, DNS filters may not be the most effective means of preventing citizens from accessing certain websites because a client computer can either be configured to use DNS servers in an outside, non-filtered country, or use a non-filtered DNS server inside the country that is doing the filtering.

c. Keyword Filters

Keyword filters go a step further than both IP filters and DNS filters. Keyword filters actually examine the content of the data traffic between clients and servers. Further, they can look at content in any part of the requested data, be it a specific uniform resource locator (URL) in a Web request or an offensive word/phrase in an email.[48] This capability allows keyword filters to be much more precise. So, for example, www.espn.com/football can be blocked while www.espn.com/baseball may be transmitted freely. Also, specific phrases deemed offensive to the filtering government, "Taiwan independence" in China for example, can be blocked using a keyword block

[47] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 12.

[48] Ibid., 12.

filter. The downside to this technology is that it is much more expensive compared to IP filtering and DNS filtering. Just as other filtering techniques, keyword filters can be circumvented.

Internet users can prevent filtration by keyword blockers by using encryption on all data that is sent over the Internet. However, this technique only works with hyper-text transfer protocol with secure sockets layer (HTTPS) sites that support SL/TLS. Additionally, non-text data is basically impossible to filter via keyword filters.[49] In addition to these technical means of filtering Internet content, governments use other means to control the flow of information to their people.

4. Search Results Removals

A transparency report from search engine company Google indicates that dozens of governments, even the United States and other western democracies, are requesting that Google censor or block certain Web pages from populating a user's search requests. For example, government regulators in Spain asked Google to omit 270 different search results that linked to articles and blogs that referenced various public figures, including mayors and prosecutors. Poland sent Google a request to remove links to websites that criticized several unnamed public institutions. Various United States government agencies requested a total of 6,192 pieces of Internet content be removed from search results, blog posts, or archives of online videos during the second half of 2011, up 718 percent from the six months just prior.[50]

5. Content Removals

In addition to search result removals, governments can ask companies to remove content that they host. One such request came from Canadian officials, who asked Google, the owner of YouTube, to delete a YouTube video that showed a Canadian citizen urinating on his passport and then flushing it down the toilet. Regardless of the

---

[49] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 12.

[50] John D. Sutter, "Google Reports 'Alarming' Rise in Government Censorship Requests," CNN, http://www.cnn.com/2012/06/18/tech/web/google-transparency-report (accessed February 13, 2013).

requesting government, or the subject of the request, the overall trend of governments asking Google and content providers to censor search results or delete content is on the rise. These requests are simply another option in a government's arsenal of censorship tools.

6. Shut-Downs

In the event that all other methods and technologies fail, a governing body can choose to simply cut off Internet access to its people. The government of Myanmar, for example, shut off access to the Internet completely when it found out citizens were reporting on the Saffron Revolution. These protests were fueled by the government's decision to double the price of petrol and diesel, while increasing the price of compressed natural gas (which powers public buses) by five-fold.[51] This was crude but effective in preventing many pictures and videos from the protests from making it to mainstream media outlets.[52]

The Chinese government, while never completely shutting down the Internet in the entire country, did shut down the Internet in Xinjiang province for 10 months between 2009 and 2010 to help subdue the riots in Urumqi.[53] These riots were the result of ethnic tensions between the Muslim Uighurs and the Han Chinese, which highlighted the deep seated frustrations felt by numerous minority groups in western China.[54] A third, and probably the most infamous example of a government going to this extreme measure to gain control of the Internet occurred in Egypt during the Arab Spring.

The Mubarak regime, fearful of the growing volume of social media-based protests, cut off all communications in Egypt on January 29, 2011. Not only did the regime "pull the plug" on the Internet, it also shut down all three cellular telephone

[51] BBC News Staff, "Burma Leaders Double Fuel Prices." The BBC, http://news.bbc.co.uk/2/hi/asia-pacific/6947251.stm (accessed February 15, 2013).

[52] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 3.

[53] Roberts, Zuckerman, and Palfrey, "2011 Circumvention Tool Evaluation," 1.

[54] Edward Wong, "Riots in Western China Amid Ethnic Tensions." *The New York Times,* July 6, 2009, http://www.nytimes.com/2009/07/06/world/asia/06china.html?_r=0&pagewanted=print (accessed November 22, 2012).

operators and all short messaging services (SMS).[55] This action ultimately ended up being counter-productive in that it brought awareness to the masses that a challenge to the regime was taking place and signaled to the people that it was time to go into the streets in protest. The situation in Egypt provides an excellent example of how much power the Internet inherently holds, and how dictatorial leaders fear the free flow of information to their citizens.

In the overall examination of government's efforts to censor the Internet, it is the combination of social, political, and technical filtering that proves most effective. These means, and the continued increase in removing search results from major search engines, are effective in preventing the vast majority of citizens living under repressive regimes from freely accessing information. Therefore, despite the fact that most circumvention tools can overcome technical filters, the vast majority of citizens living in countries that censor the Internet are effectively prevented from viewing prohibited content.[56]

Understanding how Internet filters work, and more importantly to the insurgent, figuring out which Internet controls their particular government is utilizing, is important because from this information, an insurgent group can develop a plan on how to circumvent these government efforts. Additionally, this information will assist a revolutionary to determine the best ways in which to utilize social media, given their understanding of the specific social media environment that they will be operating in. Many of the conditions that make up the realities of a specific country's digital environment are created by the various means a country implements to repress the free flow of information to their citizens. Therefore, the better an insurgent understands the social media environment, the better he or she will navigate within the environment. In addition to censoring social media platforms and the Internet, governments also conduct cyber-based surveillance.

---

[55] Wael Ghonim, *Revolution 2.0* (New York: Houghton Mifflin Harcourt Publishing Company, 2012), 212.

[56] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 10.

E. SURVEILLANCE—OBSERVATION AND FIELDS OF FIRE

Governments, and those that oppose governments, have the ability to conduct surveillance of the opposing side using a number of methods and tools for collection. Additionally, each side has the ability to collect various types of data that can provide greater situational awareness about their opponent. Examples of the types of data that can be collected using cyber-based tools include real-time communications (Internet traffic, mobile phone calls, SMS messages, hidden microphones and video cameras), communication headers from digital message traffic (the to/from of an email message for example), relational data derived from social networks (open source information gained from various social media websites), the content stored either online or on a user's hardware, billing data, and locational data.[57] Additionally, there are five principle cyber-surveillance methods. These methods are open source collection, client/customer/visitor (CCV) tracking, remote monitoring, communications intercepts, and data requests and seizures.[58]

Open-source collection refers to looking for information on platforms that are available to the public and are unclassified in nature. Examples include social media websites such as Facebook and Twitter. The types of data available from these well-known platforms can include locational information, especially when users allow their created content to be geo-enabled. An example of this type of data collection can be found by examining the software called Creepy. Creepy allows a user to quickly obtain geolocation aggregator data.[59] The easy-to-use software provides the location (on Google Maps) of social media users who share their locations. The only data needed to obtain this information is the user name of a person's Twitter or Flickr account. The CCV tracking involves collecting the data that is captured when someone visits a website.

---

[57] Dorothy Denning, "Cyber Surveillance," Lecture presented at the Naval Postgraduate School, Monterey, CA, January 13, 2013.

[58] Ibid.

[59] CNET Staff, "Creepy: CNET Editor's Review," CNET.com, http://download.cnet.com/Creepy/3000-12941_4-75445808.html (accessed May 21, 2013). Please note that a free download of Creepy software is also available at the above link.

Powerful (and often free) software allows website owners to collect a wealth of data on individuals when a person visits a website, including information about the user's browser, operating system, and IP address.

Also, the products and services that people use, including mobile phones, tablets, and computers, may provide a wealth of information to their vendors. All of this data collected by site owners and vendors could be turned over to a government on demand. Remote monitoring involves watching, listening, and/or recording the activities of a person or group using assets that do not require physical proximity to the target of the surveillance effort. This type of monitoring can be done in a number of ways. Software can be installed on computers that allows a person's webcam to be turned on and controlled from afar.

Crowdsourcing is another technique for conducting remote monitoring. In the United Kingdom, for example, paid members can watch participating store's in-store security cameras to try to catch shoplifters. The Border Sheriff's Coalition in Texas allows closed circuit television cameras to be watched by civilians, who can report suspicious activities on the border. Another example is the PlaceRaider application for Android phones. This software can turn on a person's mobile phone camera and provide a three dimensional model of the phone's surroundings as well as provide close-up images.[60]

There are a number of ways to conduct communication intercepts. These methods include placing taps in telecommunications switches or in the routers that control the flow of information on the Internet.[61] Also, signals can be captured both in the air and over communication lines. Remote access software can be installed on a target's computer which will allow information to be retrieved from the computer. Another method is to simply plant microphones or other listening devices on a target's devices.

[60] Denning, "Cyber Surveillance."

[61] Ibid.

The fifth method of cyber surveillance is through data requests and seizures. This method involves states forcing service providers to provide digital records of their users. A typical seizure could involve the gathering of emails, SMS messages, call logs, or Web logs.

Having discussed how governments try to control information on the Internet, and how governments conduct cyber-surveillance, the author will now examine the ways to circumvent these efforts. Circumvention technologies and techniques comprise the final letter in the OAKOC framework, cover and concealment. The various ways in which an insurgent can navigate or act within the social media environment represent the camouflage of this competitive space. Some of the most common circumvention technologies are summarized in Table 2.

Circumvention Tools			
1. Encryption:	**Basic purpose is to hide digital content**		
2. Proxies:	**Basic purpose is to hide the desitination of a data request; there are multiple types**		
Name of Proxy	**Advantages**	**Disadvantages**	**Software Required?**
HTTP	Operator can use browser transparently	Requires trust in proxy operator	Yes (or manual configuration of browser)
	Multiple non-circumvention related uses of HTTP proxies	Users have to contiually seek out new HTTP proxies	
		Public HTTP proxies generally do not provide encryption	
		Detectable changes are left behind on a users computer	
CGI	No trace of use left behind on users computer	Requires trust in proxy operator	No
	Can be used on public / locked computers (library, café, etc)	Requires an alternate browser within a browser	
		Circumvention exposed if wrong URL window is used	
		Typically does not provide encryption	
IP Tunneling	Operator can use browser transparently	Requires trust in proxy operator	Yes
	Multiple non-circumvention related uses of IP Tunnels		
	Supports more than web browsing: email, IM, file sharing		
	Can be created multiple ways: VPNs, SSH, & HTTP Tunnels		
Re-Routing	Can use browser transparently once software is installed	High cost to use and establish	Yes
	Does not require trust in system operator-uses multiple proxies	Requires a lot of bandwidth to operate	
	Data is encypted at each individual proxy	Generally slow performance compared to other methods	
Distributed Hosting	Stores multiple copies of data requests on multiple servers	Requires trust in proxy operator	Yes (or manual configuration of browser)
	Can use browser transparently once software is installed	No distributed hosting systems developed for end users	
	Provides redundency is the primary server is attacked or down		

Table 2. Circumvention Tools

F. CIRCUMVENTION TECHNOLOGIES—COVER AND CONCEALMENT

The idea that it is important to have free media expression in closed societies is not new. Efforts to this end include Radio Free Europe and Radio Liberty. These two

radio stations played a significant role in ending state communism in the Soviet Union.[62] Building on this lineage, digital communication technology, especially social media technology and the potential it brings to communicating with the masses, has reinvigorated the call to push for free media expression across the globe. On the other side of the coin, dictatorial leaders have also recognized the potential that social media has on ultimately deciding who wins the battle of the narrative. Therefore, it is important for those working for freedom of information to find ways to keep the lines of communication open on the Internet. The next few sections of this chapter will focus on the technological aspects of accessing information on the Internet when a state entity is trying to prevent unfiltered access to the Internet. These technologies will fall under the categorical title of circumvention tools.

All circumvention methods use some combination of hiding the content (encryption) and/or the destination (proxies) of digital information.[63] Most simply, proxies conceal destinations and encryption conceals content. Circumvention tools work by allowing users to bypass Internet filtering and access blocked content. Although there are multiple types of circumvention tools such as Web proxies, virtual private networks (VPNs), and HTTP/SOCKS proxies, they all provide connections to Internet sites that would otherwise be blocked.[64] Another way to view circumvention tools is to conceptualize them as virtual ISPs, which reroute an Internet user's traffic around a government's blocking filters.[65] An example of a very basic proxy service will make the idea behind circumvention technology easy to understand.

> A user in China who cannot reach http://falundafa.org directly can instead access a proxy machine like http://superproxy.com/, which can fetch http://falundafa.org for the user. The network filter only sees a connection

[62] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 3.

[63] Ibid., 13.

[64] Hal Roberts et al., "2010 Circumvention Tool Usage Report," Berkman Center For Internet & Society at Harvard University, http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage (accessed November 17, 2012), 2.

[65] Ibid., 5.

> to the proxy machine (superproxy.com), and so long as the proxy itself remains unfiltered, the user can visit sites through the proxy that are otherwise blocked by the network filter.[66]

In general, most circumvention tools work as intended, but there are some drawbacks. If, for example, China decides to block the proxy site (superproxy.com in the above example), then any requests sent through the proxy will not work.

Despite the advantages that proxy technologies (and other circumvention tools) bring to Internet users, there are some serious concerns and drawbacks that must be considered before using these technologies. These considerations will be fully explored later in the chapter, but as an example, using a proxy requires double the bandwidth compared to a non-proxy connection. This may not impact users in the United States much, but in less developed parts of the world, bandwidth is a major factor to consider in understanding the social media environment. Also, most circumvention tools (Tor being a notable exception) require users to place a high amount of trust in the tool's developers, as the developers could share, lose, or sell user data to potentially dangerous third parties (including a repressive regime).[67] Finally, in trying to understand the role that circumvention tools play within the social media environment, one must keep in mind that there are no absolutes in either filtering (by the state) or circumvention (by dissidents). It is a resource battle between the two sides, and the landscape is constantly evolving.

Another interesting aspect to this topic is that in countries with aggressive Internet filtering, there are not a lot of people using circumvention tools. A 2009 research report estimated that only two percent of all Internet users in countries where filters are in place used circumvention tools.[68] One reason for this low percentage is that social pressure to avoid known, prohibited websites is a powerful filter in and of itself. This, combined with the initial burden to actually acquire, implement, and use a circumvention tool, serves as

---

[66] Hal Roberts et al., "2010 Circumvention Usage Report," 2.

[67] Ibid, 5.

[68] Ibid, 7.

a deterrent. Other reasons that explain this low usage rate include the fact that some of the tools do not work as well as advertised, governments keep circumvention tools off search provider search results, and circumvention tool users can face incarceration.[69] This is an important consideration for SOF personnel who are conducting UW. The training provided to the insurgents they are supporting may need to include how to use circumvention tools.

A follow up of the 2009 study, published in October, 2010, solidified the findings of the initial report in that in the roughly two years between the studies, the percent of all Internet users utilizing circumvention tools in countries that filter content rose to only three percent.[70] Another key finding of this later study is that most users only utilize simple Web proxies, and not more sophisticated and potentially more effective circumvention tools. This situation appears to be occurring because users are entering simple search terms such as "proxy" in their search engines, which overwhelmingly return lists of simple Web proxies or HTTP/SOCKS. Additionally, people in countries, such as China, with aggressive Internet filtering systems, may simply prefer websites written in their native language, by other Chinese people, about subjects that directly affect their local communities.[71]

Despite this relatively low percentage of users, it is important to understand that it only takes a select group of people who are highly connected socially in their local communities for the impact of circumvention tools to be significantly magnified. Bestselling author Malcolm Gladwell calls these types of highly connected people connectors, mavens, or salesmen.[72] Thus, if a core cadre of users can distribute information they find by using circumvention tools to access otherwise blocked websites, or they post information on websites for the world to see, then the effect is basically that of a larger number of Internet users utilizing circumvention tools in Internet filtering

---

[69] Hal Roberts et al., "2010 Circumvention Usage Report," 7.

[70] Ibid., 2.

[71] Ibid., 13.

[72] Malcolm Gladwell, *The Tipping Point* (New York: Back Bay Books, 2002), 30–88.

countries.[73] This is the idea championed by Professor Xiao Qiang, who teaches that a small number of internationally connected activists can be extremely effective by using their highly connected status to disseminate key information through local networks. These individuals, therefore, can act as social bridges or the information brokers between the international community and their local neighborhoods.[74]

Following is more detail about circumventing Internet filtering. The two principle ways are encryption and proxies. There are several proxy methods. These include HTTP proxies, CGI proxies, IP tunneling, re-routing, and distributed hosting.

1. HTTP Proxy

An HTTP proxy is a software tool that allows an Internet user to use his or her existing browser transparently. That is, the user will not notice a difference in how the browser looks or operates. Basically, an HTTP proxy acts as a middleman between a requesting client and a destination server. The HTTP proxies take requests from their clients and hold them. The proxy server then sends what appears to be an independent request to the ultimate destination server, and then returns the response from the destination server to the client. Therefore, it appears that no communications has occurred between the client and the final destination server. A person wanting to use the Internet anonymously must be careful using HTTP proxies because a resourceful government could put up its own public proxies for the purposes of spying on its citizens.[75] This would be an example of government using technical tools to observe the social media environment. Also, most proxy sites do not provide encryption. However, circumvention tools that use an HTTP proxy avoid the aforementioned problem found in simple proxies.

---

[73] Hal Roberts et al., "International Bloggers and Internet Control," Berkman Center for Internet & Society at Harvard University, http://cyber.law.harvard.edu/publications/2011/International_Bloggers_Internet_Control (accessed November 20, 2012).

[74] For more information on social bridges and information brokers, see Patti Anklam, *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World* (Oxford: Buttersworth-Heinemann, 2007), 77.

[75] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 14.

First, circumvention tools that use HTTP proxies automate the process of locating HTTP proxy sites that are not blocked and then configuring a user's Internet browser to use the unblocked HTTP proxy.[76] Second, the majority of circumvention tools that utilize HTTP proxies actually host their own proxy servers. This means that users of the circumvention tool can trust the proxy server as much as they trust the developer of the actual circumvention tool. Finally, most circumvention tools that use HTTP proxies will only connect to proxy servers that are encrypted. This means that the tools can circumvent surveillance and keyword filtering.[77]

In wrapping up the discussion of HTTP proxies, it is important to note that using an HTTP filter on a computer leaves detectable changes on the user's computer. This means that a confiscated computer that has been using an HTTP filter will contain evidence of its use. This is an important consideration for SOF personnel who are using this type of proxy on a computer while in a denied area. Also, it must be remembered that HTTP proxy programs can only be trusted as far as one is comfortable trusting the operator of the proxy server.[78]

2. Common Gateway Interface (CGI) Proxy

A CGI proxy works by using an alternate Web browser within an existing Web browser. Typically, a CGI proxy appears as a second URL address bar under a user's normal URL address bar. To use the CGI proxy, one must remember to use the correct address bar, otherwise there will be no proxy function. Although this sounds simple in concept, it is easy for someone to mistakenly access the Web through the incorrect address bar and inadvertently give out location information.[79]

The CGI proxies work by taking a client's request and embedding it in the data portion of an HTTP request.[80] This embedded request goes to the CGI proxy server.

---

[76] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 14.

[77] Ibid, 14.

[78] Ibid., 13.

[79] Ibid, 15.

[80] Ibid., 14.

After this, the CGI proxy server finds the final destination information, sends out what appears to be its own data request, and then returns the appropriate data to the user of the CGI proxy.

The CGI proxy users experience similar problems to HTTP proxy users. The CGI proxy sites are always at risk of being blocked, they lack encryption, and require a user to trust the proxy host.[81] Despite these potential problems, CGI proxies do not require clients to install any software on their Web browsers. This means that no trace of software is left behind on a user's computer. Additionally, CGI proxies can be used on locked computers such as those in a library, Internet café, or university setting. Thus, CGI proxies may be a superior option for U.S. SOF personnel using social media technology while abroad.

3. IP Tunneling

Unlike a CGI proxy, IP tunneling does require the installation of client side software.[82] However, IP tunneling allows clients to use their normal Web browsers in a transparent method. Another advantage of IP tunneling is that it can be used for more than just Web traffic in terms of its circumvention function. There are basically three types of technologies used for IP tunneling. These technologies include virtual private networks (VPNs), HTTP tunnels, and secure shell (SSH) tunnels.

The VPNs are primarily designed to connect remote clients to private intranets. For example, the Naval Postgraduate School (NPS) allows students to connect to the school's online, intranet resources from home by logging into the NPS VPN. What this connection does, in addition, is to give a user an Internet connection that originates from the VPN host as opposed to the location of the client.[83] So for the purposes of revolutionary type activity, a user that is located in a filtering country, but is connecting to a VPN that is located in a non-filtering country, can access the Internet as if there were

[81] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 14.

[82] Ibid, 15.

[83] Ibid, 15.

no filters in place. Even better, a VPN provides circumvention for all types of IP applications. These applications include emailing, instant messaging, and file sharing.[84] The one glaring down-side of using VPNs (from an insurgent's point of view) is that they are relatively easy to identify. Therefore, VPNs are easily blocked. Thus, VPNs may be more effective in countries with less sophisticated censoring and surveillance capabilities.

An HTTP tunnel works like a standard HTTP/HTTPS request and response mechanism. Because of this feature, HTTP tunneling appears like normal HTTP traffic. This makes it much more difficult to detect and block an HTTP tunnel as compared to a VPN. The downside to this technology is that a user's Web browsing experience is typically much slower than that of a VPN.

The primary use of SSH tunneling is to provide secure remote access to an end user. The most difficult aspect of SSH tunnels is that they require an individual tunnel for every remote machine the user needs access to. Therefore, SSH tunnels are not very practical for Web browsing purposes.[85] They are good, however, for tasks such as consistent/efficient secure file sharing between two computers.

4. Re-Routing

Like other proxy methods, a re-routing proxy functions by routing a request for data through a non-filtered location (or locations in the case of a re-route proxy). Also, a re-routing proxy requires that a user install client-side software. Once the software is installed, the user can use his or her Web browser in a transparent manner. A key distinction between a re-routing proxy and the three previously discussed proxies (HTTP, CGI, and IP tunneling), is that all of the others require that a user place trust in the host of the proxy. This is always a concern because even if the proxy host is trustworthy, the host may be legally forced to divulge private data at any time.

A noteworthy advantage of a re-routing proxy is that it significantly decreases the amount of trust that one must place in the proxy host. The reason for this is that a re-

[84] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 15.

[85] Ibid., 16.

routing proxy actually routes the data through multiple proxy servers. Further, at each proxy, the data that is being transferred is encrypted.[86] This means that a single proxy server knows the immediate sources of the data and the next server the data is going to, but not the ultimate destination and the originating source. Therefore, a re-routing proxy user need only trust that the multiple proxy servers will not communicate and share data with each proxy in the chain of communication. So trust must be placed in the system as a whole, but not on individual proxy servers. Despite this added layer of security, re-routing proxy servers are still vulnerable to attack, and the revelation of the location of the proxy user.

If an entity, such as a state government, can correlate the time of the requests, where the origin of the request is known but the destination is not, and can correlate the responses, where the destination of the request is known but the origin is not, the state can learn both the origin and destination of a given set of data.[87] The key prerequisite for this scenario to be possible is that both the requesting user and the responding server must be physically located in the country that is doing the filtering. This means that a re-routing client is only at risk for detection if the client is browsing Internet sites that are located within the filtering country. A second key point is that the technology needed to do this type of two-way search is prohibitively expensive even for a government, especially when there are a large number of re-routing users.[88]

Another disadvantage to re-routing systems is that they require large amounts of bandwidth to operate. This, of course, makes running a re-routing proxy system expensive to operate. Each proxy in a re-routing system costs the same amount of money to operate as a single proxy server in one of the single proxy systems. Therefore, the operator of a three proxy re-routing proxy system must pay three times as much as the operator of a single proxy system. Using the assumption that there is a fixed amount of money to spend on a proxy system, the performance of a re-routing proxy system is

---

[86] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 16.

[87] Ibid., 16.

[88] Ibid., 16.

roughly equal to the inverse of the number of individual servers in the system (a two server system would have one half the performance of a single server system, a three server system would have one third the performance, and so on).[89]

G. DISTRIBUTED HOSTING

A distributed hosting proxy system provides multiple copies of data across multiple participating servers. Each individual server in the system has the ability to serve the requested data content to a client upon request. At its core, a distributed hosting proxy system is a caching HTTP proxy that has been optimized to store a large amount of the same data across different servers.[90] This type of proxy requires either the manual configuration of a client's Web browser or the installation of client side software for it to work. The obvious advantage of this system is that a user can still receive requested data even after the original server has been shut down. The original server may have been the victim of a directed denial of service attack, overwhelmed by sheer volume of requests, or may simply have experienced a malfunction. Either way, a distributed hosting proxy system can still get the needed data to the requesting client. Despite these advantages, it is important to note that no one has developed a distributed hosting system with circumvention as its primary intended use.[91]

By knowing about the various circumvention tool options, how each functions, and the relative advantages and disadvantages of each, a SOF operator will be able to better advise insurgents on using the best circumvention tools in terms of security, anonymity, functionality, cost, ease of use, and speed. This will allow an insurgent network to select the best circumvention tool for the specific social media environment in which it will be operating. Now that the various means to circumvent a state's attempts at blocking and/or monitoring Internet use has been examined, the thesis will look at the two principle proxy hosting models.

---

[89] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 17.

[90] Ibid., 17.

[91] Ibid., 17.

H. PROXY HOSTING METHODS

Circumvention tools generally rely on either a centralized proxy server in which a firm hosts its own project or on volunteer peer hosting. There are advantages and disadvantages to each of these general methods. Centralized hosting requires a user to put trust and faith in the single host. For some potential clients, this may preclude their consideration for a centralized proxy server because of the higher risk of sensitive data being disclosed. Also, a centralized host represents a simple, linear relationship between the overall cost of providing a service, the performance of the system, and the total number of users. Therefore, increasing the performance of the system is simply a matter of increasing the amount of bandwidth and servers allocated to the system. However, this arrangement is much more costly to the individual project host as it bears the entire cost of the system. So, as the number of users goes up, so too does the amount of capital needed.

Peer hosting systems, on the other hand, spread the trust a user must place in a circumvention tool to the volunteer servers. This could be a significant advantage compared to centralized systems for users wanting to ensure their data is kept confidential. Additionally, scaling a peer hosted system is less resource intensive as long as the number of volunteer hosts scales along with the total number of clients. One potential down-side to a peer hosting system is the freeloader issue. A freeloader is a client who only uses the tool but never volunteers to act as a host for the greater good of the community of users. A final potential issue with peer hosting systems is that most volunteer servers offer low, consumer level bandwidth. This means that the overall performance of a peer hosted system can be slow, even under light data loads.[92] All of these circumvention tools are designed to allow individuals to use the Internet in a manner that allows them to remain anonymous. There is, however, a cost to anonymity.

When an Internet user wishes to remain anonymous, he or she can use Internet proxies, encrypt data requests, and re-route requests over multiple servers. All of these

[92] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 18.

techniques assist in keeping the ultimate origin and destination of a data request confidential. However, each of these tools incurs costs to the Internet user's performance and usability. In addition, to truly hide a user's IP address from the destination Web server, a tool used for remaining anonymous must also filter out Javascript, Java, Activex, and any other active content on the websites they are accessing. This is a requirement because a server with malicious intent can use these active content products to determine the real IP address of the user trying to connect.[93] In a country trying to block access to circumvention tools, this information could identify an Internet user attempting to utilize a circumvention tool.

Cookies can also be deadly kryptonite to Internet users wanting to remain anonymous because a complicit website can identify a person trying to access two different websites at the same time. Thus, a filtering regime could collect personal information from a user using an "approved" website, and then correlate that same personal information with the user's visit to a fake website that would typically be accessed by a revolutionary (such as a website devoted to exposing regime corruption, for example). This situation represents a tradeoff that each circumvention tool developer must address.

Although filtering out active content (JavaScript and others) and cookies is easily done and relatively cheap, it is very degrading in terms of maintaining a website's functionality. Thus, it is important to consider the balance between filtering out the type of content that can take away a user's anonymity at the cost of a website's usability and functionality, and providing access to a fully functioning website, which may cost anonymity.[94] Finding the right balance depends to a large degree on the type of user the circumvention tool is designed for, and on how aggressive and repressive the filtering country is where the user is located. For example, a person who is a well-known blogger

[93] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 18.

[94] Ibid, 19.

in a country with few such bloggers is much more visible, and therefore becomes a much bigger target of the government as compared to a blogger who is one of hundreds or thousands in a particular country.

Whereas filtering and surveillance methods become prohibitively expensive in terms of trying to affect a large number of targets, when used against singletons, filtering and surveillance can be effective. Thus, a lone blogger might prefer anonymity over functionality, whereas a single blogger in an environment with a lot of other bloggers might prefer full functionality over increased anonymity. Again, individual circumstances will dictate the circumvention tools that are right for a given person and situation. To summarize, basic circumvention tools simply require that user requested data is encrypted, and that the request is redirected through an intermediate server which is located in a country that is not filtering the requested website. The difficulty lies in finding tools that provide anonymity and circumvention, while maintaining usability, security, the ability to avoid being blocked, and speed.[95]

In concluding this section, it is important to remember that when operating in the cyber domain, especially on social media, it is critical for SOF operators to understand this virtual environment. This includes knowing how the regime in question censors, monitors, and conducts surveillance. It also includes knowing which circumvention tools will allow secure and anonymous communication.[96] At the individual level, there are dozens of ways that a person can use Internet-based social media platforms as well as mobile phone-based social media platforms in a secure manner.[97] Finally, caution is the key watchword when using social media in a UW environment. Users must always be aware of the possibilities that modern communications technology represents. As an example, some members of the U.S. Congress are concerned that Chinese cell phone

---

[95] Roberts, Zuckerman, and Palfrey, "2007 Circumvention Landscape Report," 85.

[96] A thorough guide to bypassing Internet censorship and a detailed description of dozens of circumvention tools can be found in PDF form at the web site http://howtobypassinternetcensorship.org/.

[97] A by device-type list of security and anonymity TTPs can be found at http://irevolution.net/2009/06/15/digital-security/#comments. This guide is highly recommended for anyone needing to use the Internet or mobile communication devices. The reader comments section of this article also provides a wealth of information on the topic.

maker Huawei, which sells cell phones to populations in developing countries, may be installing software on its phones that would enable the Chinese government to spy on the Huawei phone users, as well as conduct other nefarious activities.[98]

I. FUTURE TRENDS

A key aspect of the social media environment is being able to connect to it. As previously discussed, connectivity represents the key terrain of the social media environment. An emerging technology that will potentially revolutionize this key terrain is a Wi-Fi antenna in a spray can! It is possible to imagine rebel insurgents appearing to be spray painting or "tagging" a prominent public wall, bridge, or building. Instead of paint, however, the insurgents will be spraying a liquid filled with millions of nano-capacitors that can receive radio signals. Furthermore, when paired with a basic router, Chamtech Enterprises' (the company that is developing the Wi-Fi spray) spray antennas can communicate with a fiber network, receive signals from satellites, and be added to other networks. This means that an insurgent group could cheaply and easily create its own network of broadband Wi-Fi hot spots.[99] This development could fundamentally alter the way the world thinks about Internet connectivity. Another emerging platform that could be especially effective in a UW environment is a social media tool called Vibe.

Vibe is a social media platform that allows messages to be sent anonymously from a mobile phone to other mobile devices within a select physical radius. Also, the messages automatically will expire after a certain amount of time, which is a powerful feature for those wanting to communicate securely. This is different from social media platforms like Twitter and others that automatically store user generated content.[100] Also, unlike most social media platforms, Vibe does not require users to create an

---

[98] Michael Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment," *The New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all&_r=0 (accessed May 2, 2013).

[99] Rachel Swaby, "7 Massive Ideas that Can Change the World," *Wired Magazine*, January 17, 2013, http://www.wired.com/business/2013/01/ff-seven-big-ideas/all/ (accessed February 10, 2013).

[100] Ravi Gupta and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis, IN: John Wiley & Sons, Inc., 2013), 382.

account or even log in to its website. Although this tool was not originally designed for political protests, it was used by the demonstrators of the Occupy Wall Street movement as a quick and effective means of sharing important information in the local area.[101] Finally, the concept known as augmented reality will fundamentally alter the social media environment.

Augmented reality refers to the intersection of the virtual world and physical world.[102] An example that already exists lies in the robust internal computers found in a growing number of new cars. These built-in systems allow motor vehicle operators to access social media through voice commands. This includes having words converted into text messages and then sent out through a mobile phone that is linked via Bluetooth to the vehicle's computer system. This increased convenience will come with a trade-off in terms of privacy and potential government monitoring and surveillance. The security implications of Google Glasses should be considered as well.

Google Glasses enable wearers to access and interact with social networks and the Internet in general through a small screen that is positioned in front of the user's eye. Based on where the person is located, Google Glasses can automatically push information to the user.[103] This type of technology could potentially be used by governments in combination with facial recognition software, social media databases, and criminal databases to rapidly identify known dissidents simply by scanning a crowd.

J. CONCLUSION

At the time this thesis is written, it is important to realize the social media landscape described throughout this chapter is not the same environment that will exist a year from now. The social media environment is constantly growing, evolving, and changing. One day, social media users prefer Myspace; the next month, this platform is obsolete. Smart phone users who once relied on text messaging for rapid communication

---

[101] Lindsay McComb, "Social (Media) Revolution: There's An App for That," The Metaq.com, http://themetaq.com/articles/social-media-revolution-theres-an-app-for-that (accessed February 20, 2013).

[102] Gupta and Brooks, *Using Social Media*, 34.

[103] Ibid., 34.

with peers now prefer Twitter. Those interested in understanding the social media environment must stay up to date on the latest technologies, and constantly challenge their own ways of thinking about and conceptualizing this growingly important domain. Social media has and will continue to help shape the outcome of future conflicts. Understanding the tools and technologies that facilitate social media conflict is critically important to successfully operating in this emerging terrain.

III. USING SOCIAL MEDIA IN CONFLICT

Army Special Operations Forces (ARSOF) are charged with supporting the defense of the United States by executing nine core activities. These core activities include: unconventional warfare (UW), foreign internal defense (FID), special reconnaissance (SR), counterterrorism (CT), security force assistance (SFA), counterinsurgency (COIN), direct action (DA), military support operations (MISO), and civil affairs operations (CAO). In addition to these nine core activities, ARSOF units have two additional secondary core activities: counterproliferation (CP) of weapons of mass destruction (WMD) and information operations (IO).[104] With this type of diverse mission set, some would informally liken ARSOF to a Swiss Army knife, meaning ARSOF units are one tool that can perform many functions. In a similar manner, social media technology has been used in a multitude of ways to support various operations during periods of conflict across the globe. However, little systemic research exists on how to operationalize social media for various missions in a specific type of warfare. This chapter aims to fill this gap in the literature.

To that end, it will provide an overview of how certain social media platforms and technologies have been used to assist in the execution of various types of operations, in different types of warfare. More specifically, the focus of this chapter will center on the use of social media to support unconventional warfare (UW)/insurgency warfare, counterterrorism (CT), and counter-insurgency (COIN) to achieve a range of desired end-states ranging from disruption at the lower end of conflict to overthrowing/defeating a ruling regime or a major insurgent group at the upper end, depending on perspective. One important caveat is that the examples provided in the UW/Insurgency column are not case studies of UW. The examples are mostly of homespun insurrections. However, these

[104] Department of the Army, *Field Manual 3-18, Special Forces Operations* (Washington DC: Department of the Army, 2012), 2-3.

examples involve the same complexities a UW practitioner would encounter in a denied area and the aims of UW are the same as a revolutionary.[105] Therefore, those planning a UW operation will find value in the examples provided.

Table 3 provides an organizing framework for this chapter and summarizes the examples that will be discussed. In addition to providing examples for each of these nine combinations of a type of war and paired goal, additional cases will be provided which demonstrate how social media can also support other ARSOF core activities including CP of WMD, SFA, and IO. Of the examples used throughout the chapter, the Egyptian Revolution of 2011 (UW/Insurgency—Overthrow/Defeat) is singled out as the principle case study of this chapter.

[105] Brian Petit, "Social Media and Unconventional Warfare, *Special Warfare Magazine* 25, no. 2 (2012): 33–34.

		Type of Conflict		
		UW / Insurgency	**Counter-Terrorism**	**COIN**
Operational Goal	**Disrupt**	Anonymous DDOS and other forms of attack against Tunisian government in support of Tunisian Protestors	FBI's use of Facebook to stop Antonio Martinez from detonating a car bomb against a military recruiting station FBI use of Facebook to arresting Quazi Nafis who tried to blow up the NY Federal Reserve	Tunisian government taking control of individual activists' social media accounts
	Coerce/Deter	SMS used to organize protests to coerce the Philippines federal court to impeach President Estrada April 6th Youth Movement protests to change Egyptian labor laws	Center for Strategic Counterterrorism's Digital Outreach Team's work on social media to deter would-be terrorists from joining terrorist organizations	CIA's Open Source Center's monitoring and potentially actioning intelligence gleamed from social media
	Overthrow/Defeat	Egyptian Revolution of January 25, 2011	ODA 5122's use of social media to cause a violent extremist group to self-implode in Mosul, Iraq	Iranian government defeating the Green Movement insurgents who protested the 2009 presidential election results

Table 3. Social Media's Utilization in Conflict

Before beginning the examination of specific uses of social media technology in conflict, the thesis will examine the origins of social media's use during periods of

struggle. Starting in late 2010 and continuing into the present, a wave of popular uprisings have spread across North Africa and the Middle East, resulting in regime changes in Tunisia, Egypt, Libya, and Yemen. These social revolutions, commonly referred to as the Arab Spring, fundamentally altered the way in which people connected to each other during periods of warfare. As such, researchers have devoted countless hours of study, examination, and analysis of the results and continuing struggles related to the Arab Spring.[106]

One factor that has played some part in each of the countries affected by the Arab Spring has been the citizenry's use of social media. A simple search engine query will return countless articles recalling how social media impacted the collective actions of thousands of protestors. In fact, most of the research seems to have been devoted to describing how social media empowers the average citizen with the ability to reach a vast audience in a very rapid manner. Additionally, it is important to note that social media has been used in conflict elsewhere. Examples can also be found in places like Iran, China, the Philippines, and Myanmar, and dates back to at least 2002, although the Arab Spring marks the beginning of the extensive use of social media as a tool of warfare.

But just as social media can be used by groups of people to communicate, organize, and "get the story out," so, too, can social media be used by various government entities to achieve their own objectives. This paper, within the framework provided in Table 3, aims to provide an overview of how various governments use social media, as well as how insurgent groups utilize social media in support of their own objectives. In doing so, it will highlight the competitive nature of social media where it does not inherently favor those wishing to disrupt the status quo (insurgents, criminals, terrorists,) or those wishing to maintain the status quo, namely the ruling power in a given nation. Additionally, these examples will provide the ARSOF planner with potential ways in which social media can be used to achieve future Department of Defense (DoD) objectives. From catching petty criminals to tracking nuclear warheads,

[106] For a thorough bibliography of the Arab Spring Uprising, see the Project on Middle East Political Science website at http://pomeps.org/category/academic-works/arabuprisings/.

from the United States to Syria, governments and insurgents are only beginning to exploit the potential of using social media to help realize desired end states in times of conflict.

A. UW / INSURGENCY—GOAL: DISRUPT

To be clear, the uprisings that ultimately ended up toppling several regimes in the Middle East and North Africa should not be viewed as case studies in UW.[107] These rather accidental revolutionaries were not reliant on an outside sponsor for the majority of their successes. Thus, they do not meet the doctrinal definition of an UW campaign. However, it is easy to conceptualize the Arab Spring uprisings as conflicts which could have been aided by direct assistance from ARSOF personnel. In this next example, though, it was not ARSOF operators who intervened to free an oppressed people.

The likelihood of anyone outside immediate friends and family ever knowing the name Sidi Bouzid was highly unlikely. However, when on December 17, 2010, Bouzid immolated himself in protest against police brutality and corruption in Tunisia, this single act sparked a wave of protest around Tunisia.[108] Within two weeks protests broke out all over the country. A large number of those protestors utilized the Internet via social media platforms to inform, organize, and build support for their cause. The Ben Ali regime responded by blocking access to social media sites such as Facebook, censoring Wikileaks cables that were damaging to the regime, and even shooting and arresting protestors.

In an unexpected turn of events, members of the "hacktivist" group Anonymous conducted distributed denial of service (DDOS) attacks and defaced Tunisian government websites, helped spread media reports, provided proxy websites to allow Tunisians to remain connected, and helped Tunisian protestors remain undetected by the Tunisian government.[109] Such DDOS attacks involve sending large amounts of useless data, in a

---

[107] Petit, "Social Media," 32–38.

[108] Quinn Norton, "Anonymous 101 Part Deux: Morals Triumph over Lulz," *Wired Magazine*, December 30, 2011, http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux (accessed January 25, 2013).

[109] Ibid.

short of amount of time, to a targeted website in order to prevent legitimate users from accessing the website. This action, along with the others mentioned above, was effective in disrupting the Tunisian government's ability to act in an unencumbered manner.

B. COUNTERTERRORISM—GOAL: DISRUPT

Retired 28-year CIA employee Arthur Hulnick stated that the most deadly and committed terrorists always act in a secretive manner. Nevertheless, law enforcement and intelligence agencies such as the FBI and CIA have acquired useful information on social media sites like Facebook that allowed them to disrupt would-be terrorists. One such example is the arrest of Antonio Martinez in late 2010.

Martinez, a Baltimore area resident, posted his desire to commit an act of terrorism in the United States. More specifically, he wrote about his plot to blow up a military recruiting station.[110] Eventually, Martinez's use of terrorist related language on Facebook got the attention of federal authorities, and several FBI agents eventually joined Martinez's online plot. After gaining his confidence, undercover agents supplied Martinez with a fake car bomb. A few days later, Martinez tried to detonate the car bomb in the parking lot of a military recruiting station, which obviously failed to cause any damage, and his terrorist plot was effectively disrupted. A second example involving the FBI centers on a Bangladeshi citizen in the United States.

According to a court document, an undercover FBI agent used the social media platform Facebook to communicate with Quazi Mohammad Nafis about his intentions to detonate a car bomb near the Federal Reserve building in New York. Quazi, who was in the United States on a student visa, had alleged links to the terror group Al-Qaeda.[111] Additional reports from the FBI indicate that Quazi originally came to the United States in January of 2012 with the intention to conduct violent jihad. He attempted to recruit

---

[110] Maria Glod, "Va. Man Allegedly Used Facebook to Threaten D.C. Area Bombings," *The Washington Post*, December 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/14/AR2010121406829.html (accessed December 20, 2012).

[111] Shara Tibken, "FBI Uses Facebook to Nab NY Terrorist Suspect," CNET.com, http://news.cnet.com/8301-1023_3-57535887-93/fbi-uses-facebook-to-nab-ny-terrorist-suspect/ (accessed December 21, 2012).

individuals for his own terrorist cell inside of the United States. One of Mr. Nafis's potential recruits was actually the FBI agent posing as an Al-Qaeda facilitor. The agent later learned that possible targets included a high-ranking official from the U.S. and the New York Stock Exchange.[112]

After communicating several times with the undercover FBI agent, Quazi asked the agent to supply him with 20 50-pound bags of explosives. After receiving the fake explosives, Mr. Nafis assembled the explosives for the attack, purchased a detonator, and conducted several reconnoiters of the financial district in lower Manhattan.[113] On the day of the planned attack, Quazi met with the FBI agent and drove a van filled with 1,000 pounds of inert explosives to the Federal Reserve building and parked it. The two men got out of the van and walked to a nearby hotel where Quazi made a video statement. After completing his statement, Mr. Nafis tried several times to detonate the explosives. Immediately following the failed attempts, the Joint Terrorism Task Force arrested Quazi. On February 7, 2013, Quazi Nafis plead guilty to attempting to use a weapon of mass destruction and now faces a sentence of up to life in prison. He was set to receive sentencing on May 30, 2013.

C. COUNTERINSURGENCY—GOAL: DISRUPT

A growing buildup of civil discontent over rising food prices, corruption within the government, and unemployment, among other factors, came to an explosive head on the streets of Tunisian in December, 2010 after the aforementioned Mohamed Bouazizi's self-immolation. Bouazizi was an underemployed college graduate, forced to sell fruit and vegetables from a cart because there were no other jobs available.[114] After police

---

[112] U.S. Attorney's Office, "New York Man Pleads Guilty to Attempting to Bomb New York Federal Reserve Bank in Lower Manhattan," The FBI New York Field Office, http://www.fbi.gov/newyork/press-releases/2013/new-york-man-pleads-guilty-to-attempting-to-bomb-new-york-federal-reserve-bank-in-lower-manhattan (accessed March 12, 2013).

[113] Ibid.

[114] Richard Spencer, "Tunisia Riots: Reform or be Overthrown, US Tells Arab States Amid Fresh Riots," *The Telegraph*, January 13, 2011, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/tunisia/8258077/Tunisia-riots-Reform-or-be-overthrown-US-tells-Arab-states-amid-fresh-riots.html#mm_hash (accessed January 21, 2013).

discovered that Mohamed did not have a vendor's license, they confiscated his cart, rendering him completely jobless. In protest, Mr. Bouazizi stood in the middle of the street in front of the governor's office and lit himself on fire. This single act set off a renewed wave of protests, particularly through social media platforms such as Facebook and Twitter.

As the voices of discontent grew louder and angrier towards the Ben Ali regime, the government began to target the most vocal online activists in an effort to disrupt this emerging insurgency. The Tunisian government began to block the social media accounts of individuals such as Sofiene Chourabi, at the time a journalist for *Al-Tariq al-Jadid* magazine.[115] Sofiene and other online activists began to have their individual Gmail and Facebook accounts hacked and taken over. This type of action provides an example of a COIN operation with the goal of disrupting a potential movement against the government.[116] China provides another example of an ongoing COIN effort to disrupt Chinese dissidents from even starting to mobilize against the government.

China has one of the most sophisticated systems of Internet and social media censorship in the world. While many assume that China censors criticisms of the government, certain policies, or even specific leaders, the 20 to 50 thousand members of China's so-called Internet police are primarily concerned about efforts to act collectively.[117] Anytime Chinese citizens try to gather together for any reason, to criticize the government, support the government, or even celebrate a holiday, Chinese officials will try to censor it. In total, an amazing 13 percent of all posts in China are censored.[118] Looking into the future, some states like Russia are looking to expand their offensive social media capabilities in order to increase their effectiveness in disrupting any insurgent groups.

---

[115] Ryan, "Tunisia's Bitter Cyber War."

[116] Ibid.

[117] Gary King, "China's 'Internet Police' Targets Collective Action," National Public Radio, August 8, 2012, http://www.npr.org/2012/08/08/158448847/chinas-internet-police-targets-collective-action (accessed September 6, 2012).

[118] Ibid.

Recently, the Russian government purchased three new social media targeting software packages valued at $1 million each.[119] The first system is called *Dispute*. It is "responsible for overall monitoring of the blogosphere and social networks in order to single out the centers where the information is created and the ways by which it is spread among the virtual society."[120] The second system is called, rather interestingly, *System Three*. It is designed to develop methods of organizing and managing a "virtual community of experts." Despite its officially stated purpose, some believe the Russian government, like the Chinese government, is trying to anticipate any efforts to undermine the government's authority. This idea was furthered by the Russian government's recent decision to selectively block content on social media sites that it deems illegal or harmful to children. Although the majority of censorship requests made by the Russian government to date appear to be legitimate concerns (about Facebook pages that promote suicide, for example), opposition political leaders fear the law will begin to be abused and lead to more broad social media and Internet censorship.[121]

D. UW/INSURGENCY—GOAL: COERCE/DETER

One of the earliest uses of social media technology in working towards political change occurred in the Philippines in 2001. In what became known as the People Power II movement, the Filipinos used social media technology to coerce their country's Supreme Court to reinstate damaging evidence in the impeachment trial of then President Joseph Estrada. But with less than one percent Internet penetration at that time, it is interesting to see how the people use social media to ensure that the documents were seen

[119] Bristol Voss, "Governments Shop for Latest Internet Weapons," Minyanville, August 28, 2012, http://www.minyanville.com/business-news/politics-and-regulation/articles/internet-weapons-cyberspace-social-media/8/28/2012/id/43548?page=full (accessed September 6, 2012).

[120] Ibid.

[121] Andrew Kramer, "Russians Selectively Blocking Internet," *The New York Times*, March 31, 2013, http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-internet-content.html?_r=0 (accessed April 12, 2013).

by the jury and entered into the record. People used mobile phones to send and receive SMS messages to and from their existing social networks to coordinate mass protests.[122]

Although, in hindsight, this million-person protest was viewed in a somewhat negative light by foreign audiences, it still provides a good example of the use of social media technology by insurgents to coerce a government to capitulate to the will of the people. By simply forwarding simple SMS messages such as "Go 2 EDSA (an acronym for a street in Manila). Wear Black," "Wear black to mourn the death of democracy," and "Military needs to see one million at a rally tomorrow, Jan. 19, to make a decision to go against Erap! Please pass on," the people were able to coordinate the date, time, what to wear, and a basic narrative for the protests. After five days of protesting, the chief of the military informed President Estrada that the military was withdrawing their support of his presidency, and the Supreme Court ruled in favor of removing the President from office because the "welfare of the people is the supreme law.''[123] A second example can be found in Egypt.

A rather small group of young Egyptian activists, who eventually took on the moniker the April 6 Youth Movement, started to rebel against the Mubarak regime by demanding labor reform. The group, which officially started on March 23, 2008, protested against rising food prices as well. Instead of taking a traditional route of either protesting on the streets, or going to see a local politician, the leadership of the April 6 Movement launched a Facebook page to show their support of laborers in the city of Mahalla. This Facebook page, initiated by group leader Ahmed Maher, started with about 300 individuals initially joining the page. However, within the first day of its being launched, the page had over 3,000 members, and after only a couple of weeks, the social

[122] Brannon Cullum, "People Power II in the Philippines," Movements.org, June 25, 2010, http://www.movements.org/case-study/entry/people-power-ii-in-the-philippines/ (accessed November 10, 2012).

[123] Seth Mydans, "People Power II' Doesn't Give Filipinos the Same Glow." *The New York Times*, February 5th, 2005, http://www.nytimes.com/2001/02/05/world/people-power-ii-doesn-t-give-filipinos-the-same-glow.html (accessed November 15, 2012).

media based network had grown to over 70,000.[124] As the number of members grew, so too did the goals of the network. The network's goals now included the call for free speech and an end to government nepotism.[125] Eventually, Mr. Maher, an engineer, realized that to be effective in coercing the government to change its economic and regulatory policies, the group had to physically take to the streets.

Using graphic images taken mostly by members of the Facebook group and heartfelt posts on the Facebook page's community wall, Maher was able to rally thousands of workers in the Mahalla area to take to the streets in protest of the Mubarak regime. The protests, which occurred on April 6 (the reason for the group's name), was not the first worker protest in the area. In fact, the laborers in Mahalla had been periodically striking for over a year. However, these past protests were never formally organized or coordinated.[126] The April 6 Youth Movement changed this by coordinating the mobilization of thousands of protestors on a single day. The protests included general labor strikes to disrupt the various industries throughout Mahalla. Additionally, the April 6 Facebook page was used to direct supporters to hand out informational leaflets and to spray paint various areas to allow non-Internet users know what was going on.

Ultimately, this insurgency was short-lived, but not without consequence. Egyptian security forces did not stand idly by and let the protests occur. Rather, police actions that day led to at least four protestor deaths and the arrests of over 400 citizens.[127] Despite the group failing to significantly change government policies on that day, the protests formed the genesis of a much larger insurgency that would ultimately succeed in its objectives.

---

[124] PBS Frontline,"April 6th Youth Movement," PBS, February 22, 2011, http://www.pbs.org/wgbh/pages/frontline/revolution-in-cairo/inside-april6-movement/ (accessed on December 9, 2012).

[125] Samantha Shapiro, "Revolution, Facebook Style," *The New York Times*, January 25, 2009, http://www.nytimes.com/2009/01/25/magazine/25bloggers-t.html?_r=0&pagewanted=print (accessed January 18, 2013).

[126] Ibid.

[127] PBS, "April 6th Youth Movement."

Other examples that fit into this category of citizens using social media (SMS in particular) to coerce governments into taking specific actions include South Korean students organizing protests against the highly competitive college entrance exams, Chinese citizens protesting against the potential of Japan joining the United Nations Security Council, and Lebanese citizens rallying in Beirut to force Syrian troops out of Lebanon permanently. Although there was a great deal of pressure from the United Nations for this same end state, the one million Lebanese protestors helped apply even more pressure to the Assad regime, which eventually agreed to withdrawal all 14,000 Syrian troops from Lebanon.

E. COUNTERTERRORISM—GOAL: COERCE/DETER

The U.S. government established the Center for Strategic Counterterrorism Communications (CSCC) in September, 2011 to "coordinate, orient, and inform Government-wide public communications activities directed at audiences abroad and targeted against violent extremists and terrorist organizations, especially Al-Qaida and its affiliates and adherents…to reduce radicalization by terrorists and extremist violence and terrorism that threaten the interests and the national security of the United States."[128] To that end, the CSCC established the Digital Outreach Team (DOT) to aggressively monitor and counter terrorist propaganda and recruiting efforts, primarily on social media websites on the Internet.

Publishing content in multiple languages including Arabic, Urdu, Somali, and Punjabi, the CSCC has posted over 7,000 separate messages in online forums, established 53,000 Facebook fans, and produced over 50 videos that have been posted to social media sites like Youtube. The videos in Arabic have alone received over two million views. This digital content is fully attributed to the U.S. Department of State, and is designed with three immediate goals.

[128] Alberto Fernandez, "The Center for Strategic Counterterrorism Communications" (speech, Naval Postgraduate School, Monterey, CA, April 14, 2013).

The CSCC's first goal is to contest the digital space used by Al-Qaeda. Effectively, this means that the CSCC is trying to change the dynamics of the social media "circles" that interact within the model described in Chapter II. Formerly, the extremist social media space, most notably forum websites like Ana al-Muslim and Ansar al Mujahideen, were uncontested.[129] The second goal is to redirect the conversation. This means the CSCC is trying to challenge the narrative advanced by various terrorist groups. To achieve this goal, the CSCC does not try to affirm the positive actions of the U.S. government's foreign policy. Rather, the CSCC highlights the negative about the groups they are targeting. This is an offensive versus defensive posture. The third goal is to unnerve the adversary. This is simple Psychology 101: get inside the head of one's opponent. An example of the type of work that the CSCC is doing involved a suicide bomb attack in Salamiyah, Syria.

In January 2013, the DOT saw an online post by the Al-Qaeda affiliated group Nusrah Front that claimed responsibility for the attack against a rug factory that killed dozens of innocent civilians, including children. After the attack was criticized by local Syrians, the Nusrah Front claim was retracted.[130] The DOT was able to find local footage of the attack from credible sources, which included images of some of the children that were killed, and post a video on Youtube which highlighted this terrorist group's actions and the after- effects of the bombing. The DOT later found forum postings by Nusrah Front members complaining about the anti-Nusrah Front video, and the group created its own video that tried to counter the DOT's work. This vignette provides a good example of a government organization deterring a terrorist group from executing future attacks that target civilians. The DOT's efforts also disrupted the group's operational cycle by causing it to spend manpower, resources, and time to produce their counter-product.

In addition, the CSCC believes it has deterred significant numbers of would-be jihadists from joining violent extremist organizations. Although it is not possible to know exactly how many (how can it be proved that someone was deterred from joining based

[129] Fernandez, "The Center for Strategic Counterterrorism Communications."

[130] Ibid.

on products posted by the DOT?), based on the counter-messaging and sheer number of comments made in reference to DOT's products, it is not difficult to think that some individuals have been persuaded against joining a terrorist organization. It should be noted that this example of deterrence does not fit the classical definition of deterrence in that there was no denial or punishment associated with the DOT's actions. In fact, some security experts point to this exact issue as a problem and they think that this strategy is inadequate in the fight against terrorism.

A recent article by John Arquilla states that simply presenting a moderate portrayal of Islam in combination with highlighting heinous acts of terrorism on the Internet is not sufficient. Dr. Arquilla argues that what is needed is to develop an effective way to "back hack" and geo-locate those that post violent jihadi materials as well as those that retrieve the information. The argument is that only by tracking down and capturing or killing terrorists will groups like Al-Qaeda truly be beaten.[131]

F. COUNTERINSURGENCY—GOAL: COERCE/DETER

The CIA's Open Source Center has full time staff that include translators, researchers, and analysts. As of late 2011, these teams were monitoring over five million updates, tweets, and the like, every single day.[132] The staff, which pales in comparison to some other nations in terms of pure numbers of staffers, includes many who hold masters of library science degrees. The Open Source Center searches for obvious subjects and key words related to terrorism and political unrest but also tries to understand a given country's narrative. In addition, the CIA tries to determine what is trending or popular at any given moment. This means that if the CIA determines that something like a satellite

[131] John Arquilla, "How to Defeat Cyber Jihad," *Foreign Policy*, April 29, 2013, http://www.foreignpolicy.com/articles/2013/04/29/how_to_defeat_cyber_jihad (May 5, 2013).

[132] Robert Siegal, "How Does the CIA Use Social Media," National Public Radio, November 7, 2011, http://www.npr.org/2011/11/07/142111403/how-does-the-cia-use-social-media (accessed September 1, 2012).

television show is the most talked about subject on social media sites, and not something like government corruption or injustice, then it is a sign that the general political situation is stable at that time.[133]

Although the CIA has increased its ability to develop important intelligence from social media, it still has difficulty in determining where an individual who is making the posts is located. One of the most difficult obstacles for the CIA to overcome is people's use of shadow Internet IP addresses, which help individuals remain hidden. For example, a person could be sending tweets in Arabic under an email address registered in Yemen, but could actually be a citizen of the United States living in South America. One way the CIA has worked to overcome this obstacle is to try to find those who are sympathetic to terrorist organizations and individuals, and then try to monitor their postings for clues on identifying and locating the true terrorists.[134]

The Open Source Center also has problems associated with countries of interest in which there is minimal access to the Internet for average citizens. In these countries, individuals must rely on cellular phones and SMS services. In these instances, groups like the Taliban and Al-Qaeda can use a closed loop of network subscribers to limit who receives their text messages. This forces the CIA to have to devote disproportionate resources, including covert eavesdropping resources, to penetrate these networks.[135] As in the previous example highlighting the CSCC's efforts, for the CIA's Open Source Center to effectively deter would-be insurgents, the CIA must act on the social media gleaned intelligence and strike at those networks through direct action. In examining open source research materials, it is not apparent whether or not the CIA has acted on social media-based intelligence gathered by the Open Source Center.

---

[133] Rachel Martin, "CIA Tracks Public Information for the Private Eye," National Public Radio, January 22, 2012, http://www.npr.org/2012/01/22/145587161/cia-tracks-public-information-for-the-private-eye (accessed September 1, 2012).

[134] Ibid.

[135] Siegal, "CIA Use Social Media."

G. UW/INSURGENCY—GOAL: OVERTHROW/DEFEAT

During the Egyptian Revolution, which occurred during the Arab Spring, it was common to read headlines that described the regime change in Egypt as a Facebook or social media-caused revolution. This would imply that the network that ultimately ended the regime was rapidly and spontaneously formed. These types of portrayals are categorically false and misleading. And, although this section of the chapter focuses on Wael Ghonim's revolutionary network, which did form in a relatively short amount of time, it was ultimately a network of networks that came together to overthrow Hosni Mubarak's regime, not some mystical Facebook page or Twitter user.

When the Arab Spring first broke out in Tunisia, Wael Ghonim was the head of marketing at Google for the Middle East and North Africa. Although living outside of Egypt, Wael continually monitored what was going on inside of Egypt. One particular story that effected Wael in a profound way was the story of Khaled Said. Khaled was the recipient of a severe beating by Egyptian police that eventually resulted in Khaled's death. Rather than stand idly by while this police brutality continued, Wael decided to protest this specific action.

Originally, Wael did not have a grand network in mind to bring about political changes in Egypt. Rather, he started a Facebook page tilted "Kullena Khaled Said," or "We are all Khaled Said." In his first Facebook post on this newly created page, Wael wrote, "Today they killed Khaled. If I don't act for his sake, tomorrow they will kill me."[136] Within a few hours, Wael had dozens of people *Like* his post and add comments. Thus, a social-media- based- revolutionary-network was born. Its original purpose was two-fold; hold the security force officers who killed Khaled Said responsible for their crime and end the continual police brutality that was so common in Egypt. Six months later, the network's purpose had matured.

By January 2011, Wael's network had developed a purpose that was multifaceted. The objectives included ending the large economic gap that existed between the political

[136] Ghonim, *Revolution 2.0*, 60.

elite and the common Egyptian, annulling the emergency law, firing the Minister of Interior, and limiting the Presidency to two terms.[137] The articulation of these network goals corresponded to one of the network's first major activities, the January 25 day of protest in Egypt. From there, the network's purpose became even more ambitious, though simplified. The only purpose after January 25 was overthrowing the regime of President Hosni Mubarak.

The network that finally overthrew the Mubarak government consisted of multiple networks formed during different times, out of all the frustration with the ruling party in Egypt. The first major component of this overall network was the Muslim Brotherhood, formed in 1928 and organized around political change. The second component was the Kefaya or "Enough" network. Kefaya was formed in 2004 and consisted of several hundred Egyptian intellectuals. Their common purpose was to reform the executive branch.[138] A third network whose original purpose was political change was the aforementioned April 6 Youth Movement. Eventually, individual members of these networks formed relationships with each other and with outside entities.

These outside entities included the Youth Movement of Tunisia, Otpor in Serbia, the Academy of Change, and the Youth Movement of the Muslim Brotherhood. Additionally, the overall revolutionary network grew to include opposition party leader Mohamed El Baradei's Constitution Party. Wael Ghonim's Facebook-initiated network formed relationships with members of several of these other sub-networks. Together, the networks developed reciprocal relationships that allowed this network of networks to achieve a common purpose in forcing President Mubarak to resign. This overall network's structure is captured in Figure 5.

---

[137] Ghonim, *Revolution 2.0*, 166.

[138] Nadia Oweidat et al., "The Kefaya Movement," The RAND Corporation, December 3, 2012, http://www.rand.org/pubs/monographs/2008/RAND_MG778.pdf (accessed January 16, 2013).

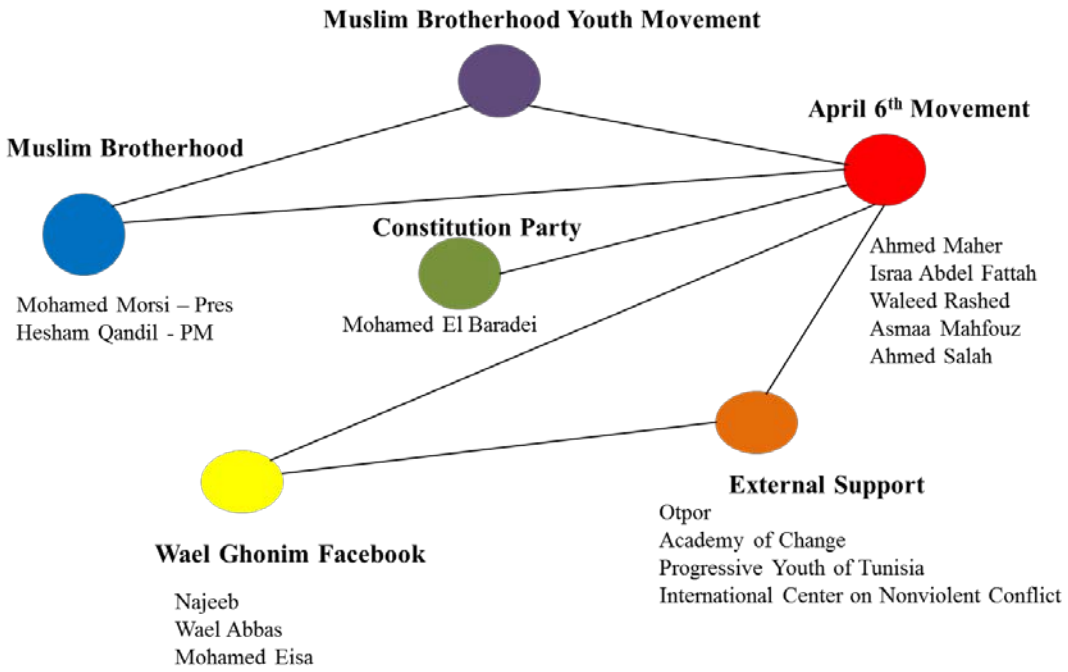

Figure 5. The Egyptian Revolutionary Network of Networks

Although Figure 5 is a simplification of the Egyptian revolutionary network, it does show that no single network or group of people was responsible for achieving the overall network's ultimate purpose. Additionally, the regime change did not occur overnight. The situation in Egypt had been deteriorating for decades. As the deterioration continued to grow, so too did the number of networks that were formed with political, social, and economic reforms in mind.

Turning attention back to Wael Ghonim's Facebook network, one of the most striking things about the network was that of the hundreds of thousands that eventually joined it, the vast majority did not know who Wael Ghonim was, nor did very many of the members know each other. Thus, this network was very large in terms of its total number of participants, but most of the ties were weak. One compensating factor for the large percentage of weak ties was that the network had a lot of social capital. In fact, one

of the things that made Wael's network successful was that it was able to establish both bonding social capital (social capital within a network), and bridging social capital (social capital that links to outside networks).[139]

Another compensating factor that held the participants together was that the network's mission-based purpose affected all of the members in deep and personal ways. Decades of despair, misery, and frustration can inspire a network of people to achieve goals once thought impossible. This shared purpose helped form the social capital between the participants of Wael's network. Additional factors about the way Wael ran his network help explain its ultimate success.

Wael set up the "We Are all Khaled Said" Facebook page to be administered anonymously. Wael did this for two reasons. First, he wanted the revolutionary movement to be about the Egyptian people themselves. He wanted to avoid centering the network's purpose on advancing any one leader's agenda. Second, the network's purposes, throughout the life of the network, were nefarious in the eyes of the Mubarak regime. Wael was afraid of being arrested, beaten, and possibly killed. However, Wael's network did experience most of the network governance stages of emerge, connect, identify, collaborate, organize, codify, and evolve.[140]

First, the network emerged via a Facebook page. The majority of the network's connections were made by discovery by other, like-minded Egyptians. What is somewhat unique about this particular network was that it was not based on an existing, offline social network. The network identified itself by having a Facebook page name, and also taking on the identity of the January 25 protestors. The network gained further legitimacy by using common logos such as the Egyptian flag and the picture of Khaled Said's battered face. As the network grew, so did the collaboration of the members within the network itself as well as with other networks. The network organized itself primarily

[139] Nancy Roberts, "Social Capital," Lecture given at the Naval Postgraduate School, Monterey, CA, September 26, 2012.

[140] Anklam, *Net Work*, 60.

using social media technology. But the network was also organized around functional areas such as writing, reporting, capturing video, taking pictures, and recruiting.

Although most people do not think of codified rules when looking at images of tens of thousands of protestors, Wael's network codified the rules when it implored its participants to follow in executing the network's most important activity of protesting in the streets of Egypt. Some of these rules included: protesting peacefully and without breaking any laws, being at the pre-determined protest locations on time, not carrying any unnecessary items such as licenses or credit cards, carrying only the Egyptian flag (shows solidarity), using the pre-written chants, not disturbing traffic, and not going to the protests alone. Finally, as was described in the exploration of the network's purpose, the network evolved from several hundred members calling for justice for Khaled Said, to several hundred thousand calling for the end of Hosni Mubarak's rule. A further interesting aspect of how Wael's network was governed was how he made important decisions.

Wael Ghonim was clearly a leading figure in the overall network of networks that caused President Mubarak to resign. He was also the leader of his Facebook-based revolutionary network. Despite his status in the network, Wael relied on participatory democracy for many of the decisions made on behalf of the network, especially those that involved activities on the ground.[141] Using web-based technology, Wael would poll his network participants before making major decisions in order to ensure the network was comfortable with the decisions being made.[142] This focused Wael on the most important issues of his network, a rather ingenious way to democratize network members' feedback. Finally, he demonstrated good network leadership skills by deferring decision making to others (such as April 6 Youth Movement leader Ahmed Maher) in areas with which he was not familiar. Wael also showed he was a good leader in the way that the network's tasks, activities, operations, and processes were managed.

---

[141] Ghonim, Revolution 2.0, 108.

[142] Ibid, 93.

First, and most obviously, the network relied on Facebook to store and distribute information to members. Social media platforms provide an extremely low cost, efficient, and effective way to communicate with a network. Next, Wael and the other network leaders used Google tools to help manage their information. The network developed a massive email list that was managed in a Gmail account. This provided redundancy should the Egyptian government block Facebook, which it eventually did. The network also used Google Moderator. This is a tool that gives a person the ability to ask questions of a limitless number of users, and then rank those questions based on popularity.[143] This innovative technology provided an easy way to democratize network members' feedback. Google Docs was also utilized in controlling and managing information.

The network's first major activity was a large-scale protest on January 25. In order to disseminate important details, rules, and coordinating instructions to his network, Wael compiled all pertinent information into a single document and uploaded it to the Internet using Google Docs. Wael then gave over 50,000 network members access to the document, and asked members to help get the document to the masses by posting it, or links to it, to various online forums, politically based websites, other Facebook pages, and through Twitter.[144] Reaching out to this many people for assistance, also known as crowdsourcing, was another common part of the processes that Wael's network used in executing its tasks and operations.

Other examples of crowdsourcing tasks and operations included asking members to contact any known journalists to help spread the network's messages and asking network participants to send mass text messages (SMSs) to reach non-Facebook-using Egyptians. Additionally, Wael and other revolutionary leaders realized that the majority of Egyptians were not using the Internet. Therefore, another crowd-sourced critical task was to distribute printed fliers to both poor, urban areas and rural areas of Egypt. Also, network members were asked to contact at least five other people by phone or in person and encourage those people to join the protests on January 25.

---

[143] Ghonim, Revolution 2.0, 55.

[144] Ibid, 164.

Ultimately, after only 18 days of mass protests, the regime of Hosni Mubarak stepped down. The President officially resigned on February 11, 2011. The military leadership stepped in to fill the power void, and the people had achieved their goal, at least in the short term. Though it remains to be seen whether this revolution truly brings about the desired changes of the Egyptian people, it is clear that social media technology played a large role in helping organize and direct the protests of many Egyptians.

H. COUNTERTERRORISM—GOAL: OVERTHROW/DEFEAT

In late 2009, Operational Detachment—Alpha (ODA) 5122 began tracking a Jaysh Rijal al-Tariqa al-Naqshbandia (JRTN) affiliated terrorist group that was operating south of Mosul, Iraq. The 12-plus-man group was actively facilitating the movement of foreign fighters, money, weapons, and equipment. Intelligence reports indicated there were several individuals competing to be the leader and that distrust was beginning to seep into the group. Although the details and specific TTPs cannot be discussed in an unclassified thesis, the ODA used behavior modification messaging, delivered through social media technology, to capitalize on this internal competition and distrust.[145] The messages were of two basic types.

The first message type was a series of insults aimed at the individuals competing to be leader of the group. The second message type was a series of accusations against various group members. These messages accused certain individuals of working with the United States. To reinforce these messages, the ODA conducted a kinetic strike shortly after the accusatory, pro-U.S. messages went out. The combination of kinetic and non-kinetic, social media-based targeting caused the group to self-implode. This particular terrorist group, while relatively small, was effectively defeated largely through social media-delivered messaging. This vignette also demonstrates the multiplicative effects of non-lethal cyber targeting on the overall targeting of terrorist groups.

[145] Ben Williams, Presentation given at the Naval Postgraduate School, Monterey, CA, October 23, 2012.

I. COUNTERINSURGENCY—GOAL: OVERTHROW/DEFEAT

Unfortunately for people living under repressive regimes, social media is used for more than capturing criminals and terrorists. In Iran, for example, authorities use social media to repress their own citizens. The most well-known instance of this repression occurred in 2009 following Iran's presidential election. Protestors, upset by obvious election fraud, began calling for nationwide protests throughout the country. Alarmed and concerned, the Iranian government took steps to defeat the dissent.

The Iranian regime used several social media websites to gather photos of various protestors and circulated the photos in order to identify individuals in the photos. Iranian authorities also used sites, especially Facebook, to find out personal information and the whereabouts of protestors. Also, the regime sent messages to Iranian citizens living abroad, warning them not to support the so-called Green Movement unless they wanted to hurt their own relatives and friends in Iran. Further still, the Iranian government used social media sites to distribute pro-regime propagandistic videos and sent mass text messages to Iranian citizens warning them to stay away from protests in the streets.[146] Thus, Iran's government was effective at undermining the Green Movement.

More recently, the Iranian government has increased its blocking and censorship of certain websites, including many popular social media sites. In addition, Iran's cyber police have been cracking down on citizen's use of virtual private networks (VPNs). As Chapter II described, VPNs use secure protocol to encrypt users' data and identities and allows individuals to circumvent blocks on the Internet put in place by the government.[147] In addition to efforts inside its own borders, the Iranian government is also using social media to help its ally, the Assad regime in Syria.

Besides traditional military weapons and equipment, Tehran is providing Assad's security forces with technology designed to prevent Syrian protestors from being able to

---

[146] Morozov, *The Net Delusion*, 10–11.

[147] Marc Burleigh, "Iran to Crack Down on Web Censor-Beating Software," Google News, June 10, 2012, http://www.google.com/hostednews/afp/article/ALeqM5jIFi-LdqBsdtrj7mRYnCMTlSGjCA?docId=CNG.f710ad6e0ee1dc52f64c985918d1bac1.741 (accessed September 5, 2012).

communicate through social media platforms such as Facebook and Twitter.[148] Iranian officials also share techniques, hardware, and software to conduct Internet surveillance. This assistance is being combined with electronic surveillance systems, as well as drone aircraft. Together, these tools provide a significant advantage to the Assad regime in the on-going battle in Syria.[149] In a recent example of how Syria is trying to defeat the opposition, the official Reuter's Twitter account was hacked. The hackers, allegedly part of the Syrian Electronic Army, then sent out a series of false tweets that were designed to undermine and discredit the Free Syrian Army and reduce the amount of support the group was receiving from the local populace.[150] This example completes the three-by-three matrix template for this chapter. The remainder of the chapter provides some additional examples of how social media can support other ARSOF core activities.

J. SECURITY FORCE ASSISTANCE

Although some people in the United States, especially those living outside of major cities, may view spray-painted graffiti as a relatively harmless crime, Los Angeles County crews removed nearly 40 million square feet of graffiti in 2007. This massive clean-up effort cost taxpayers almost $30 million.[151] One tagger, or person using spray paint to illegally deface property, especially problematic in the greater Los Angeles area, was known by the moniker "Buket." Buket was believed to have been personally responsible for at least $150,000 in damages.

Having failed for months to determine the real identity of Buket using traditional means, Los Angeles county deputies began combing the Internet for clues as to who Buket was in order to finally arrest him or her. Officials state their big breakthrough came

---

[148] Mark Hosenball, "Iran Helping Assad to Put down Protests," *Reuters*, March 23, 2012, http://www.reuters.com/article/2012/03/23/us-iran-syria-crackdown-idUSBRE82M18220120323 (accessed September 6, 2012).

[149] Ibid.

[150] Jon Herring, "Disinformation Flies in Syria's Growing Cyber War," *Reuters*, August 7, 2012, http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807 (accessed September 6, 2012).

[151] Andrew Blankstein, "Tagger Used YouTube, and the Police Watched," *The Los Angeles Times*, May 28, 2008, http://articles.latimes.com/2008/may/28/local/me-buket28 (accessed September 2, 2012).

in the form of a YouTube video showing Buket spray painting 20 feet above the busy Hollywood Freeway during broad daylight. The video was set to music and posted to YouTube and other tagger-related blogs.[152] This video, and others like it, allowed authorities to learn that Buket's work was featured in a book titled *Los Angeles Graffiti*. After contacting the book's author, law enforcement officials were able to determine that Buket's real name was Cyrus Yazdani, a 24 year-old convention planner from Las Vegas. Yazdani was subsequently arrested. The U.S. attorney's office and the Secret Service are also using social media to pursue criminals.

Another example of how these two U.S. government agencies using social media involved a man named Maxi Sopo. Mr. Sopo was accused of bank fraud in Seattle, Washington. When Sopo learned that federal agents from the attorney general's office were looking into his activities, he fled to Mexico. After safely arriving in Mexico, Sopo started to update his Facebook status, saying things like "living in paradise" and "loving it."[153] He continued to add posts indicating how great his life had become and how much fun he was having with his friends. In one post, Sopo posted a picture that showed him in front of a BMW and a Courvoisier liquor backdrop.

A Secret Service agent was able to use the backdrop to narrow down Sopo's location to Cancun, Mexico. Digging further on Facebook, this same Secret Service agent was able to view. Sopo's friends' list because of the Facebook settings Sopo had chosen. In scrubbing this list of friends, it was determined that Sopo was Facebook friends with a person associated with the U.S. Justice Department. A call went out to this former Justice Department official who cooperated with authorities and was able to contact Sopo to get his exact location. Shortly thereafter, Sopo was arrested by Mexican authorities and sent

[152] Blankstein, "Tagger Used YouTube."

[153] Alexandra Topping, "Fugitive Caught after Updating His Status on Facebook," *The Guardian*, October 14, 2009, http://www.guardian.co.uk/technology/2009/oct/14/mexico-fugitive-facebook-arrest (accessed September 1, 2012).

back to the United States. Ultimately, Sopo received 33 months in prison, five years of supervised release, and $147,249 in restitution for four counts of bank fraud.[154]

K. COUNTER-PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

A final example of the CIA's use of social media is rather fascinating: finding nuclear weapons. Rose Gottemoeller, the acting U.S. Undersecretary of State for Arms Control, is behind a campaign to explore ways in which social media (as tools of communication) can help rid the world of nuclear weapons. In particular, Gottemoeller is interested in crowd sourcing problems such as locating nuclear warheads, determining the location of nuclear facilities, knowing the status of deployed weapons, and helping to learn if nations are upholding their nuclear arms agreements.[155] Gottemoeller said the basic concept is to empower ordinary citizens through various civilian monitoring projects, whereby the insight provided by citizens is combined with the usual methods of verifying a given country's nuclear intentions.[156]

The Institute for Science and International Security has been uploading satellite photos of Iranian nuclear sites for several years.[157] By examining photos of the same facility over a period of months or years, individuals can assist in monitoring the development of these potentially dangerous locations. The key to making this arrangement successful is the marrying up of verification technologies and the networking capabilities provided by Facebook, Twitter, and related Internet sites. Another important aspect that Gottemoeller points out is that the emergence of citizen-led efforts should result in an increased level of trust between the state and the citizens of that

---

[154] Emily Langlie, "Seattle Area Man Who Fled to Mexico, Sentenced for Bank Fraud in 'Lies for Loans' Scheme Defendant Defrauded Credit Unions with Phony Purchase Orders for Luxury Cars," The United States Attorney's Office Western District of Washington, August 9, 2010, http://www.justice.gov/usao/waw/press/2010/aug/sopo.html (accessed September 2, 2012).

[155] Mike Shuster, "A New Weapon against Nukes: Social Media," National Public Radio, February 8, 2012, http://www.npr.org/2012/02/08/146589700/a-new-weapon-against-nukes-social-media (accessed September 2, 2012).

[156] Ibid.

[157] Ibid.

state. Additionally, the decreasing cost of technology will continue to allow non-governmental agencies to acquire advanced technologies ranging from satellites to hand-held devices.

There are several iPhone applications, for example, that can turn an everyday iPhone into a fairly accurate radiation meter. Increasing one's investment from 99 cents to around $50, people can buy a surprisingly accurate Geiger counter attachment that connects directly to an iPhone or iPad. The potential of combining open source satellite verification and transparency qualities, Facebook and Twitter communication and dissemination qualities, and the ability to use an everyday, hand-held Geiger counter device in an effort to locate and track nuclear materials is important. Of course, the opposite view of this combination could be viewed by some as espionage or treason. Thus, the CIA must be cautious about how it advances this empowerment of citizens.

L. INFORMATION OPERATIONS

There are numerous ways in which social media can be used to conduct information operations. At the strategic level it is being used by U.S. European Command (EUCOM) to influence multi-lingual citizens across EUCOM's area of operations. The primary platforms are a regional Web initiative call Southeast European Times or SETimes and a companion Facebook page.[158] These websites provide a variety of tools such as forums, and polls that encourage online community interaction. Over time and through repeated exposure to EUCOM messaging, a surprising 93 percent of SETime's Facebook fans who responded to a poll acknowledged they had been affected by information provided on SETimes.com and the companion Facebook page.[159] Another example involves the Russian government's use of social media.

The Russian government recently purchased a software package called *Storm 12*. Storm 12 is designed to automatically spread government generated messages throughout the social media environment, in addition to pre-prepared influence messages aimed at

[158] Jamie Efaw and Christopher Heidger, "Another Tool in the Influencer's Toolbox: A Case Study," https://globalecco.org/97#All (accessed May 20, 2013).

[159] Ibid.

the mass social media network audience. Clearly, governments around the globe realize the potential power inherent in social media and are investing in the technology to stay ahead of the competition within the social media environment.

M. OPEN SOURCE INTELLIGENCE (OSINT)

The U.S. consulate in Benghazi was attacked by terrorists on September 11, 2012. The result of the attack included the deaths of four Americans. Despite a delay in mainstream news coverage, information about the attack, including videos and pictures, appeared on social media almost immediately.[160] On September 12, President Obama announced the death of U.S. Ambassador Chris Stevens at 0721 EST. Five hours before the announcement gruesome pictures of the Ambassador's body had already been posted on Facebook. Additionally, anti-American Twitter accounts reported that Salafi Islamists were responsible for the attacks. Subsequent investigations into the attacks revealed that several DoD operations centers in the region were relying on mainstream reporting sources for information on the attack and had not scanned social media platforms for additional details.[161]

Although information taken from social media cannot replace traditional intelligence sources, it can help establish what is happening on the ground, especially in times of crisis. Thus, social media should augment, but not replace, OSINT and other forms of intelligence. Ignoring the information that social media provides during periods of conflict is no longer acceptable. There are many other ways to make use of the open source information available on social media platforms.

Language sentiment analysis (LSA) software can be used to analyze written content that is posted to the Internet to determine who authored the material. Social media data can also be used as an early warning system since the frequent appearance of certain key words can be used as predictors of future violent events such as riots and

[160] Gupta and Brooks, *Using Social Media*, 143.

[161] Ibid., 144.

protests.[162] In the Common Operational Research Environment (CORE) lab at the Naval Postgraduate School, analysts are able to combine open source social media data with advanced analytical methodologies to provide commanders greater fidelity about their operating environment. Using social network analysis software, temporal records, geospatial data, and relational analysis, CORE lab researchers can create new ways of visualizing the battlefield which allows policy-makers and military leaders to make more informed decisions.[163]

N. PREDICTIVE CAPABILITY

A final look at the U.S. government's use of social media revolves around the efforts of the Federal Bureau of Investigation (FBI). Although the FBI readily acknowledges the value of the information provided by open source social media sources, the organization is looking to develop the ability to identify and geo-locate breaking events and emerging threats.[164] In a posting on the Federal Business Opportunities website, the FBI wants to develop the following application:

> The information gathered from news and social media outlets would be overlaid onto a digital map, pinpointing the location of the "breaking events," along with all other relevant contextual data. Additional information, including U.S. domestic terror data, worldwide terror data, the location of all U.S. embassies, consulates and military installations, weather conditions and forecasts, and traffic video feeds, would also be overlaid on the map. A robust search feature would also be incorporated into the app, which would allow the ability to instantly search and monitor key words and strings in 'publicly available' tweets across the Twitter Site and any other 'publicly available social networking sites/forums,' according to the RFI. The FBI wants the search function to allow for simultaneous key word searches that can look at 10 or 20 separate incidents/threats at the same time within the same 'window.' The ability to

---

[162] Gupta and Brooks, *Using Social Media*, 157.

[163] Seth Lucente, Greg Wilson, Rob Schroeder, and Gregory Freeman, "Crossing the Red Line," From the *CORE: Common Operational Research Environment Quarterly Newsletter*, April 2013, Issue 3, 3.

[164] Andrew Counts, "Minority Report is Real: FBI Wants to Use Social Networks to Prevent Future Crime," Digitaltrends, January 26, 2012, http://www.digitaltrends.com/social-media/minority-report-is-real-fbi-wants-to-use-social-networks-to-prevent-future-crime (accessed September 4, 2012).

> monitor tweets and other social media data in a minimum of 12 foreign languages, and to immediately translate those posts into English, is also outlined as a required feature of the application.[165]

As opposed to simply understanding the current situation on the ground, the FBI wants to use social media to actually predict the future. According to the FBI, social media provides unique access to communications about non-ordinary events in advance of their occurrence. An example of how this can work is provided by a Rand Corporation study which used Linguistic Inquiry and Word Count (LIWC)[166] software to analyze the Twitter hashtag #IranElection during the 2009 elections. The Rand study found that an increase in swear words in tweets was an accurate predictor of where and when protests would occur. This is similar to the research referenced earlier in this discussion of using LSA software to predict riots and protests.

O. CROWDSOURCING:[167] THE FUTURE OF SOCIAL MEDIA IN CONFLICT

Crowdsourcing is not a new concept. Examples abound in everyday life including putting pictures of missing children on milk cartoons, posting a wanted fugitive's mug-shots on television news programs, and providing general crime phone tip lines for citizens to report suspicious activity. However, when crowdsourcing techniques are combined with social media platforms, new possibilities emerge. These possibilities represent the next wave of social media technology applications for use in conflict.[168]

With crowdsourcing one can "accomplish previously unattainable objectives and accomplish existing objectives in a more efficient and inexpensive way."[169] Generally speaking, there are three primary objectives for using crowdsourcing for security purposes. These objectives include collecting intelligence, solving problems, and

---

[165] Counts, "Minority Report is Real."

[166] Linguistic Inquiry and Word Count (LIWC) is a text analysis software program designed by James Pennebaker, Roger Booth, and Martha Francis. For more information, see www.liwc.net.

[167] For complete instructions on building and running a crowdsourcing platform, see Chapter Eight of Gupta and Brooks, *Using Social Media*, 197–224.

[168] Gupta and Brooks, *Using Social Media*, 194.

[169] Ibid., 180.

influencing populations.[170] Collecting intelligence from crowdsourcing is a form of human intelligence collection (HUMINT). This type of HUMINT can be either direct or indirect. Direct intelligence requires asking someone for specific information (who pulled the trigger?). Indirect intelligence refers to the information received that still has to be sifted through and analyzed.[171] Crowdsourcing to solve problems simply refers to asking for the "wisdom of the crowd" to help solve challenging problems or complete difficult tasks. The third use of crowdsourcing with social media involves influencing target populations.

The key distinction between a crowdsourcing platform that utilizes social media technology and traditional influence platforms is that crowdsourcing involves continuous two-way dialogue and interaction. Rather than bombard people with radio advertisements or fliers handed out at markets, crowdsourcing correctly involves slowly persuading others to make changes to their behavior by facilitating their own belief that it is they, the participants, who are the ones promoting the change that you, the administrator want.[172]

Crowdsourcing platforms allow one to discreetly persuade a given populous and, if executed correctly, change a targeted group's behaviors and points of view. Goals for influence operations using crowdsourcing include countering extremist propaganda, providing intelligence, coming together to oppose a regime, and adopting a position more favorable to U.S. forces. Crowdsourcing can achieve these goals because by harnessing social media. Crowdsourcing platforms can provide a variety of media including pictures, videos, and text, and can send these repetitively to a target audience.[173] This is different from putting out information on a regular social media platform. Whereas social media sites such as Facebook and Twitter may help persuade dissidents to overthrow an

[170] Gupta and Brooks, *Using Social Media*, 191–193.

[171] Ibid., 194.

[171] Ibid., 180.

[171] Ibid., 226–27.

[172] Ibid., 301–02.

[173] Ibid., 305.

oppressive, dictatorial leader, combining crowdsourcing with social media allows one to ask those same dissidents the best way the U.S. government can help them overthrow their dictator.[174] Despite the potential that crowdsourcing represents, this technology should not be used when confidentiality and secrecy is very important or when a command's risk tolerance is low.

P. CONCLUSION

As shown, there are a variety of ways in which governments and those that oppose them use social media to achieve certain security objectives. In the United States, law enforcement agencies are using social media to catch criminals and terrorists who have already committed illegal acts, to spot potentially dangerous developments, and to try to stop criminals and terrorists before they act. In more oppressive states, social media is being used to monitor, identify, track, and locate those who oppose the powers in charge. Social media is also used to warn citizens to avoid government protests, as well as to spread pro-government propaganda. Despite this growing trend, discussions of social media and its integration into military operations is largely absent or non-systemic. Clearly, though, social media technology and the added value it brings in fusing the effects of kinetic and non-kinetic operations is too important to ignore in future special operations doctrinal publications.

Looking forward, social media will continue to be more intertwined and integrated into our everyday lives. The decreasing costs of hardware and software provide citizens access to technology once limited to nation states. The ability for governments to maintain and secure "secrets" is decreasing. Marrying assets that provide transparency and the ability to verify, such as civilian satellites, with social media assets, which allow for rapid communication and collaboration, will further blur the lines between ordinary citizens and their governments. This creates a delicate trust relationship between the government and the people. In addition, these developments should serve as

[174] Gupta and Brooks, *Using Social Media*, 199.

a warning to good natured citizens around the world. The Taliban, for example, has been reported to be using Facebook to gather intelligence on Australian soldiers heading to Afghanistan.

Basically, Taliban insurgents use attractive photos of women to befriend soldiers on sites like Facebook. Using the geo-tagging function built into many websites then allows the Taliban to determine the exact location where a post is made or photo is uploaded. Not only can soldiers unintentionally compromise on-going operations in country, but family and friends of soldiers can inadvertently jeopardize the military operations as well as themselves by providing sensitive information online.[175] Clearly, then, individuals must understand that everything that they post online could potentially be used by government entities and others for a multitude of purposes, some of which may not be in their best interests. Like it or not, social media is here to stay. Governments and citizens alike must be aware of its potential and be deliberate in their planned use of this powerful medium.

[175] Anthony Deceglie, "Taliban Using Facebook to Lure Aussie Soldier," *The Sunday Telegraph*, September 9, 2012, http://www.news.com.au/national/taliban-using-facebook-to-lure-aussie-soldier/story-fndo4bst-1226468094586 (accessed September 9, 2012).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ASSESSING THE USE OF SOCIAL MEDIA IN A REVOLUTIONARY ENVIRONMENT

As social media technological capabilities progress and the number of world-wide users of social media platforms continues to increase at a rapid rate (one in four people on earth will be using social media by 2014), it is inevitable that this communication medium will play some role in determining the outcome of all significant conflicts in the future.[176]

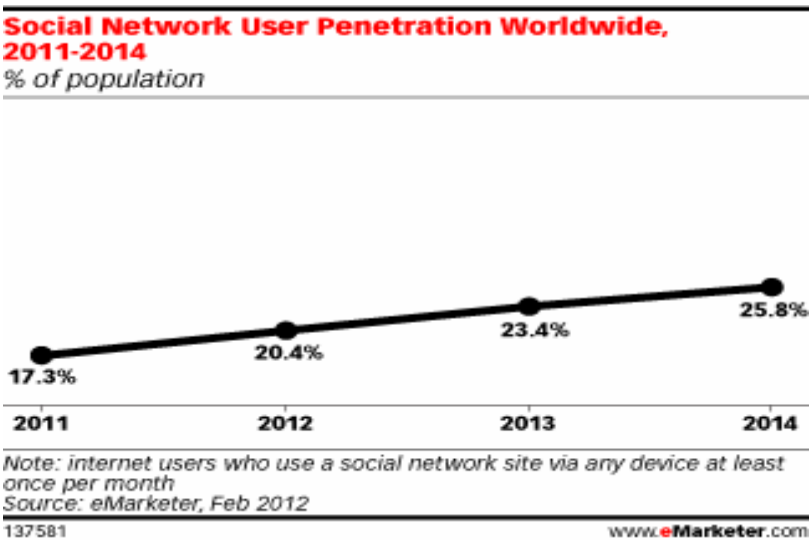

Figure 6. Percentage of the World's Population Using Social Media

Also, social media integration appears almost seamless to many people around the globe in nearly every facet of life from politics to entertainment, sports, the economy, education, and health care. For example, in some countries in East Africa, young people tend to think that Facebook *is* the Internet.[177] Therefore, it is of the upmost importance to understand how social media will impact the United States military's ability to shape

[176] e-Marketer.com, "Facebook Helps Get One in Five People Worldwide Socializing on Online Networks," http://www.emarketer.com/Article/Facebook-Helps-One-Five-People-Worldwide-Socializing-on-Online-Networks/1008903 (accessed April 22, 2013).

[177] Gupta and Brooks, *Using Social Media*, 20.

and influence the outcome of future military engagements. To that end, the first part of this final chapter will outline a number of key factors that should be taken into account by military planners in assessing the most appropriate use of social media technology in conflict. More specifically, this chapter primarily focuses on assessing the best use of social media technologies in support of an UW campaign. The second part of the chapter identifies the various overarching ways in which social media can be used in conflict. This menu of options is ranked based on the relevant amount of risk a person would face in using social media in a particular way. Finally, this chapter will address and identify the limitations and potential misuses of social media technology in revolutionary warfare, that is, both the conditions in which social media should not be used and the objectives that social media should not attempt to accomplish. This chapter is significant because the author suggests that the U.S. DoD must develop a methodology for assessing how to incorporate social media technology into war time plans.

Developing an assessment methodology is important because as the events of the Arab Spring unfolded it became apparent that the stories, videos, and still images that spread through the use of social media created the necessary spark of activism and outrage that fueled many people's revolutionary feelings.[178] This was evident in Tunisia where videos posted online to websites, like YouTube, of government forces committing violent acts against protestors motivated others to join the insurgent movement.[179] Social media can also accelerate and increase a key ingredient in building and sustaining revolutionary movements - the sense of inevitable victory.[180] This is achieved in part by rapidly and effectively spreading the narratives of the insurgent movement, which can ultimately help persuade otherwise neutral bystanders into supporting a resistance effort.[181] Finally, social media technology can rapidly accelerate the pace in which

[178] Petit, "Social Media," 32.

[179] Gupta and Brooks, *Using Social Media*, 5.

[180] Petit, "Social Media," 32.

[181] Ibid., 37.

social organizations are formed, and expand the possibilities for recruiting, communicating, and mobilizing those individuals that make up an insurgent group.[182]

With the importance that social media will play in future UW and insurgent operations established, the thesis will examine how to assess the appropriate use of social media technology in a given country/situation to help U.S. armed forces achieve their desired end-states. By going through the following list of considerations, a military strategist will be in a better position to determine which of the uses of social media would best support U.S. objectives in a revolutionary environment.

A. INTERNET USAGE

This is the first and most basic consideration a strategist should consider when analyzing the social media environment in a given country. The total number and percentage of the population with access to the Internet helps to make the first big "cut" when designing the integration of social media into military plans. Basically, it would not make a lot of sense to attempt to engage a target population through Internet-based social media platforms if the vast majority of citizens were not online. However, just because a given citizenry does not have access to the Internet does not mean that using social media to support military operations should be ruled out.

Mobile phone-based social media applications, for example, might still be a viable option. Additionally, Internet-based social media platforms may still be appropriate despite a relatively low number of Internet users in a given country should the operation have a limited desired end-state. In other words if the goal is to overthrow a dictatorial regime and less than five percent of the total population is online, a Facebook-like social media platform may not be appropriate in mobilizing a large percentage of the citizens to protest in the streets of the target country. As a point of reference, Tunisia's Internet penetration is 39.1 percent, Egypt's is 35.6 percent, Libya's is 17.0 percent, and

[182] Petit, "Social Media," 34.

Yemen's is 14.9 percent.[183] Although social media were used to some degree in each of these four countries that experienced regime change during the Arab Spring, the citizens in Tunisia and Egypt relied on social media to a greater extent in mobilizing their populations. However, if the goal is more limited in nature, such as building a core cadre of defectors, then even in a country with minimal Internet access, using Internet-based social media platforms may be appropriate. An example will make this point clear.

Despite Cuba's recently (January 2013) activating an undersea fiber optic ALBA-1 cable, the majority of Cuban residents do not have full access to the Internet. Estimates range from 2.9 percent to 10 percent.[184] However, even before this fiber optic cable was activated, certain categories of Cuban citizens were (and still are) allowed to have Internet access in their homes. Groups that are authorized to have Internet access at home include doctors, senior managers, and select academics.[185] Therefore, if the U.S. military wanted to build a core group of underground leaders that included individuals from these groups, then Internet-based social media might be an appropriate means of reaching and interacting with them. Table 4 provides data on potential countries of interest.

[183] Internet World Stats, "World Internet Usage and Population Statistics June 30, 2012," http://www.internetworldstats.com/stats.htm (accessed March 22, 2013).

[184] Peter Orsi, "Cuba Internet Cable Turned On, Juicing up Country's Connection to Outside World," *The Huffington Post*, January 21, 2013, http://www.huffingtonpost.com/2013/01/22/cuba-internet-cable_n_2521330.html (accessed February 5, 2013).

[185] The Economist, "Wired, at Last," *The Economist*, March 3, 2011, http://www.economist.com/node/18285798 (accessed February 4, 2013).

Country	# of Internet Users	% Internet Penetration
Iran	42,000,000	53.3%
Russia	67,982,547	47.7%
Venezuela	12,097,156	41.1%
China	538,000,000	40.1%
Syria	5,069,418	22.5%
Djibouti	61,320	7.9%
Afghanistan	1,520,996	5.0%
Somalia	126,070	1.2%
North Korea	Not Significant	Not Significant
Tunisia	4,196,564	39.1%
Egypt	29,809,724	35.6%
Libya	954,275	17.0%
Yemen	3,691,000	14.9%

Table 4. Internet Access and Penetration in Select Countries as of June 30, 2012[186]

B. SOCIAL MEDIA USAGE

After determining the total number of Internet users and the percentage of the population this represents, it is important to understand how many of those with access to the Internet actually use social media technology. Additionally, it is important to determine which social media sites people in a targeted country actually use. Regimes concerned about the mobilizing potential that can be achieved through the use of social media technology are increasingly blocking major, non-state controlled social media websites like Facebook and Twitter in favor of social media sites that are controlled from within the country. Examples of state-authorized social media platforms in repressive countries include Qzone, Tencent Weibo, Sina Weibo, and Wechat in China.

Some of the countries that block major U.S.-based social media platforms including Facebook include China, Iran, North Korea, Syria, Myanmar, Cuba, and Zimbabwe. In these instances, a planner may have to use alternate social media platforms or mobile phone-based platforms, or start a new social media website using ning.com or another turn-key type Internet service company. The difficulty with this latter option is to

[186] Internet World Stats, "World Internet Usage."

drive enough people from a targeted demographic to make a newly created social media site viable. This option also depends on the nature of the goal for the use of social media technology. If the goal involves executing information operations on a large scale, developing a newly created social media website may not be the right course of action.

Country	# of Facebook Users	% Facebook Penetration
Iran	Not Significant	Not Significant
Russia	7,963,400	5.6%
Venezuela	9,766,540	33.1%
China	633,300	0.0%
Syria	Not Significant	Not Significant
Djibouti	50,140	6.5%
Afghanistan	384,220	1.3%
Somalia	123,480	1.2%
North Korea	Not Significant	Not Significant
Tunisia	3,328,300	31.0%
Egypt	12,173,540	14.5%
Libya	781,700	13.9%
Yemen	495,440	2.0%

Table 5. Total Number of Facebook Users as of December 31, 2012[187]

In terms of planning to use social media technology to support UW, the key take-away from this section is two-fold. First, before going into a given country, how indigenous personnel use social media must be understood. Second, what specific websites or technologies local people use must be known so that these platforms may be monitored and utilized.

C. MOBILE PHONE USAGE

After examining the targeted countries Internet and social media usage aggregate numbers, the next step in assessing the social media environment is to look at the country in question's mobile phone usage and penetration rate. A quick examination of Table 6 shows that the number of cell phones in service in each country and the penetration rate is

[187] Internet World Stats, "World Internet Usage."

much higher than the number of Internet and social media users. A closer examination reveals certain situations in which Internet-based social media platforms may not be appropriate in a given country, but where the mobile phone-based social media may be appropriate. For example, Afghanistan's Internet penetration rate is only 5.0 percent, but the country's mobile phone penetration rate is 57.7 percent.

Another important consideration, especially in relatively poor countries where mobile phone social media platforms may be the only viable option, is to factor in the cost of SMS to one's target audience. If the cost of sending and receiving SMS messages is exceedingly costly, individuals are less likely to engage through this medium.[188] However, there are ways of off-setting the cost of SMS to potential movement participants such as automatically reloading their SIM card with additional credits. One other important characteristic of global mobile phone usage is that in several countries there are more mobile phones in service compared to the total population. This is not unusual even in poorer countries in Africa where it is normal for people in the upper-income levels to have two mobile phones on different networks and sometimes even three or more phones.[189]

[188] Sokari Ekine, "Introduction," in *SMS Uprising: Mobile Activism in Africa*, ed. Sokari Ekine (Oxford: Pambazuka Press, 2010), xiii.

[189] Ibid., x.

Country	# of Mobiles Registered	% Mobile Penetration
Iran	56,043,000	71.1%
Russia	236,700,000	166.1%
Venezuela	28,782,000	97.6%
China	986,253,000	73.4%
Syria	13,117,000	58.2%
Djibouti	193,000	24.9%
Afghanistan	17,558,000	57.7%
Somalia	655,000	6.5%
North Korea	1,000,000	4.1%
Tunisia	12,388,000	115.4%
Egypt	83,425,000	99.7%
Libya	10,000,000	178.1%
Yemen	11,668,000	47.1%

Table 6. 2011 Total Number and Penetration Rate of Mobile Phones[190]

D. THE SOCIAL MEDIA ENVIRONMENT

This consideration focuses on trying to gain an understanding of the overall social media environment. This can be partially accomplished by using the conceptual model introduced in chapter 2. This graphical representation provides a means of organizing and framing the overall media environment and can help determine how much freedom of maneuver on social media platforms a person has within the specific country of interest. The next three considerations (government Internet and SMS censorship, government Internet surveillance, and security force effectiveness and enforcement capability) will provide the details needed to develop a more robust understanding of the social media environment one will be potentially operating in. An example will provide clarification as to how to examine this aspect of the assessment methodology.

In a recent field survey, Iranian citizens were asked what their three most important news sources were. Of those Iranians surveyed, the vast majority stated that television (96 percent), the press (55 percent), and strong personal ties (51 percent,

[190] Central Intelligence Agency, "Country Comparison: Telephones—Mobile Cellular," https://www.cia.gov/library/publications/the-world-factbook/rankorder/2151rank.html (accessed February 17, 2013).

including family and close friends) were the top three sources for general information.[191] The complete list is shown in Table 7. It is interesting to see that information obtained from the Internet and through SMS ranked higher than information received from mosques. Also, the information received while in a taxi cab was almost as valued as information communicated in mosques. Finally, only one percent of people indicated they used government offices as a source of information, though the state run IRIB television channel was listed most frequently (86 percent) as the most watched channel in Iran. State controlled radio station Radio Payam (31 percent) was the most popular among those who selected radio as a primary means of receiving information, while Radio Farda (4 percent) was the most popular international radio program.

Communication Medium	% Using As Source of Information
Television	96%
Press	55%
Strong Social Ties	51%
Radio	32%
Weak Social Ties	28%
Internet	26%
Work / School	19%
SMS	12%
Mosque	9%
Taxi	7%
Shops / Café	2%
Government Offices	1%

Table 7. Ranked Communications Mediums that Are Used to Gather Information in Iran

In discussing SMS texting, most survey respondents indicated that SMS was a popular advertising medium and was used frequently to exchange jokes.[192] However, it is not used as extensively for new and informational purposes and was subject to some

[191] Magdalena Wojcieszak, Briar Smith, and Mahmood Enayat, "Finding a Way: How Iranians Reach for News and Information," The Iran Media Program's 2011-2012 Report on Media Consumption in Iran, http://www.global.asc.upenn.edu/fileLibrary/PDFs/FindingaWay.pdf (accessed April 12, 2013), 11.

[192] Wojcieszak, Smith, and Enayat, "Finding a Way," 12.

regime blocking when politically and socially sensitive topics were discussed.[193] Despite being a signatory of the International Covenant on Civil and Political Rights, an international agreement that stresses that every person should have the freedom of expression, most Iranian citizens feel anything but free to express themselves.[194] In fact a common trait that can be seen in the lowest news sources (mosques, taxis, shops/cafes, and government offices) is that they are all public places. This may mean that individuals are especially guarded when outside of their own homes. Also, the strong scores given to both strong and weak social ties indicate that a certain level of trust exists among offline social networks in Iran.

In terms of Internet use, the younger demographic members favored the Internet compared to older demographic members, and the majority (66.5 percent) used the Internet at home compared to only 14 percent at work and nine percent in Internet cafes. Specifically looking at social media platforms, 42 percent of Internet users reported reading blogs, 20 percent reported using Internet-based social media websites, 18 percent stated they commented on other peoples blogs, and eight percent reported writing their own blogs.[195] Only two percent of Internet users reported using Twitter, and of those, most stated they only used Twitter a few times a month. The survey also asked Iranian citizens what topics they discussed most often on social media. The results are summarized in Table 8.

[193] Iran Media Project, "Text Messaging as Iran's New Filtering Frontier," April 25, 2013, http://www.iranmediaresearch.org/en/blog/227/13/04/25/1360 (accessed May 2, 2013).

[194] Wojcieszak, Smith, and Enayat, "Finding a Way," 5.

[195] Ibid., 18.

Topic Discussed	% of Respondents
Personal Issues	37%
Social Issues	32%
Cultural Issues	30%
News	29%

Table 8. Most Frequently Discussed Topics on Social Media in Iran[196]

A second, online only survey was conducted using the file sharing website 4shared.com. The survey was written in the Persian language. Surprisingly 4shared.com is not filtered in Iran.[197] The survey was designed to examine the potential of using social media for sociopolitical exchange and mobilization. The results of this second survey, completed by 2,802 respondents, showed more promise in terms of the potential of social media's utilization in Iran.

Before discussing the results of this survey, it is helpful to describe the demographics of those completing the survey: 80 percent of respondents were under 30 years old, 92 percent were male, 78 percent had a university degree, and 20 percent stated they held a masters or PhD.[198] To start examining the results of the follow-on survey, the information sources that these Internet experienced Iranians stated were most important to them is covered. Table 9 summarizes the results.

[196] Wojcieszak, Smith, and Enayat, "Finding a Way," 22.

[197] Ibid., 26.

[198] Ibid., 27.

Communication Medium	% Using As Source of Information
Internet	85%
Television	67%
Strong Social Ties	39%
Press	29%
Work / School	22%
Radio	11%
Government Offices	9%
Weak Ties	6%
Mosques	4%
Taxi	4%
SMS	3%
Shops / Café	0%

Table 9. Iranian Internet Users Most Important Sources of Information[199]

It is interesting to note how the Internet went from only 26 percent to 85 percent in terms of how many people view it as an important source of information. Admittedly, these results are from a different survey using a different collection methodology. Still, the significant difference is telling. It is also noteworthy to see that Internet savvy individuals did not place a higher value on information gleamed from SMS. It is also interesting to examine where this target demographic accesses the Internet.

The survey respondents indicated that accessing the Internet was mostly done at home (84 percent), followed by work (36.5 percent), school (33 percent), their mobile phone (30 percent), and Internet cafes (25 percent). In terms of specific online activities, reading blogs (92 percent) and commenting on blogs (70 percent) were more popular compared to simply belonging to an online social network (68 percent). Twitter use amongst this specific group was much higher compared to the population at large with 17 percent reporting they use Twitter and follow other's tweets. The mobile phone use findings are a bit more promising for those interested in the potential of social media utilization in Iran.

[199] Wojcieszak, Smith, and Enayat, "Finding a Way," 29.

A full 91 percent of respondents stated they had cell phones. Although this figure is higher than what is listed in Table 9, this survey was taken in late 2012 whereas the CIA data was collected in 2011. Of those with cell phones, 79 percent reported sending text messages in the past month and 35 percent stated they recorded a video using their cell phone in the past month. However, only five percent of those who recorded videos on their phone followed this action up and posted the video to the Internet. Roughly half of mobile phone users reported either sending or receiving digital content through Bluetooth.

This part of the social media assessment tool tells how using social media technology in Iran might be approached. It points to using mobile phones if a broad audience is desired, but that if the targeted demographic is young, highly educated, tech-savvy males, Internet-based social media may still be a viable option for interacting with this specific group. Additionally, the data shows the importance of off-line social networks, and highlights a trust undercurrent amongst the citizens in Iran in terms of the faith they put in their family, close friends, and neighbors. The survey also hints at the possibility that people do not blindly follow what is disseminated at their local mosques, nor what their local government offices are reporting. The data also suggests that most Iranians are hesitant about discussing topics of a sensitive nature in public. This means there may be a real fear of surveillance and enforcement mechanisms under state control. The next several parts of the assessment methodology are designed to provide additional details that should be accounted for in operational planning.

E. GOVERNMENT CENSORSHIP

The next step in the social media assessment process is to examine how and what the targeted government is censoring on both Internet-based social media and SMS texting. Additionally, it is important to know which social media sites are blocked and which ones are not and whether or not SMS is restricted in any way. These considerations furthers an understanding of what the social media model described in Chapter II looks like in a specific country by describing the contested and uncontested media spaces. Opennet.net provides a wealth of information on dozens of governments' attempts to

censor and block the Internet in their own countries.[200] The figures on the following pages provide examples of the types of data available at the website. The countries shaded in grey are ones where no data was collected, but this does not mean that filtering does not take place in those countries. By understanding what websites are blocked, and what types of content or keywords are filtered, an understanding of the constraints and obstacles that are in place and must be accounted for when developing plans that incorporate social media technology can be considered

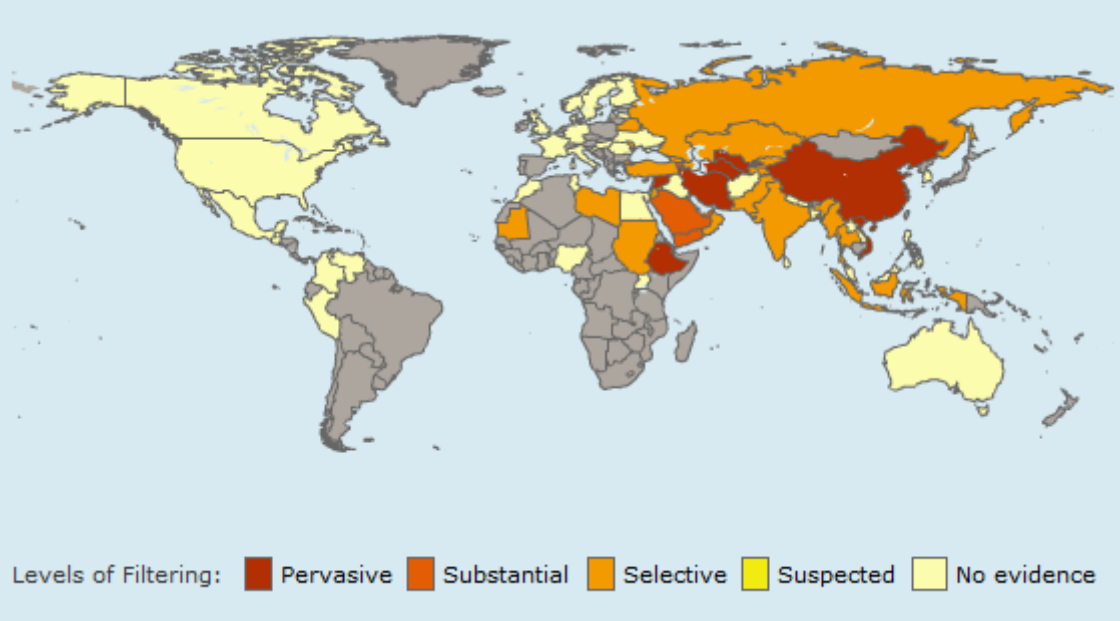

Figure 7. Global Internet Filtering of Internet-Based Political Content[201]

[200] For more information on country specific filtering of the Internet see https://opennet.net/research/profiles, or the books found at http://access.opennet.net/, *Access Denied*, *Access Controlled*, and *Access Contested*.

[201] OpenNet Initiative, "Global Internet Filtering Map," Opennet.net, http://map.opennet.net/filtering-pol.html (accessed December 12, 2013).

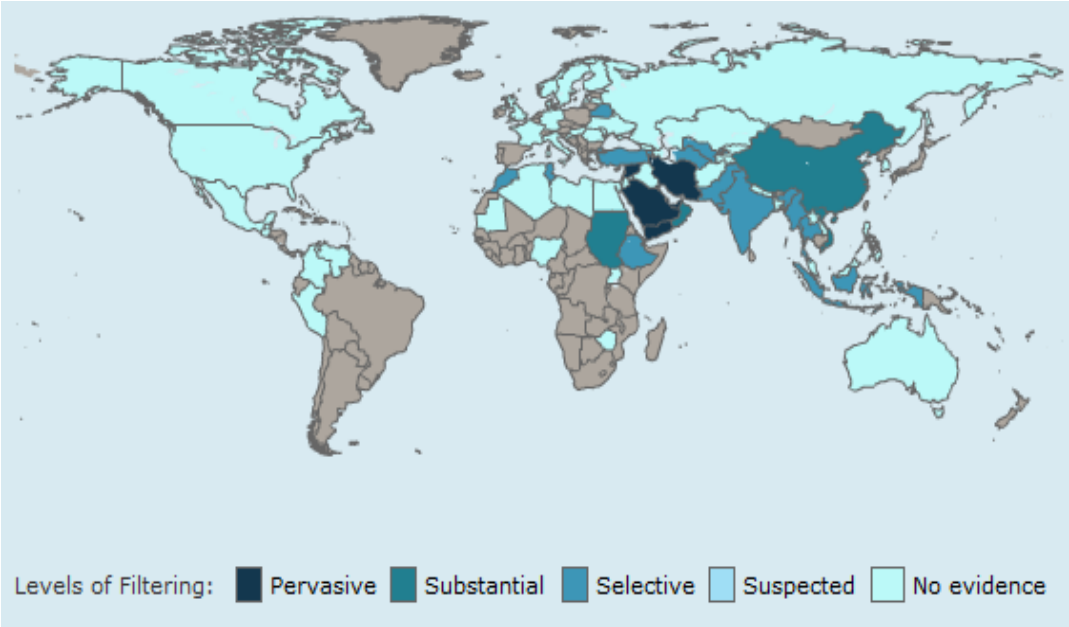

Figure 8. Global Internet Filtering of Internet Tools[202]

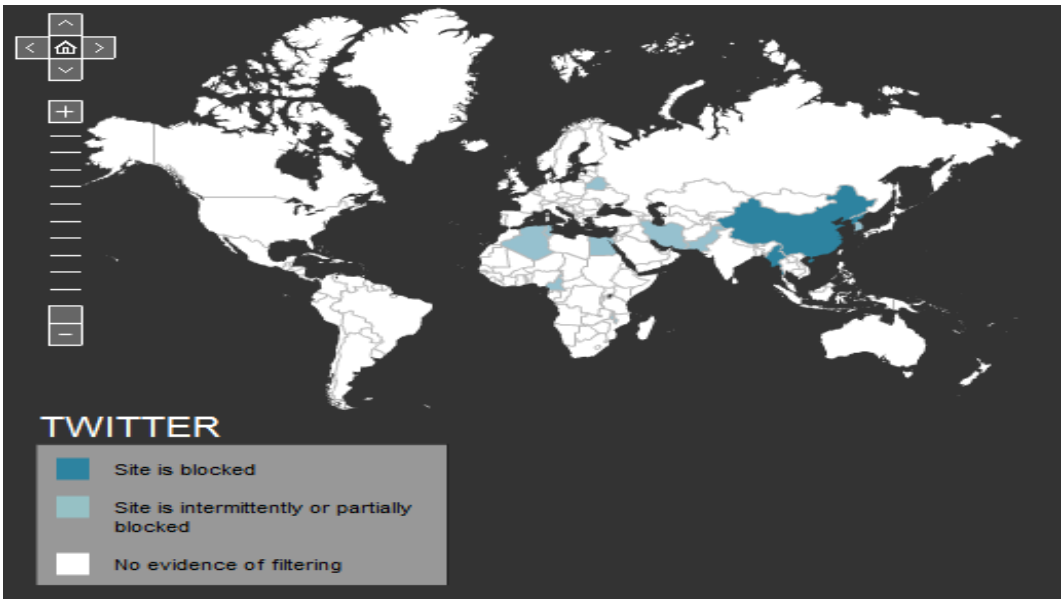

Figure 9. Global Internet Filtering of Twitter[203]

[202] OpenNet Initiative, "Global Internet Filtering Map," Opennet.net, http://map.opennet.net/filtering-IT.html (accessed December 12, 2013).

[203] Ibid.

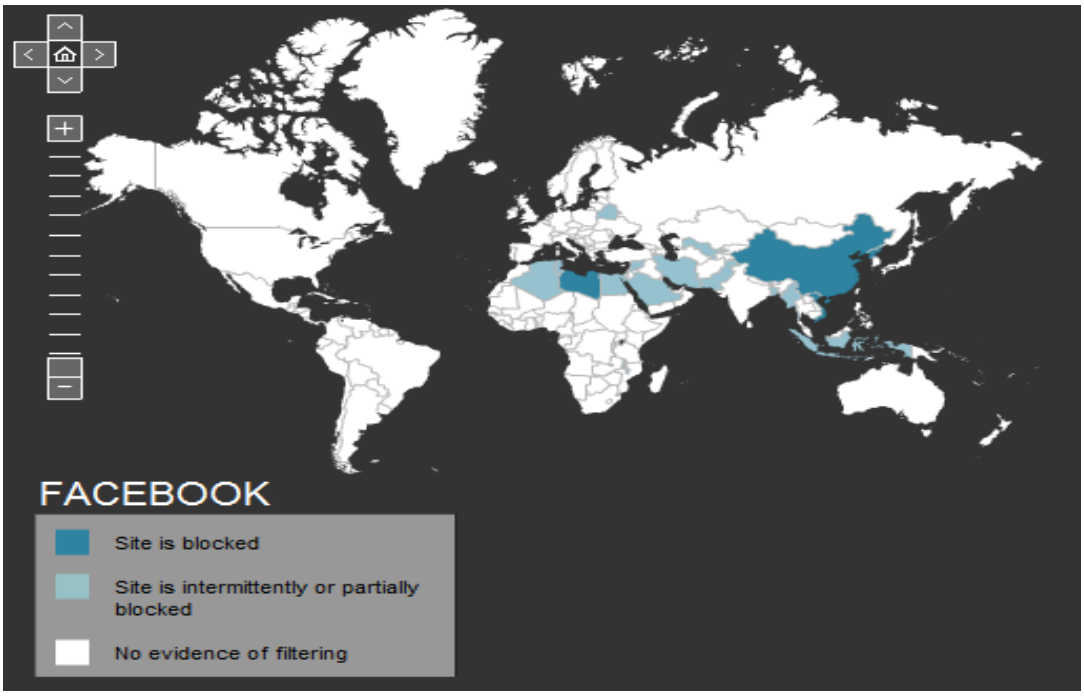

Figure 10. Global Internet Filtering of Facebook[204]

Also, this type of information helps determine whether existing social media platforms like Facebook and Twitter can be utilized, or if newly developed sites will have to be constructed to remain free from blockage. The obvious challenge in this scenario is the consideration of building an online network from scratch versus trying to tap into and utilize an existing social media-based social network. The next factor to assess is the opposing government's Internet surveillance capabilities.

F. GOVERNMENT INTERNET SURVEILLANCE CAPABILITY

As the figures above illustrate, a multitude of countries actively block social media websites and censor/filter certain keywords and topics that are posted online. In addition to these measures, governments use a variety of hardware and software to conduct surveillance on individuals active on the Internet. Specific techniques were described in detail in Chapter II. The point in this portion of the assessment is to gain an understanding of how a target government conducts online surveillance, and how

[204] OpenNet Initiative, "Global Internet Filtering Map."

pervasive the surveillance actually is. An interesting example of a repressive regime using a unique means of keeping its citizens off the Internet as well as keeping social media users under surveillance can be found in the former Soviet republic of Azerbaijan.

During the last several years the government of Azerbaijan has executed a media campaign designed to discourage its people from even accessing the Internet, let alone using social media websites such as Facebook. This form of social filtering associates the use of social media with being a deviant, criminal, and a traitor![205] To this end, state controlled television programs air episodes of shows that result in various family tragedies and criminal incidents because a young person joins Facebook and Twitter. In early 2011, the state's chief psychiatrist stated publically that social media users cannot maintain relationships and will suffer mental disorders. In April 2012, the Ministry of the Interior linked Facebook with human trafficking and the sexual abuse of young people.[206] All of this effort has been put into curtailing the use of the Internet even though 78 percent of Azerbaijanis have never been on the Internet, and while only seven percent of citizens report having a Facebook account.

Also, instead of openly restricting all citizens from using the Internet or blocking sites like Facebook and Twitter as other repressive regimes do, the government of Azerbaijan uses Internet surveillance to allow the regime to monitor and punish any rebellious activity.[207] By purporting the narrative that Internet use is bad, the government has fewer individuals to keep under online surveillance. One example of the effectiveness of leaving popular social media sites unblocked, but under surveillance, occurred in 2010. Two Azerbaijan activists were arrested and imprisoned for posting a video on YouTube. The video the activists posted satirized government waste. Although this particular case

[205] Sarah Kendzior and Katy Pearce, "How Azerbaijan Demonizes the Internet to Keep Citizens Offline," Slate.com, May 11, 2012, http://www.slate.com/blogs/future_tense/2012/05/11/azerbaijan_eurovision_song_contest_and_keeping_activists_and_citizens_off_the_internet_.html (accessed April 10, 2013).

[206] Ibid.

[207] Ibid.

was not publicized in Azerbaijan print media, it was reported online. The online reporting created fear among other bloggers, and the net result was a decrease in Internet-based political dissent.[208]

After events unfolded during the Arab Spring, the government of Azerbaijan became even more aggressive in its campaign against social media use as well as its Internet surveillance. The government portrayed users of social media sites as bad citizens of Azerbaijan. This campaign appears to be effective as neighboring Georgia and Armenia (which have similar Internet access and computer hardware costs) have more than doubled the amount of daily Internet users (20 percent versus seven percent) and computers with Internet connections at home (33 percent and 40 percent versus 11 percent). By framing the Internet as a "dangerous" place, the government has been especially effective in keeping women offline, as only 14 percent of women across the country have been on the Internet. Additionally, women in Azerbaijan are concerned about violating their family's honor by engaging in online discussion forums.[209] Thus, by combining and reinforcing social filters with the demonstrated ability to keep social media platforms under surveillance and to punish those who "misuse" it, the government of Azerbaijan has been effective in controlling the information its citizens consume.

G. SECURITY FORCE EFFECTIVENESS AND RANGE OF INFLUENCE

Ultimately what people care about in terms of whether or not to join a resistance movement and what potentially prevents them from joining a social or insurgent movement is partially based on their perceived level of risk to themselves and their families. As an insurgent movement begins to gain increased political power, which also encourages those in a movement to act collectively, the risks associated with being an insurgent begin to diminish.[210] This in turn, is one factor that assists in facilitating the process of cognitive liberation, which research indicates can lead to a sustained social

[208] Kendzior and Pearce, "Azerbaijan Demonizes the Internet."

[209] Ibid.

[210] McAdam, *Political Process*, 43.

movement.[211] One of the most critical important factors in determining if a social movement can increase its political power is the effectiveness of the ruling regime's security force effectiveness and range of effectiveness.

In Yemen, for example, the military and Central Security Forces generally have control of the capital city of Sana'a, though the city is basically divided between the areas in the southern part of the capital that are loyal to former president Ali Abdullah Saleh and the northwest part of the city that is loyal to Ali Mohsen and the Ahmar family.[212] However, regime control of much of the areas outside the capital are extremely diminished. The al-Houthi rebel group, for example, has complete control over the northern provincial capital of Saada.[213] Thus, in Yemen, the reach of the government's security forces is limited. This situation provides potential insurgents in Yemen with a lot of physical freedom of movement. In other words, an insurgent operating outside the capital of Sana'a could post any type of information on social media platforms without the fear of being arrested simply because Yemen's security forces do not have the necessary range of influence to do anything about the online protests. This relationship between an insurgent's relative strength and the distance from a state capital is shown graphically in Figure 11.

---

[211] McAdam, *Political Process*, 51.

[212] Sudarsan Raghavan, "Powerful elite Cast a Shadow over Reforms in Yemen," *The Guardian*, February 22, 2013, http://www.guardian.co.uk/world/2013/feb/26/yemen-powerful-tribal-families-influence (accessed March 12, 2013).

[213] Adam Baron, "Yemen's 'Death to America' Rebels Bring Calm to Northern Yemen," *The Christian Science Monitor*, October 28, 2012, http://www.csmonitor.com/World/Middle-East/2012/1028/Yemen-s-Death-to-America-rebels-bring-calm-to-northern-Yemen (accessed March 12, 2013).

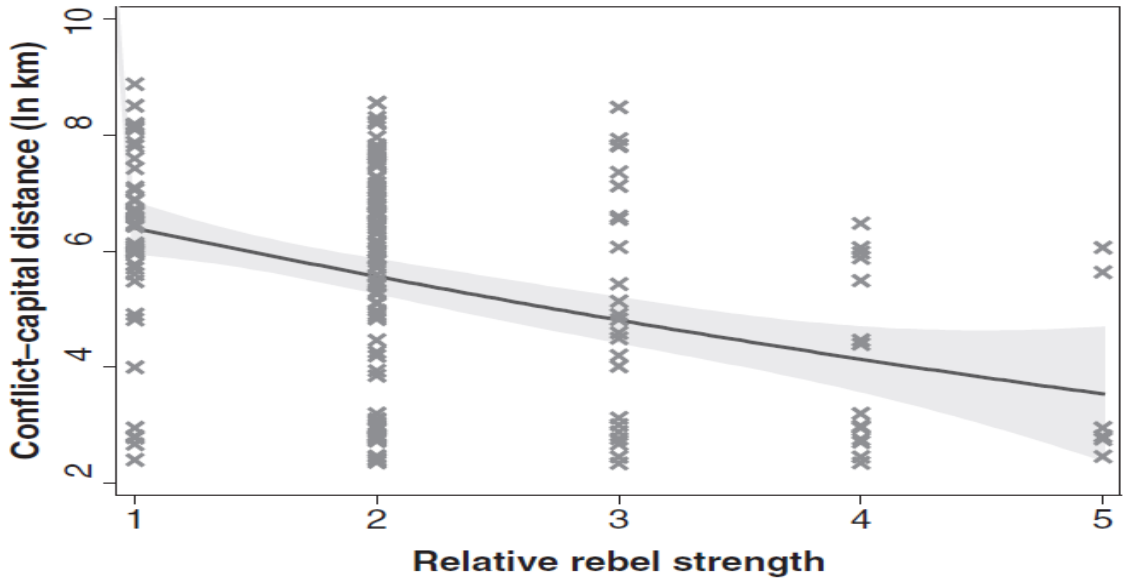

Figure 11. Rebel Military Strength in Relation to the Distance From the Capital City[214]

Also, the absence of restrained or repressive control measures is associated with an increase in social movement activity. Thus, research indicates that as a state's ability to act repressively declines, the chances of seeing a resistant social movement increases.[215] Examples of this dynamic can be found in Iran in the late 1970s, when large portions of the armed forces withdrew support for the Shah, in the Solidarity Movement in Poland when Soviet leaders failed to aggressively repress that movement, and more recently in Egypt when the Egyptian Army refused to fire on its own people during the January 20 Revolution that resulted in the removal of Hosni Mubarak from office. So, in this portion of the social media assessment, it is necessary to evaluate the effectiveness of a government's security forces, the operational reach of those various security forces, and whether or not a particular country's military is willing to turn against its own people with violent force.

[214] Halvard Buhaug, "Dude, Where's My Conflict? LSG, Relative Strength, and the Location of Civil war," *Conflict Management and Peace Science* 27, no. 2 (2010): 107–128.

[215] Doug McAdam, "Micromobilization Contexts and Recruitment to Activism," *International Social Movement Research*, 1(1988), 130.

H. INTERNET AND MOBILE PHONE INFRASTRUCTURE

Assessing existing Internet and cell phone infrastructure will help the U.S. determine whether it will have to provide additional, potentially mobile and/or temporary infrastructure to support the use of Internet-enabled or cell phone-enabled social media technology. This information will in turn help determine whether the U.S. should focus on Internet-enabled social media technology or on cell phone-enabled social media technology (i.e., SMS).

The SMS can be used for some of the same purposes as Internet-based social media such as mass messaging. An effective tool that facilitates this capability is BulkSMS. Also, cell phones, particularly Internet-connected smart phones, can combine all other communications media. Cell phones can send and receive various forms of information and document events with text, audio, and video. Cell phones can broadcast multimedia almost instantly, and can be used to network with other cell phone users.[216] More generally speaking, cell phones can be used as a strategic tool to communicate, collaborate, coordinate, and support collective actions.[217] Mobiles are also advantageous as they are dynamic, diverse, discreet, and direct.[218] Cell phones are dynamic in the sense that they are generally carried by users all of the time, which facilitates instant and simultaneous communications. Cell phones are diverse in that they can connect otherwise unconnected people in a given society through the viral spreading of SMS messages. These devices are discreet in that they are often equipped with cameras and video cameras that can be used to film and take photos in situations in which using traditional camera equipment could be dangerous. Finally, cell phones are direct in that they can be used to communicate directly with a targeted audience.[219]

---

[216] Christian Kreutz, "Mobile Activism in Africa: future trends and software developments," in *SMS Uprising: Mobile Activism in Africa*, ed. Sokari Ekine, 17–31(Oxford: Pambazuka Press, 2010), 18.

[217] Ibid.

[218] Cristiana Charles-Iyoha, "Mobile Telephony: Closing the Gap," in *SMS Uprising: Mobile Activism in Africa*, ed. Sokari Ekine, 116–123 (Oxford: Pambazuka Press, 2010), 117.

[219] Ibid.

I. OFFLINE SOCIAL NETWORKS

This is an important consideration because ignoring traditional forms of communicating and bypassing indigenous forms of organizing can actually remove power from a given network of people.[220] One key to developing a strong network of individuals is to capitalize and utilize existing social networks. This was an important factor in the rapid expansion of the Nazi political party in the 1930s.[221] Existing social networks lower information and transaction costs for various resources by tapping into the trust inherent in pre-established social networks. These existing trust relationships also facilitate faster and more efficient member recruitment and member retention.[222] Social networks also provide channels through which unfiltered information can be circulated and which provides a counter-balance to official "state" information channels.[223]

Additionally, strong existing social networks can bypass barriers to collective action. Social networks, in other words, create an initial disposition to participate in a social movement. Social networks also connect potential recruits with an opportunity to protest by moving from internal objectives to taking action[224] Networks bypass these obstacles by raising money and providing resources needed for mobilization, spreading the risk amongst more individuals (and thus reducing each person's individual level of risk), and increasing social solidarity which all increase the likelihood of a collective identity emerging.[225] It is also important to note that social networks form the pool of

---

[220] Sokari Ekine, "Introduction," xiv.

[221] Helmut Anheier, "Movement Development and Organizational Networks: The Role of 'Single Members' in the German Nazi Party, 1925–30," in *Social Movements and Networks*, ed. Mario Diani and Doug McAdam, 49–76 (New York: Oxford University Press, 2003), 53.

[222] Ibid.

[223] Maryjane Osa, "Networks in Opposition: Linking Organizations Through Activists in the Polish People's Republic," in *Social Movements and Networks*, ed. Mario Diani and Doug McAdam, 77–104 (New York: Oxford University Press, 2003), 78.

[224] Florence Passy, "Social Networks Matter. But How?" in *Social Movements and Networks*, ed. Mario Diani and Doug McAdam, 21–48 (New York: Oxford University Press, 2003), 24.

[225] Osa, "Networks in Opposition," 78.

recruits most likely to join a social movement.[226] Thus, social media can be used to activate and mobilize people who are already part of an existing social network into a more robust, purpose driven movement, that is, existing social ties and networks can elevate the end-state or overall goal possible by tapping into these existing offline networks through social media technology. These elevated movement goals could include, for example, robust and rapid information sharing, a rapidly disseminated narrative, mobilization on the streets, or sustained protests.

J. BACKUP COMMUNICATIONS PATHS

These are an important consideration because in times of crisis, people will often revert to more traditional forms of communication rather than rely on social media technology such as SMS. An example of this can be found in the Democratic Republic of Congo where people prefer the use of voice calls over SMS in times of distress.[227]

Additionally, planners should always develop a communications PACE (primary, alternate, contingency, emergency) plan. For example, a central Facebook page (We are all Khaled Said in Egypt for example) could be the primary means of communication. The alternate means may be a mass SMS distribution list. The contingency could be an email distribution list, or an obscure, unknown, insurgent-created social media website developed on a platform like Ning.com which was described in Chapter Two. The emergency means of communication could be to use a concept called "beeping." Beeping refers to calling another person, who lets the call go unanswered and evaluates the meaning of the call based on the number of rings heard before the caller ends the call.[228]

---

[226] Sidney Tarrow, *Power in Movements* (Cambridge: Cambridge University Press, 1998), 124.

[227] Bukeni Waruzi, "Using Mobile Phones for Monitoring Human Rights Violations in the DRC," in *SMS Uprising: Mobile Activism in Africa*, ed. Sokari Ekine, 138–142 (Oxford: Pambazuka Press, 2010), 141.

[228] Kreutz, "Mobile Activism in Africa," 26.

For example, ending a call after letting the phone ring one time could mean to move ahead with the plan as agreed upon, while three rings could be to execute the alternate plan.

K. KEY SOCIAL MEDIA INFLUENCERS

There are movement entrepreneurs to be tapped into. These individuals provide the bridging social capital needed to bring together people from various local organizations.[229] Part of the success of the Nazi movement, generally considered an extremely effective social movement in the 1930s, was the ability to directly recruit and mobilize local leaders whose opinions were valued and respected within their local communities.[230] Social movement entrepreneurs strive to maximize the number of network members, mobilize necessary resources, provide a bridge between various local groups, forge alliances, and seek out opportunities that will increase the group's political power and influence.[231] These individuals appear to be most important and effective during the initial building phases of a movement.[232]

United States military planners need not look far to find two such social entrepreneurs. Although Paul Revere and Joseph Warren lived long before the advent of social media, the characteristics of these famous men of U.S. history can provide an example of the type of individual that should be sought out within the social media environment. In essence, both men excelled in their roles as social bridges that linked various disparate organizations spanning the gamut of social classes.[233] In addition both Revere and Warren had comparatively high numbers of weak ties. These ties are especially effective in connecting discrete group to each other.[234] These weak ties were the result of both Revere and Warren having connections to multiple social clubs such as

[229] Anheier, "Movement Development," 49.

[230] Ibid., 53.

[231] Ibid., 53.

[232] Ibid., 58.

[233] Shin-Kap Han, "The Other Side of Paul Revere: The Brokerage Role in the Making of the American Revolution," *Mobilization: An International Quarterly* 14, no. 2 (2009): 143.

[234] Ibid., 144.

the St. Andrews Lodge, the Loyal Nine, the Long Room Club, the Boston Committee of Correspondence, and several others. However, these organizations were only a loose alliance of groups. This lack of cohesion is what made Revere and Warren critical to the ultimate success of the American Revolution as they filled the roles of communicators, coordinators, and organizers between and amongst these various groups.[235] Thus, in examining the social media environment in a given country, it is imperative to seek out those online activists who appear to have wide-spread relationships and belong to several diverse groups. For example, if an individual writes his or her own blog, frequently comments on several other blogs, belongs to multiple Facebook groups, and has 500 or more Twitter followers, he or she may be a valuable person to seek out to assist in achieving U.S. objectives in a given situation.

L. PREVAILING NARRATIVES AND FRAMES

Whether engaged in planning an unconventional warfare campaign or planning for another type of warfare, understanding the competitive narratives in the target area is a key part of proper preparation for strategists at all levels of the military.[236] Narratives provide the overall context for the specific actions that each side in a competitive environment take. Before continuing this discussion, one clarifying comment must be provided. Despite some research literature that describes narratives and frames as distinct concepts,[237] for the purposes of this thesis, the terms narrative, frame, and story will be used interchangeably. With that caveat, the thesis will examine the advantages of identifying and utilizing insurgent narratives to support an unconventional warfare campaign.

First, insurgents have historically harnessed the power of narratives that evoke exodus and redemption because they are powerful at motivating people into collective

---

[235] Han, "The Other Side," 150.

[236] The Open Source Center and Monitor 360 provide in-depth master narrative reports. An example for Syria can be found at http://publicintelligence.net/osc-syria-master-narratives/.

[237] Francesca Polletta, "Contending Stories: Narrative in Social Movements," *Qualitative Sociology* 21, no. 4 (1998): 421.

action.[238] When used effectively, these types of narratives can be used to create a sense of injustice, identity, and collective efficacy.[239] Second, narratives can be used at a strategic level to strengthen a collective identity and may also facilitate the development of a coherent community, nation, or collective actor.[240] In periods of extreme turmoil such as in times of insurgent warfare, narratives can help maintain stability of the entire group. Finally, narratives provide shared meaning for the members of a resistance movement.[241]

Narratives work in a variety of ways. First, they provide a link between the collective identity of a network and the target an individual's personal experiences, interests, and beliefs.[242] They also reconfigure past events, add meaning and continuity to the present, and provide a vision of what the future will hold.[243] Narratives communicate, explain, and persuade people to accept a specific perspective as to what happened and why it happened.[244] Finally, narratives assign meaning to and interpret relevant events and conditions in order to win bystander support and the mobilization of antagonists.[245]

Ultimately, a narrative should be designed to motivate others to participate in collective action that aims to achieve the insurgent's desired end-state. This is accomplished by appealing to a target audience's intellect, emotion, and imagination.[246] Successful mobilization efforts often depend on how well a narrative resonates with the local populace. This is a critical point because at the end of the day, a successful UW

---

[238] Polletta, "Contending Stories," 419.

[239] Ibid., 421.

[240] Ibid., 422.

[241] Joseph Davis, *Stories of Change: Narrative and Social Movements* (Albany: State University of New York Press, 2002), 19.

[242] Ibid., 7–9.

[243] Ibid., 12.

[244] Ibid., 12.

[245] David Snow and Robert Benford, "Ideology, Frame Resonance, and Participant Mobilization," *International Social Movement Research* 1 (1988): 198.

[246] Davis, *Stories of Change*, 19.

campaign involves getting large numbers of indigenous people to take up arms against their own government. Narratives can help motivate people to take up arms.

In examining narratives in more detail, it is found that there are generally three types.[247] The first type is labeled as stories of origin. Stories of origin use phrases like "being born" or "I was blind, but saw the true light." These narratives explain why a group came together for a common purpose. The second are called stories of defeat and are designed to explain hardships. Having narratives that adequately explain a potential setback or defeat is important for sustaining a movement in the face of difficulty. This is certainly the case in executing UW, as it is extremely challenging to battle an entrenched regime. These stories should blame anyone but the group itself (or the group's leadership) for failures. Finally, there are stories of victory. Stories of victory are strategic in nature and are designed to entrench the group into the formal political process.[248] These narratives are especially important in the latter phases of a UW campaign including phase six, employment, and phase seven, transition.

In summary, narratives should provide three things: "a diagnosis of some event or aspect of social life as problematic and in need of alteration, a proposed solution to the diagnosed problem that specifies what needs to be done, and a call to arms or rationale for engaging in ameliorative or corrective action."[249] All things equal, the more robust and developed a movement is in executing these three core tasks, the more successful the mobilization effort will be. So the importance of incorporating narratives into one's planned use of social media technology to support a UW campaign cannot be overstated. Social media allows for rapid and robust communication and distribution of narratives. Unlike any other communications vehicle, social media allows a given entity to spread narrative messaging almost instantly to a world-wide audience. Marrying narratives and

---

[247] Snow and Benford, 1988, provide an alternate way to categorize frames: diagnostic, prognostic, and motivational. Diagnostic frames identify a problem and assign blame for the problem. Prognostic frames suggest solutions to problems and identifies strategies, tactics, and specific targets. Motivational frames are basically calls to arms.

[248] Polletta, "Contending Stories," 426–434.

[249] Snow and Benford, "Ideology and Participant Mobilization," 199.

social media provides the opportunity to capitalize on emerging events in almost real time. For example, an insurgent group could use a narrative designed to communicate that a regime's security force is comprised of thugs who indiscriminately target innocent civilians. Then, if the insurgents can evoke overreactions from regime security forces, capture the brutality on video, and post the video to YouTube in a matter of seconds, it has effectively used social media to communicate and rapidly disseminate this narrative.

The second part of this chapter will provide a general menu of options for which social media can be used in support of UW. This section will also highlight the conditions under which social media should not be used. The options are broken down into two categories: mobile phone-based social media and Internet-based social media. Each of these broad categories has a set of three identical options: information operations, passive mobilization, and active mobilization. This information is summarized in Table 10.

M. SOCIAL MEDIA OPTIONS

Social Media Options	Examples
Mobile Information Operations	Narrative, Propaganda, PSYOPS
Mobile Passive Mobilization	Recruiting, Spreading Information
Mobile Active Mobilization	Protests, Demonstrations, Attacks
Internet Information Operations	Narrative, Propaganda, PSYOPS
Internet Passive Mobilization	Recruiting, Spreading Information
Internet Active Mobilization	Protests, Demonstrations, Attacks

Table 10. Summary of Options for Using Social Media in an UW Environment

It is important to note that the social media options and suggestions provided in this chapter are not meant to establish limits or hard and fast rules in terms of how social media are or are not ultimately utilized in support of an UW campaign. Additionally, the options provided are not all inclusive. As the case studies in Chapter III demonstrated, social media's use in times of conflict are varied and dynamic. With social media, like other weapons platforms, there are no simple flow charts that can be read to determine the best use of social media in every situation. The following information and suggestions are meant to provide an organizational framework from which planners can glean general guidelines and concepts. The intent is to provide some foundational information from

which specific strategies in the utilization of social media in support of UW can be derived. Additionally, the three primary uses outlined below are presented in order from the option that presents the least risk to personnel (versus risk to mission) to the option that presents the greatest risk to personnel.

1. Information Operations

U.S. Special Forces (SF) soldiers are specifically selected and trained to conduct UW. In fact, SF is the only unit specifically designed to conduct UW.[250] As such, SF is the principal elements in conducting a UW campaign. However, other elements including Military Information Support Operations (MISO) forces, Civil Affairs (CA), and U.S. interagency entities also play an important role in the execution of UW. In examining the role that MISO plays in support of a UW mission, five key tasks emerge from UW doctrine. These information operations tasks are as follows. First, determine key psychological factors in the operational environment. Second, provide training and advisory assistance to insurgent leaders and units on the development, organization, and employment of resistance information capabilities. Third, identify actions with psychological effects that can create, change, or reinforce desired behaviors in identified target groups or individuals. Fourth, shape popular perceptions to support UW objectives. Finally, counter enemy misinformation and disinformation that can undermine the UW mission.[251] There are a number of specific ways that social media can be used to support information operations.

a. Information Dissemination

One macro political factor that has been linked to sudden collective actions is the pointing out of suddenly imposed grievances.[252] This is one of a number of

---

[250] Department of the Army, *Training Circular 18-01, Special Forces Unconventional Warfare*, (Washington, DC: Department of the Army, 2010), 1–9.

[251] Ibid., 1–10.

[252] Edward Walsh,"Resource Mobilization and Citizen Protest in Communities Around the Three Mile Island," *Social Problems* 29, no. 1(1981), as quoted by Doug McAdams, "Micromobilization Contexts and Recruitment to Activism," *International Social Movement Research* 1(1988): 131.

factors that can provide the structural potential for political action.[253] Between opportunity and action are people with perceived subjective meanings they assign to their particular situation. So, for example, simply spreading information about a regime-imposed grievance does not necessarily lead to mobilization, but if done in the correct manner, simply providing evidence of what a particular regime is doing can provide a spark that leads to revolution activity. An example of how social media can be used as a tool of information operations in support of a growing insurgency can be found in one specific event that occurred during the contentious Iranian presidential elections of 2009.

Neda Agha-Soltan was planning to join the protests in Tehran over the perceived corruption in the 2009 Iranian presidential elections.[254] As she was standing near a crowd observing what was going on around her, she was shot in her chest. Reportedly, the shot came from a member of the pro-Iranian militia group Basij.[255] While Neda was lying on the ground fighting for her life, several individuals, including her father tried desperately to revive her. As these events were unfolding, an Iranian citizen started to film Neda's struggle using a mobile phone. A still image from the video is shown in Figure 12.

[253] McAdam, "Micromobilization Contexts," 132.

[254] Thomas Mayfield, "A Commander's Strategy for Social Media," National Defense University, http://www.ndu.edu/press/commanders-strategy-social-media.html (accessed May 3, 2013).

[255] Ibid.

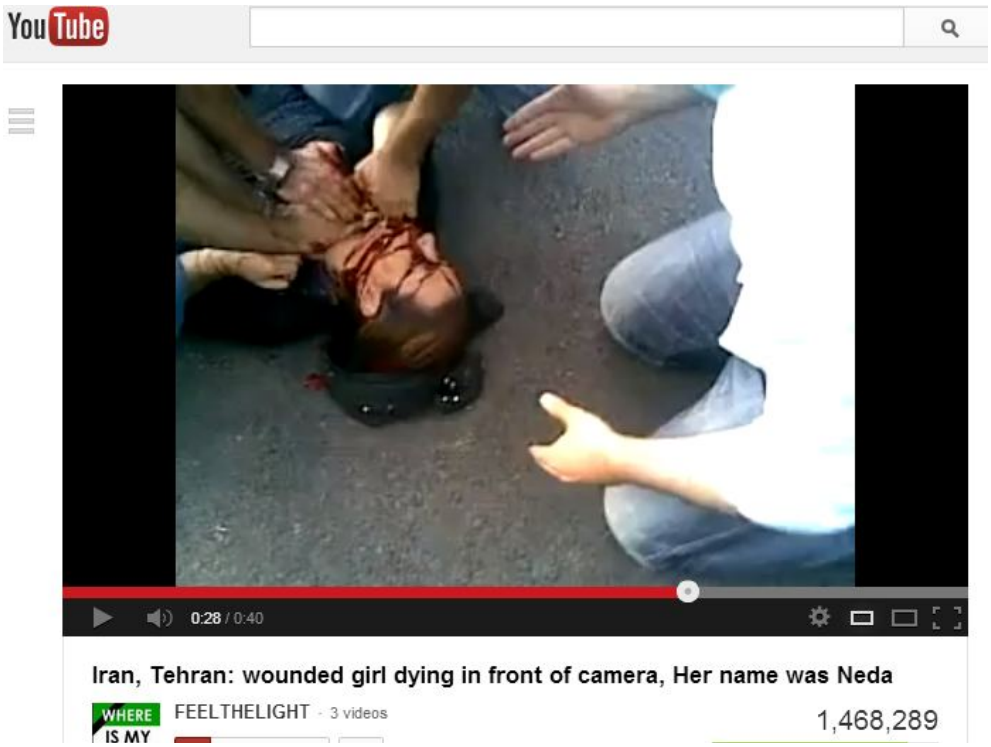

Figure 12. Neda Agha-Soltan, A Protestor of the 2009 Iranian Presidential Elections[256]

The video was quickly posted to YouTube and spread virally around the globe through the use of social media platforms. This video clearly showed a suddenly imposed grievance by a repressive Iranian regime. The video's rapid dissemination led to more intense protesting over the next 10 days in Tehran as Iranian students used Twitter, Facebook, and Flickr to spread information about the next series of protests.[257]

The key take-away from this discussion in terms of planning and executing a UW campaign is that operators must be prepared at all times for an information operation opportunity. For example, if those involved in an insurgent movement have a pre-planned action (such as a small protest) that is intended to provoke an overreaction from a local security force, then the leaders of the movement must place assets in a position to capture the incident. This means that before any planned insurgent

[256] FEELTHELIGHT, "Iran, Tehran: Wounded Girl Dying in Front of Camera, Her Name was Neda," YouTube, http://www.youtube.com/watch?v=bbdEf0QRsLM (accessed May 14, 2013).

[257] Mayfield, "A Commander's Strategy."

action is executed, the movement must have video cameras and other recording devices in position ahead of the planned action so that they are prepared to capture the missteps of the ruling regime and exploit those actions by using social media to spread the captured incident. A second specific way to think about using social media to engage in information operations is through the deliberate spread of narratives. The following section builds on the previous discussion of narratives and provides a specific example of how one group uses mobile phones to spread their narrative in Africa.

b. Narrative

The overall aim in spreading a narrative is to achieve a "significant transformation in the collective consciousness of the actors involved."[258] This transformation, or cognitive liberation, and the resulting actions that stem from the change is the result of accomplishing three things. First, the regime's political system must lose legitimacy. Large numbers of men and women must come to view certain aspects of the institutional arrangements that they are subjected to as unjust and wrong. Second, citizens who normally believe their current situation is inevitable need to begin to assert themselves and demand certain rights. Third, people must begin to feel empowered, that they are no longer helpless, and that they can affect their current situation.[259]

It is important to note, however, that the absence of any one of these three factors, or the lack of a large portion of the population experiencing this cognitive liberation, can stifle an insurgency.[260] This is where the power of social media as a communications tool can be especially effective in supporting a UW campaign. Social media can, like no other communications medium, reach an enormous audience in an almost instantaneous manner and can do so in a constant and repetitive manner.

---

[258] William Gameson, Bruce Fireman, and Steve Rytina, *Encounters with Unjust Authority* (Homewood, Ill: Dorsey Press, 1982), as quoted in Doug McAdam, "Micromobilization Contexts and Recruitment to Activism," *International Social Movement Research* 1 (1988): 132.

[259] Frances Piven and Richard Cloward, *Poor People's Movements: Why They Succeed, How They Fail* (New York: Vintage Books, 1979), 3-4.

[260] McAdam, "Micromobilization Contexts," 133.

Additionally, social media technology has the potential to give this reach to almost anyone with an Internet connection. Thus, social media can be used to spread powerful narratives in a short amount of time which then act as cognitive cues. These cognitive cues are the signals sent to an insurgent group indicating that the current political regime is vulnerable to being overthrown.[261]

Another consideration is to look at ways to use social media to influence the three primary factors that form the calculus that most individuals use to determine whether or not they will actually participate in collective action. These three sets of expectations are:

1. Expectations about the number of participants;
2. Expectations about one's own contribution to the probability of success;
3. Expectations about the probability of success if many people participate.[262]

Social media platforms are good at magnifying the perceived level of participation. Thus, if social media can be used to show individuals that "everyone is participating" in a given insurgent movement, it is more likely that more individuals will join the movement. In particular, social media allows people to connect and form weak social ties. This is an important point because research indicates that weak social ties are especially effective serving as diffusion channels for information.[263] An example from the website irevolutions.net will demonstrate one group's use of mobile phone-based social media to spread a narrative.

In its recent past, ethnically based violence has been the hallmark of Kenya's political scene. Even remote places like the Rift Valley have witnessed horrific

[261] McAdam, "Micromobilization Contexts," 133.

[262] Bert Klandermans, "Mobilization and Participation: Social-Psychological Expansions of Resource Mobilization Theory," *American Sociological Review* 42 (1984): 585.

[263] Granovetter, "Strength of Weak Ties," 1360–1380.

violence because of prejudices and poisonous feelings that surround political elections.[264] One network that is using social media to spread a narrative to counter this on-going violence is PeaceTXT. PeaceTXT uses mobile phone technology to send out social narratives urging an end to ethnic violence. Empirical research has already shown that repetitive SMS messages can change behaviors.[265] Researchers believe that repetitive narrative messaging can always change people's behaviors as they relate to periods of conflict.[266]

2. Passive Mobilization[267]

The second overarching way of using social media to support the conduct of UW is through passive mobilization. Passive mobilization involves bringing people to see a particular issue or situation in a specific way that aligns with the point of view or objective of a given movement. There are several ways in which to use social media for passive mobilization in support of UW. Two basic means are through recruitment and social media activism.

a. Recruitment

Social media has the potential to bring large numbers of people together in a short period of time. By reaching out to a few dozen individuals who are active on social media sites like Facebook, Twitter, and various blog sites it is possible to have

---

[264] Jeffery Gettleman, "On Eve of Vote, Fragile Valley in Kenta Faces New Divisions," *The New York Times*, March 2, 2013, http://www.nytimes.com/2013/03/03/world/africa/on-eve-of-vote-fragile-valley-in-kenya-faces-new-divisions.html?ref=todayspaper&_r=0 (accessed May 17, 2013).

[265] C. Pop-Eleches et al., "Mobile Phone Technologies Improve Adherence to Antiretroviral Treatment in a Resource-Limited Setting: A Randomized Controlled Trial of Text Message Reminders," The National Center for Biotechnology Information (NCBI), https://www.ncbi.nlm.nih.gov/pubmed/21252632 (accessed May 17, 2013).

[266] Patrick Meier, "PeaceTXT Kenya: Since Wars Begin in Minds of Men," iRevoluition.net, http://irevolution.net/tag/sms/ (accessed May 17, 2013).

[267] Social movement literature refers to passive mobilization as consensus mobilization. Consensus mobilization involves a social movement's efforts to develop support for its points of view and goals. David Snow, E. Rochford, Jr., Steven Worder, and Robert Benford, "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review* 51, no.2 (1986):466. For more details see John McCarthy and Mayer Zald, "Resource Mobilization and Social Movements: A Partial Theory." *American Journal of Sociology* 82 (1977): 1212–41.

those individuals join a resistance movement. If each of those individuals have several hundred or several thousand electronically linked people that they reach out to, it is not hard to envision how quickly a network of people can grow to number tens of thousands. In fact, tapping into existing social networks (such as student unions, labor unions, clubs and other civic organizations) is the most effective way to build a large social movement.

Research indicates that it is much more effective to recruit large "blocks" of people into a given cause versus trying to recruit individuals. Thus, effective movements are those that can recruit established networks of people, not isolated individuals.[268] Additionally, people with strong interpersonal links to each other are less likely to feel powerless to change their current situation. This is because people who are isolated socially are more likely to explain their lot in life as a function of their individual circumstances instead of more broad situational factors.[269] Social media technology can help recruit individuals into a cause, that they might otherwise not join, by providing an environment in which to develop relationships with other people and thus break the feeling of isolation. Another important note is that it is important to target the right type of person in recruiting efforts.

Motivating people to take action is much easier if the right people are recruited. One characteristic of an ideal recruit is a person who is involved in several collective settings (a college student who is in the student government, in a fraternity, and plays on the rugby team).[270] Social media not only helps identify these ideal recruits, but is, in and of itself, another potential collective setting for someone to be a part of, which furthers the likelihood of that person taking an active role in support of a resistance movement. A good example of using social media to recruit large numbers of individuals into a collective movement can be found during the revolutionary protests that occurred in Egypt during the Arab Spring.

---

[268] McAdam, "Micromobilization Contexts," 142.

[269] Ibid., 137.

[270] Ibid., 138.

The April 6 Youth Movement was started on March 23, 2008 when a group of Egyptian activists started a Facebook page. The page was used to help rally support for a textile workers' strike in the city of Mahalla. The textile workers were planning to strike in protest of low hourly wages and increasingly high food prices.[271] One of the group's founders was a young woman named Asmaa Mahfouz. Over the next several years the April 6 Youth Movement grew in size and in its political goals. Eventually, the movement joined other like-minded networks for the common cause of ousting Egyptian President Hosni Mubarak. Several days before the famous January 25 protest in Tahrir Square, Asmaa and several other members of the April 6 Youth Movement tried to rally support for a protest in downtown Cairo. The turn-out was abysmal. Rather than stop her efforts, Asmaa turned to social media to recruit others to her cause.

Originally posted on Facebook, Asmaa made a four minute video explaining the grievances that she and others had experienced and explained that four people had recently immolated themselves in protest, yet no one was doing anything about it. She then challenged Egyptian men to follow her lead by joining her protest movement and encouraged them to invite their entire social network to do the same. Figure 13 is a still shot of the video that went viral on Facebook and YouTube. The English translation is at the bottom of the picture.

[271] PBS, "April 6th Youth Movement."

Figure 13. Asmaa Mahfouz Recruiting Video Posted on YouTube Prior to the January 25 Protests in Egypt[272]

Ultimately, Asmaa's recruiting efforts were successful, as the video was viewed by over a million people and motivated thousands to join the protests that eventually led to regime change in Egypt. This is one example of the many ways in which a practitioner of UW could use social media to recruit others to join resistance efforts. Engaging others through blogs, Twitter, SMS messaging, and other social media platforms provides other mechanisms that operators can use to screen and recruit indigenous personnel to join their movement. A second social media-based passive mobilization task involves motivating others to take action themselves on social media platforms.

[272] Lyad El-Baghdadi, "Meet Asmaa Mahfouz and the Vlog that Helped Spark the Revolution," YouTube, http://www.youtube.com/watch?v=SgjIgMdsEuk (accessed May 17, 2013).

b. Social Media Activism

For an UW campaign to succeed eventually, indigenous people must take up arms in revolt against their government. Getting individuals to take to the streets to oppose a repressive regime is not an easy task. As a first step in this direction, military planners and leaders should consider working to get network members to take an active role in support of the movement. Examples of using social media for passive mobilization include writing blog posts or commentary on a Facebook page, posting photos or videos on a video sharing website, forwarding emails or SMS messages, translating Internet content from a native language to English or another target language, or editing videos. The Egyptian revolution during the Arab Spring provides a good example of a movement leader passively mobilizing his network.

In June 2010, Wael Ghonim was working at Google as the head of marketing for the Middle East and North Africa. While browsing his Facebook page, Wael noticed that a friend had posted a shocking photo on his Facebook wall. The picture was of a young male with a disfigured face. After some investigating, Wael found out the man's name was Khaled Mohamed Said and that he was reportedly killed by a brutal beating sustained at the hands of two secret police officers in Alexandria.[273] Outraged and tired of the police brutality, Wael designed a Facebook page to expose the corruption that had plagued the Ministry of Interior for years.

Using the page title "We Are All Khaled Said," Wael decided to administer the page anonymously. After creating the page, Wael made his first post, which said, "Today they killed Khaled. If I don't act for his sake, tomorrow they will kill me."[274] Within two minutes the page had 300 followers. Wael continued to post to the page and the number of members in his newly created network exploded. As the page continued to grow, Wael realized he needed his network to take an active role in helping his cause. To get his members to take action, Wael started asking for assistance. The first several members to help Wael were engaged in passive mobilization.

---

[273] Ghonim, *Revolution 2.0*, 58.

[274] Ibid., 60.

One of the first to respond to Wael's call for assistance came from Mohamed Ibrahuim, an Egyptian living in the United Kingdom. Mohamed expressed interest in translating the content from the Khaled Said page, and asked Wael if he could start an English version of Wael's page. Wael immediately agreed and the English Facebook page was created. The page received immediate attention and helped spread the narrative that was beginning to play out in Egypt.[275] A second volunteer, Khaled Kamel, responded to Wael and said he would do video editing for the website. Khaled took the best parts of various videos, edited them together and set them to music.[276] The video "mash-ups" were a powerful motivating tool. Although mobilizing a network on the Internet or through mobile platforms is not as powerful as getting members to take physical actions in their environment, it is a positive step in developing an effective resistance movement. Getting people to take actions online gives them a sense of belonging and that their actions matter to the movement. Such UW practitioners should consider this intermediate step as a step towards their ultimate goals. This leads to the final and most important option in terms of using social media to support an UW campaign, active mobilization.

N. ACTIVE MOBILIZATION[277]

Active mobilization is the most difficult, yet crucial use of social media in terms of maximizing this technology's potential to support the execution of UW. Active mobilization is the process of getting existing network members to take physical actions on behalf of a movement's goals and desired end-state. Although it may not be feasible or advisable for every situation, active mobilization represents the pinnacle of the potential use of social media to support a UW mission.

---

[275] Ghonim, *Revolution 2.0*, 93.

[276] Ibid., 102.

[277] Social movement literature refers to active mobilization as action mobilization. Action mobilization "involves the activation of individuals who already support movement goals and activities." Snow et al., "Frame Alignment Processes, 466. For more details see McCarthy and Zald, "Resource Mobilization and Social Movements, 1212–41.

Viewed holistically, active mobilization really encompasses and adds to the first two uses of social media, information operations and passive mobilization. In actuality, if a resistance movement is able to actively mobilize network members through social media, the group should also be continually using social media for information operations as well as passive mobilization. All three tasks can be done simultaneously and continuously under the right conditions and circumstances.

The most obvious example of using social media for active mobilization involves the coordination and organization of a physical protest. The activists involved in the Arab Spring used social media to coordinate times, locations, and rules of conduct while protesting. They also used social media to disseminate location of security forces and areas to avoid. Other examples could be to coordinate strikes, walkouts, flash mobs, boycotts, acts of sabotage, etc. In Iran, students used the photo sharing site Flickr to communicate to fellow protestors the locations of the next round of protests, as well as which areas to avoid because of the presence of large numbers of security force personnel.[278] A more robust example can be found by returning to examine Wael Ghonim's Facebook-initiated insurgency. His actions provide a complete example of how social media can be used in each of the aforementioned ways.

Initially, Wael Ghonim's goal in creating his now famous Facebook page was to bring awareness to the police brutality that was far too common in Egypt (information operations). After experiencing some initial success, Wael's ambition for his movement grew and so did his plan of execution. To achieve his ultimate goal of active mobilization, Wael developed a four phased plan built around the "sales tunnel" approach to marketing.[279] The first phase was designed simply to get people in his network joining the Facebook page and reading the page's content (passive mobilization - recruiting). The second phase was to convince his network participants to interact with other network members by "liking" and "commenting" on the information that was being posted to the

[278] United For Iran, "16 Azar Green Routes," Flickr, http://www.flickr.com/photos/united4iran/4165827330/ (accessed May 18, 2013).

[279] Ghonim, *Revolution 2.0*, 67.

page. The third phase involved having members participate in the page's online campaigns, and begin to upload and post content to the page themselves (passive mobilization—social media activism). The fourth and most important phase was to motivate network members to take action by protesting the Mubarak regime in the streets (active mobilization).[280] Wael realized that getting the network to take action on the ground was the key to raising the level of interaction among network members and to actually have a chance of overthrowing the Mubarak regime. This interaction was vital for the sustainability of the network because it increased the connectivity of the network and built stronger social ties among the various members.[281] Now that the three primary ways to use social media to support UW have been discussed, situations in which using social media may not be the most appropriate option in terms of building, communicating, and directing a network in the context of UW will be considered.

O. DEFICIENT SOCIAL MEDIA CONDITIONS

There are two general ways of determining when it may not be appropriate to use social media to support a UW campaign. The first method is to go through the twelve factors described above in the social media assessment methodology. At the end of that assessment. if it is determined that the opposition government in question has effective social media censorship and surveillance capabilities, has the ability to shut down or significantly slow down Internet and mobile phone connectivity, and has an enforcement mechanism with a range of influence that extends to all borders, then using social media to support a resistance movement will most likely be counter-productive. Currently, the Chinese regime presents a challenging social media environment where the government's capabilities and resource advantages likely outweigh the potential that social media technology would bring to a movement's efforts. However, that is not to say that social media cannot be used in a deceptive manner or as a tool of psychological operations. Additionally, Bluetooth connectivity on mobile devices may also offer opportunities to use social media in an extremely restrictive environment. So although the more

[280] Ghonim, *Revolution 2.0*, 67–68.

[281] Ibid., 84.

traditional uses of social media may not be appropriate in a country like China, creative planners may still find ways to utilize social media in this operational area. The second way of looking at the appropriateness of social media's use in the context of revolutionary warfare is by looking at the actions and visibility of the movement.

In her examination of social networks, researcher Florence Passy examined social networks by breaking them down as having two characteristics. The two characteristics were action repertoire (legal versus illegal types of operations) and the level of public visibility (high or low). Figure 14 illustrates this simple construct. The type of network to be built (clandestine or open) and the type of activites the network will be engaged in (legal or illegal) will determine whether social media should be used to support the movement. For example, social media should not be used to recurit people in cases where one is trying to create a small, low visibility, illegal activity-based network. This type of recruiting should be done in person, preferably by someone with personal ties to the potential recruit. Having personal ties reduces the risk a clandetine network takes when it makes initial contact with a recruit and asks him or her to join the group.[282] Additionally, social media should not be used when the organization in question wants to remain off the regime's radar, so to speak, especially if the network will be engaged in illegal activities and does not yet have the strength or resiliency to withstand constant repression from the government in power. Therefore, if the movement in question would fall categorially in the lower-left quadrant (low visibily, illegal), then social media would not be appropriate in supporting this effort.

[282] Donatella della Porta, "Recruitment Processes in Clandestine Political Organizations: Italian Left-Wing Terrorism," *International Social Movement Research* 1 (1988): 160.

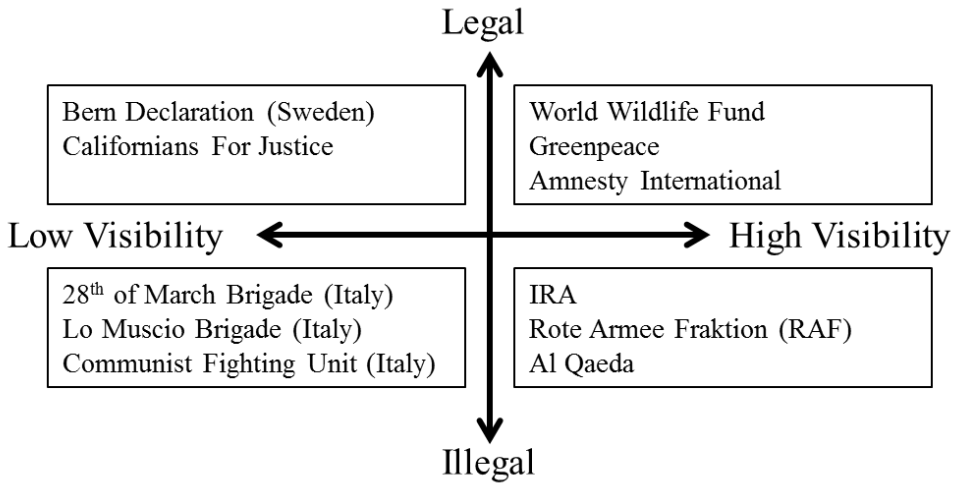

Figure 14. Organization of Social Movements Based on Legality and Visibility[283]

P. CONCLUSION

Doing a thorough analysis of the twelve factors in the social media assessment methodology will provide military planners the necessary information to determine how to most appropriately use social media technology in support of UW. Once this initial assessment is complete, the next step is to determine which basic platform to use: Internet-based social media, mobile phone-based social media, both in combination, or neither. After determining which platforms will best support the UW mission, the next step is to determine how to actually use the selected platforms. The three basic ways of social media in support of UW are information operations, passive mobilization, and active mobilization. After this step is complete, strategists are in a position to actually design a social media technology plan that would support the overall campaign plan. Finally, it is important to remember that social movements are developed as a response to an interplay between various movement groups themselves and the greater sociopolitical environment that the activists wish to improve. Additionally, because the opportunities

[283] Passy, "Social Networks Matter," 27–28.

(or lack of opportunities) for an insurgent group to engage in successful collective action varies significantly over time, it is important to remember that constant re-evaluation of the social media environment is necessary.[284]

Examples of the types of events that can cause these variances include war, industrialization, political realignments, defections, fractures among regime elites (especially between military and government leaders), extended unemployment, a natural disaster, and many others. So while using social media in a certain way at a given time may make sense, changing conditions may impact the way social media should be used going forward. The resistance elements in Iran found this out after using Facebook, Twitter, and various other social media platforms to protest the outcome of the 2009 presidential elections. Seeing the potential that these popular platforms provided insurgent elements, the Iranian government started blocking all major social media websites, including Facebook and Twitter. This situation explains why one of the assessment steps is to understand how information flows in the absence of communication technology.

[284] McAdam, *"Political Process,"* 40.

V. RECOMMENDATIONS AND CONCLUSION

A. INTRODUCTION

A headline from a 1987 edition of the *Los Angeles Times* read "Tape Recording: the Modern Medium of Dissent."[285] The article opened by stating that student demonstrators were advocating for democracy in China and free elections in Taiwan. The article then stated that "both events involved creative, effective use of technology to spread messages in ways that would have been impossible only a decade ago."[286] It continued to describe how inexpensive video recorders, tape recorders, and double-cassette decks allowed for the widespread dissemination of information, while at the same time making it difficult for repressive regime officials to eradicate these alternate sources of information. The two examples the article provided, which are now over two decades old, provide insight into both the history and potential that emerging technology brings to those that oppose oppression.

In Taiwan, members of the opposition party, the Democratic Progressive Party (DPP), used video cameras to capture government security forces beating up supporters of a dissident returning home through Taipei's Chiang Kai-Shek International Airport. Over the next several days, Taiwanese government-controlled television stations aired edited versions of the airport melee. The commentators used the doctored video to portray the opposition party as violence-prone individuals whose only intentions were to cause instability and disruption throughout Taiwan. However, because the opposition party had had their own cameras rolling during the fighting, they were able to provide a counter-narrative. They did this by duplicating the video over and over and distributing copies to their local political offices. These local offices then set up television monitors outside their offices and played the unedited videos on a continuous loop. Thousands of onlookers viewed the video and many seemed eager to view something other than the

[285] Jim Mann, "Tape Recording: the Modern Medium of Dissent," *The Los Angeles Times*, January 11, 1987, http://articles.latimes.com/1987-01-11/opinion/op-3795_1_democratic-progressive-party (accessed April 13, 2013).

[286] Ibid.

government's "official" version of the event.[287] After this incident, the DPP made a surprisingly strong showing at the polls and made gains in its overall level of popular support. During this same time period, Chinese students used even less sophisticated means to spread a counter-narrative.

Having grown frustrated by security forces' continual confiscation of their underground magazines and tearing down of opposition posters, groups of Chinese students turned to other means of communicating their anti-communist message: the tape recorder and double-cassette deck. The students would go out at night with flashlights and mini-recorders and make voice recordings of the messages written on pro-democracy posters. These same posters were being torn down each morning by local security forces. After recording the content of each poster, students would return quietly to their dorm rooms and begin copying the tapes in their double-cassette decks. The duplicated cassette tapes would then be passed around from room to room, campus to campus, and eventually city to city.[288] The Chinese students discovered that this form of information operations was much more difficult to stop or control because it was much tougher for security forces to listen to hours and hours of audio recordings compared to sifting through a stack of magazines or pamphlets.

The point in recounting these stories is to reinforce the idea that using current communication technology to disseminate information to oppose an oppressive regime is not a new phenomenon created by Facebook, YouTube, and Twitter. The insurgents in Tunisia, Libya, Egypt, Yemen, and elsewhere were not the first to use an emerging technology to help stop oppression. What is new, however, is the way in which current social media technology can hyper-accelerate the dissemination of information. A powerful narrative told through user-generated content has the potential to reach tens of millions of people in a few hours and to rally those same viewers into joining a movement. Those DPP leaders or the Chinese students would have taken much longer to have their messages reach one million people. Thus, social media exhibits a true

[287] Mann, "Tape Recording."

[288] Ibid.

demarcation point from all other previously discussed communications technology. Because of this vast potential, it is absolutely imperative for the U.S. military to make serious investments into using social media as a force multiplier in all future conflicts, especially in executing UW. The remainder of this chapter will provide recommendations for the authorities, in training and education, and in the doctrine needed to maximize the potential of social media in support of military operations.

B. RECOMMENDATIONS

1. Authority

Expanding the authorities surrounding the military's use of social media in executing UW may be the most difficult obstacle for the U.S SOF to overcome in terms of being able to successfully utilize social media in support of future UW campaigns. Two types of authorities are involved, legal and command.

a. Legal Authority

Generally speaking, the U.S. military has the legal authority to utilize social media technology in support of DoD objectives so long as foreign audiences are the target of the information operation. The most basic legal guideline comes in the form of the Smith-Mundt Act of 1948, which "prohibits domestic dissemination of information designed for foreign consumption, as a way to ban domestic propaganda. By policy and practice, the DoD adheres to Smith-Mundt restrictions on domestic propaganda."[289] Although this law appears rather straightforward, controversy still surrounds the U.S. military's use of social media because anything distributed through social media platforms has the potential to be accessed by U.S. citizens. As an example, U.S. Central Command's Operation Earnest Voice (OEV), which provides the U.S. military the ability to have one service member control multiple online personalities, created headlines by

[289] Department of the Army, *FM 3-53, Military Information Support Operations*, (Washington, DC: Department of the Army, 2013), Appendix 5.

accusing the U.S. military of using social media to run spy operations.[290] Despite the occasional negative headline, U.S. law provides the basic framework needed to operate effectively in the social media environment. Therefore, the most pressing area that needs to be addressed in order for the military to be able to effectively use social media in support of UW is command authority.

b. Command Authority

The approval chain for traditional military information support operations (MISO) programs can reach the highest levels of the U.S. government. The formal approval chain is depicted in Figure 15.

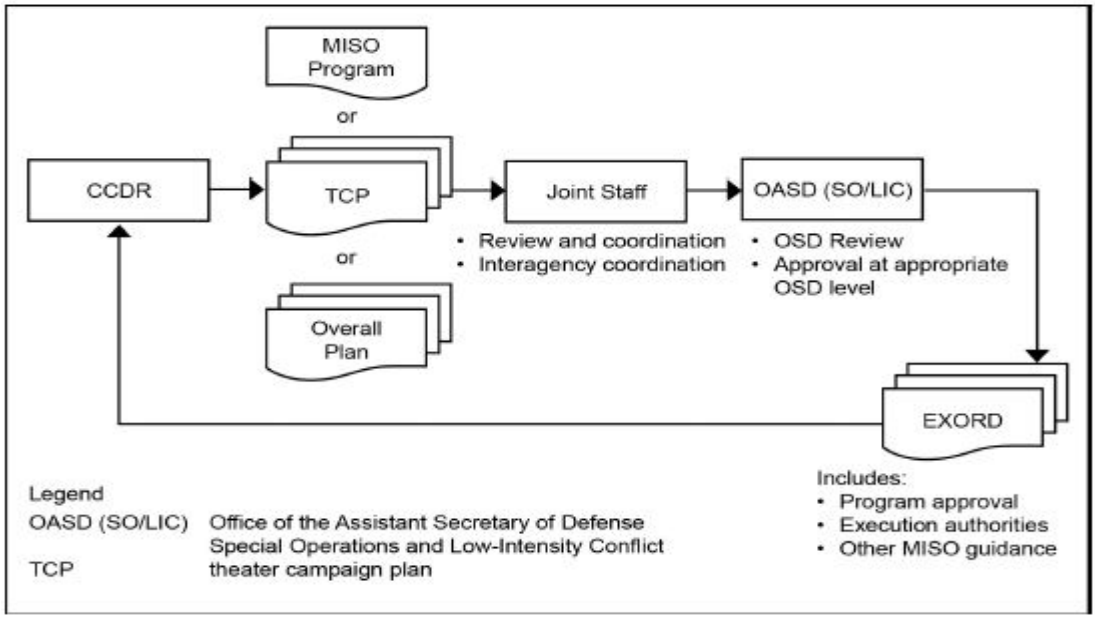

Figure 15. Military Information Support Operations Program Approval Chain[291]

This formal approval process may be sufficient for the generation and approval of MISO products when sufficient time allows for product development and dissemination. But in

[290] Nick Fielding and Ian Cobain, "Revealed: US Spy Operation that Manipulates Social Media," *The Guardian*, March 17, 2011, http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks (accessed May 10, 2013).

[291] Department of the Army, *FM 3-53*, 2–3.

fluid environments, where the adversary is not bound by any approval chains or timelines, the command authority to disseminate content on social media must be entrusted to lower level military commanders. Operation VALHALLA provides an example that crystallizes the need to streamline the MISO approval chain.

During a March 26, 2006 operation, U.S. Special Forces tracked down a group of Jaish al-Mahdi (JAM) insurgents who were responsible for the murders of Iraqi citizens and soldiers. After reaching the JAM stronghold, a firefight ensured that resulted in 16 or 17 JAM personnel killed. Additionally, a weapons cache was found, a tortured hostage was rescued, and another 16 JAM members were detained.[292] After the mission was completed, the U.S. Special Forces and Iraqi soldiers returned to their base. By all standards, this was a very successful operation for the combined force.

At the time, there was typically 24 to 48 hours between an event occurring and the insurgents posting propaganda on the Internet. However, after this particular incident, propaganda was populating the Internet in less than one hour.[293] Someone had moved the dead JAM bodies and removed the weapons that the JAM fighters had been using to engage the combined force. The bodies were arranged to appear as if they were shot while in prayer. Photographs depicting this new arrangement and a story accusing American soldiers of entering a mosque and killing unarmed men spread quickly around the Internet. Both American and Arab media outlets picked up on the story and began to report.[294]

When a story of this nature hits the U.S. press, the military's reaction is almost always to open an investigation. The Special Forces unit that conducted the operation was ordered to stand down, which meant they were no longer able to conduct combat operations. By aggressively and efficiently landing the first information operations punch, JAM not only bested the U.S. military from a strategic narrative

[292] Cori Dauber, "The Truth is Out There: Responding to Insurgent Disinformation and Deception Operations," *Military Review* 89, no. 1 (2009): 13–20.

[293] Ibid., 13.

[294] Ibid., 14.

perspective, but also gained freedom of maneuver as an effective combat force was taken out of the fight for almost one month.[295] But this situation did not have to unfold the way that it did.

The Special Forces operators had been accompanied by soldiers who were trained as combat cameramen. These specially trained soldiers record combat footage and are often embedded with tactical ground forces. In addition, several Operational Detachment—Alpha (ODA) members were wearing helmet cameras that provided additional footage of the operation. The videos captured during the operation provided clear contrasts between the JAM doctored photos and what actually occurred. Instead of the immediate chain of command (company and battalion level commanders) viewing the Special Forces footage and making a command decision to release it, the U.S. government sat on the information for three days. The briefing was finally delivered by then Secretary of Defense Donald Rumsfeld. Secretary Rumsfeld briefed from the exact same post-mission storyboards that were produced at the battalion level.[296]

By the time the truth was reported by the U.S. government, the strategic damage had been done. The inability to immediately react to the JAM account of the firefight by posting a counter-story was primarily caused by a cumbersome approval policy.[297] Operation VALHALLA demonstrated the dire need for trusting, empowering, and authorizing battalion level commanders to execute information operations through social media.

C. THE WAY AHEAD

One suggested way to move forward in terms of changing command authority is for centralized planning and decentralized execution.[298] This can be accomplished by having clear guidance issued from the Undersecretary of Defense for Policy (USD(P)),

---

[295] Dauber, "Responding to Insurgent Disinformation," 14.

[296] Ibid., 20.

[297] Mayfield III, "A Commander's Strategy," 82.

[298] Ibid., 82.

the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD[SO/LIC]), and Interagency/Intergovernmental Support (IIS). This guidance can then be refined down the military chain of command through the geographic combatant commander and the Department of State through the chief of mission. Armed with a clear set of information operation rules of engagement, commanders at the battalion level should then be given the command authority to release products through social media. In certain situations this authority may need to be extended down to the O-3 level. One example would be during the first four phases of UW. More specific to supporting UW, command authority for releasing information products also needs to include concurring host nation or partner nation or organization attribution, delayed attribution, and non-attribution.[299] These attribution methods will be more likely to be used in a UW campaign compared to immediate attribution.

Future UW proficiency will depend on these expanded command authorities.[300] Without the property authority, special operations forces will not be empowered to take the initiative when presented an opportunity to strike first with social media. In addition, SOF commanders at all levels have tasked ARSOF to improve their war-fighting capabilities in various ways. Specifically in the Commander's ARSOF 2022 strategic guidance, LTG Charles Cleveland enumerated his priorities into six categories.

Under category six, Optimize Resourcing and Commodity Areas, there is number 6G, MISO Systems. The challenge presented is that the proliferation of both Internet-based and mobile phone-based social media technology has presented unprecedented opportunities both for the enemy and ARSOF.[301] One of the potential short-term solutions presented is to develop innovative tactics, techniques, and procedures (TTPs) for utilizing social media in support of special warfare and surgical strike operations. However, the most robust, carefully crafted, and effective social media TTPs will have a significantly reduced level of effectiveness if the proper authorities are not in place to

[299] Department of the Army, *FM 3-53,* 2-4 and 2-5.

[300] Petit, "Social Media," 35.

[301] Charles Cleveland, "ARSOF 2022 Priorities," *Special Warfare* 26, no. 2 (2013): 27.

allow tactical level commanders the ability to use social media without a cumbersome and inefficient approval process. Additionally, the type of command authority described above provides one example of what is needed to achieve United States Special Operations Command's (USSOCOM) concept of enduring engagements that require small-footprint distributed operations.

According to the current USSOCOM Operating Concept, which provides the Commander's vision for the organization in 2020, enduring engagements require small, task-organized SOF teams empowered by mission command in areas where a large U.S. military presence is unacceptable.[302] Mission command refers to the idea that SOF elements require a decentralized style of command that allows for freedom and speed of action within a given set of limitations. This operating concept allows subordinate commanders to use their higher command's intent, their assigned mission, the desired effect to be achieved, and the reasons behind the mission. The tactical leader is then allowed the freedom of action and entrusted with the responsibility to determine how to best achieve mission success. Having the legal and command authorities to operate in the social media environment is the first part of empowering SOF operators to harness this technology. The next three components, education and training, doctrine, and funding are critical aspects of being able to fully realize the power of social media.

1. Training and Education

One of the key tenets of United States Special Operations Command's (USSOCOM) Operating Concept is to elevate SOF non-lethal skills to the same level of proficiency as lethal skills.[303] Developing proficiency in using social media to support SOF operations is an example of a much needed non-lethal skill. Training on using social media has already begun. Several Special Forces Groups (Airborne) have integrated social media utilization into major UW training exercises, and elements of First Special

[302] United States Special Operations Command, Special Operations Forces Operating Concept, http://fortunascorner.files.wordpress.com/2013/05/final-low-res-sof-operating-concept-may-2013.pdf (accessed May 20, 2013), 7.

[303] Ibid., ii.

Warfare Training Group (Airborne) have developed TTPs for integrating social media into UW training at the Special Forces Qualification Course. However, similar to marksmanship training on an assigned weapon system, basic standards of evaluation should be developed to ensure each SOF element has a similar baseline. Training with social media technology can be enhanced by introducing formal blocks of instruction on using social media into the educational courses offered by the U.S. Army John F. Kennedy Special Warfare Center and School (SWCS).

There are a number of specific courses in which social media technology and utilization should be taught. Introductory and basic concepts should be taught during the CA, PSYOP, and SF Qualification courses. Advanced training is appropriate in a number of courses including, but not limited to, the MISO ISO Unconventional Warfare Course, the MISO Advanced Planner's Course, the Special Forces Intelligence Sergeant Course (SFISC), the Special Forces Network Development Course (NDC), and the Unconventional Warfare Operational Design Course (UWODC). Part of the educational process should include real world experimentation. This would allow operators the opportunity to assess the effectiveness of their various social media operations. The next facet of incorporating social media into future SOF operations is to capture the lessons learned from training, education, and experience into formal doctrine.

2. Doctrine

Military doctrine bridges the gap between broad policy and tactical level TTPs. Doctrine provides the guiding principles necessary to conduct operations in accordance with approved, tested, and proven methods. Doctrine is authoritative on the subject matter covered, but it is not directive in nature. By adding social media utilization into military doctrine, SOF leaders can ensure that there is some universality in the quality of training and education that each SOF operator receives. Although the most creative and effective uses of social media may not come from those with a formalized doctrine background, it is important to establish guiding principles (strict adherence to the Smith-Mundt Act for example) that are commonly followed.

D. CONCLUSION

In examining the use of social media in support of military operations, particularly UW, it is important to keep in mind the laws of the countries in which the media will be used. As an example, the Vietnamese government recently imprisoned three bloggers for online posts that were critical of the government.[304] Additionally, it is good practice to ask whether a particular action carried out on social media is ethical or not. Careful legal and ethical considerations are critical for long-term, successful use of social media.[305] Acting in accordance with local laws and by an ethical code of conduct does not negate the need for military commanders to be pro-active and offensive in nature when using social media.

A commander who develops an aggressive social media engagement strategy can win the information and narrative fight. Ignoring social media is not an option.[306] The U.S. military can look to the lessons the Israeli military learned from losing the narrative battle on social media to Hezbollah in the second Lebanon War in 2006 and how the Israelis had social media utilization right two years later when they attacked the Gaza Strip in December 2008 and January 2009.[307] Finally, as Brian Petit stated, "the future study, practice and successful execution of future UW must deliberately incorporate and account for the highly public sphere of social media. For U.S. SF engaging in UW, the effective use of social media and the use of handheld technologies is perhaps less about technology training and more about mindset shifts in how we view the boundaries of UW."[308] This change is required from leaders at all levels and must occur sooner rather than later because of the overwhelming potential that social media represents in shaping the outcome of future military operations.

---

[304] James Hookway, "Vietnam Convicts 3 Bloggers over Posts," *The Wall Street Journal*, September 24, 2012, http://online.wsj.com/article/SB10000872396390444358804578015383720801250.html (accessed April 12, 2013).

[305] Gupta and Brooks, *Using Social Media*, 374.

[306] Mayfield III, "A Commander's Strategy," 80.

[307] Ibid., 80.

[308] Petit, "Social Media," 37.

Returning to the article from the *Los Angeles Times* that was used in the introduction of this chapter, author Jim Mann wrote the following:

> Home-made videotapes of demonstrations and audio recordings of wall posters barely begin to exhaust the possibilities for dissent raised by the new consumer technologies. What happens when personal computers are so prevalent that students can call, at a few moments' notice, for nationwide demonstrations or labor leaders for a general strike? Or when some computer-savvy firebrand can send out the word along his network: "Workers of the world, unite! You have nothing to lose but your software"?

The answer to both of Mr. Mann's questions is quite simple: the Arab Spring.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Al Jazeera English. "Empire." Accessed January 9, 2013. http://www.aljazeera.com/programmes/empire/2011/02/201121614532116986.html.

Anheier, Helmut. "Movement Development and Organizational Networks: The Role of 'Single Members' in the German Nazi Party, 1925–30." In *Social Movements and Networks*, edited by Mario Diani and Doug McAdam, 49–76. New York: Oxford University Press, 2003.

Anklam, Patti. *Net Work: A Practical Guide to Creating and Sustaining Networks at Work and in the World*. Oxford: Buttersworth-Heinemann, 2007.

Arquilla, John. "How to Defeat Cyber Jihad." *Foreign Policy*, April 29, 2013. Accessed May 5, 2013. http://www.foreignpolicy.com/articles/2013/04/29/how_to_defeat_cyber_jihad

Baron, Adam. "Yemen's 'Death to America' Rebels Bring Calm to Northern Yemen." *The Christian Science Monitor*, October 28, 2012. Accessed March 12, 2013. http://www.csmonitor.com/World/Middle-East/2012/1028/Yemen-s-Death-to-America-rebels-bring-calm-to-northern-Yemen.

BBC News Staff. "Burma Leaders Double Fuel Prices." The BBC. Accessed February 15, 2103. http://news.bbc.co.uk/2/hi/asia-pacific/6947251.stm.

Bernstein, Carl. "Empire-Social Networks, Social Revolution: Interview with Marwan Bishara." By Marwan Bishara. IITrends. Accessed November 12, 2012. http://www.iitrends.com/2011/03/video-social-networks-social-revolution.html.

Blankstein, Andrew. "Tagger Used YouTube, and the Police Watched." *The Los Angeles Times*, May 28, 2008. Accessed September 2, 2012. http://articles.latimes.com/2008/may/28/local/me-buket28.

Buhaug, Halvard. "Dude, Where's My Conflict? LSG, Relative Strength, and the Location of Civil war." *Conflict Management and Peace Science* 27. No. 2 (2010): 107–128.

Burleigh, Marc. "Iran to Crack Down on Web Censor-Beating Software." *Google News*, June 10, 2012. Accessed September 5, 2012. http://www.google.com/hostednews/afp/article/ALeqM5jIFi-LdqBsdtrj7mRYnCMTlSGjCA?docId=CNG.f710ad6e0ee1dc52f64c985918d1bac1.741.

Central Intelligence Agency. “Country Comparison: Telephones – Mobile Cellular.” Accessed February 17, 2013. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2151rank.html.

Charles-Iyoha, Cristiana. “Mobile Telephony: Closing the Gap.” In *SMS Uprising: Mobile Activism in Africa*, edited by Sokari Ekine, 116–123. Oxford: Pambazuka Press, 2010.

Cleveland, Charles. “ARSOF 2022 Priorities.” *Special Warfare* 26. No. 2 (2013): 18–28.

CNET Staff. “Creepy: CNET Editor’s Review.” CNET.com. Accessed May 21, 2013. http://download.cnet.com/Creepy/3000–12941_4–75445808.html.

Counts, Andrew. “Minority Report is Real: FBI Wants to Use Social Networks to Prevent Future Crime.” Digitaltrends, January 26, 2012. Accessed September 4, 2012. http://www.digitaltrends.com/social-media/minority-report-is-real-fbi-wants-to-use-social-networks-to-prevent-future-crime.

Cullum, Brannon. “People Power II in the Philippines.” Movements.org, June 25, 2010. Accessed November 10, 2012. http://www.movements.org/case-study/entry/people-power-ii-in-the-philippines/.

Dauber, Cori. “The Truth is Out There: Responding to Insurgent Disinformation and Deception Operations.” *Military Review* 89. No. 1 (2009): 13–24.

Davis, Joseph. *Stories of Change: Narrative and Social Movements*. Albany: State University of New York Press, 2002.

Deceglie, Anthony. “Taliban Using Facebook to Lure Aussie Soldier.” *The Sunday Telegraph*, September 9, 2012. Accessed September 9, 2012. http://www.news.com.au/national/taliban-using-facebook-to-lure-aussie-soldier/story-fndo4bst-1226468094586.

Deibert, Ronald, Ethan Zuckerman, Roger Dingledine, Nart Villeneive, Steven Murdoch, Ross Anderson, Freerk Ohling, Hal Roberts, Ethan Zuckerman, Julian York, Robert Faris, and John Palfrey. “Circumvention Tools.” Accessed February 11, 2013. http://howtobypassinternetcensorship.org/files/bypassing-censorship.pdf.

Della Porta, Donatella. “Recruitment Processes in Clandestine Political Organizations: Italian Left-Wing Terrorism.” *International Social Movement Research* 1 (1988): 155–167.

Denning, Dorothy. “Cyber Surveillance.” Lecture presented at the Naval Postgraduate School, Monterey, CA, January 13, 2013.

Department of the Army. *Field Manual 3–18, Special Forces Operations*. Washington, D.C.: Department of the Army, 2012.

———. *FM 3–53, Military Information Support Operations*. Washington, D.C.: Department of the Army, 2013.

———. *Training Circular 18–01, Special Forces Unconventional Warfare*. Washington, D.C.: Department of the Army, 2010.

———. *Army Doctrine Publication 3–05, Special Operations*. Washington, DC: Department of the Army, 2012. Accessed March 12, 2013. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp3_05.pdf.

———. *Army Field Manual 3–21.8, The Infantry Rifle Platoon and Squad*. Washington, DC: Department of the Army, 2008. Accessed March 12. 2013. https://rdl.train.army.mil/catalog/view/100.ATSC/04183AF4–34EB-47F0-BCEE-29C93432DA49–1274564010088/3–21.8/toc.htm .

The Economist. "Monitoring the Monitors." *The Economist*, July 10, 2012. Accessed November 20, 2012. http://www.economist.com/blogs/analects/2012/07/online-censorship.

———. "Wired, at Last." *The Economist*, March 3, 2011. Accessed February 4, 2013. http://www.economist.com/node/18285798.

Efaw, Jamie and Christopher Heidger. "Another Tool in the Influencer's Toolbox: A Case Study." Accessed May 20, 2013. https://globalecco.org/97#All.

Ekine, Sokari. "Introduction." In *SMS Uprising: Mobile Activism in Africa*, edited by Ekine Sokari, ix-xxiii. Oxford: Pambazuka Press, 2010.

El-Baghdadi, Lyad. "Meet Asmaa Mahfouz and the Vlog that Helped Spark the Revolution." YouTube. Accessed May 17, 2013. http://www.youtube.com/watch?v=SgjIgMdsEuk.

E-Marketer.com. "Facebook Helps Get One in Five People Worldwide Socializing on Online Networks." Accessed April 22, 2013. http://www.emarketer.com/Article/Facebook-Helps-One-Five-People-Worldwide-Socializing-on-Online-Networks/1008903.

FEELTHELIGHT. "Iran, Tehran: Wounded Girl Dying in Front of Camera, Her Name was Neda." YouTube. Accessed May 14, 2013. http://www.youtube.com/watch?v=bbdEf0QRsLM.

Fernandez, Alberto. "The Center for Strategic Counterterrorism Communications." Speech given at the Naval Postgraduate School, Monterey, CA, April 14, 2013.

Fielding, Nick and Ian Cobain. “Revealed: U.S. Spy Operation that Manipulates Social Media.” *The Guardian*, March 12, 2011. Accessed May 10, 2013. http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.

Gameson, William, Bruce Fireman, and Steve Rytina. *Encounters with Unjust Authority*. Homewood, Ill: Dorsey Press, 1982. Quoted in Doug McAdam. “Micromobilization Contexts and Recruitment to Activism.” *International Social Movement Research* 1 (1988): 125–154.

Gettleman, Jeffery. “On Eve of Vote, Fragile Valley in Kenta Faces New Divisions.” *The New York Times*, March 2, 2013. Accessed May 17, 2013. http://www.nytimes.com/2013/03/03/world/africa/on-eve-of-vote-fragile-valley-in-kenya-faces-new-divisions.html?ref=todayspaper&_r=0.

Ghonim, Wael. *Revolution 2.0*. New York: Houghton Mifflin Harcourt Publishing Company, 2012.

Gladwell, Malcolm. “Small Change: Why the Revolution will not be Tweeted.” *The New Yorker*, October 4, 2010. Accessed August 20, 2012. http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all.

———. *The Tipping Point*. New York: Back Bay Books, 2002.

Glanz, James and John Markoff. “U.S. Underwrites Internet Detour around Censors,” *The New York Times*, June 12, 2011. Accessed March 12, 2013. http://www.nytimes.com/2011/06/12/world/12internet.html?pagewanted=all&_r=0.

Glod, Maria. “Va. Man Allegedly Used Facebook to Threaten D.C. Area Bombings.” *The Washington Post*, December 14, 2010. Accessed December 20, 2012. http://www.washingtonpost.com/wp-dyn/content/article/2010/12/14/AR2010121406829.html.

Granovetter, Mark. “The Strength of Weak Ties,” *American Journal of Sociology* 78. No. 6 (1973): 1360-1380. Accessed May 15, 2013. http://sociology.stanford.edu/people/mgranovetter/documents/granstrengthweakties.pdf.

Gupta, Ravi and Brooks, Hugh. *Using Social Media for Global Security*. Indianapolis: John Wiley & Sons, Inc., 2013.

Han, Shin-Kap. “The Other Side of Paul Revere: The Brokerage Role in the Making of the American Revolution.” *Mobilization: An International Quarterly* 14. No. 2 (2009): 143-162.

Herring, Jon. “Disinformation Flies in Syria’s Growing Cyber War.” *Reuters*, August 7, 2012. Accessed September 6, 2012. http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807.

Hookway, James. “Vietnam Convicts 3 Bloggers Over Posts.” *The Wall Street Journal*, September 24, 2012. Accessed April 12, 2013. http://online.wsj.com/article/SB10000872396390444358804578015383720801250.html.

Hosenball, Mark. “Iran Helping Assad to Put Down Protests,” *Reuters*, March 23, 2012. Accessed September 6, 2012. http://www.reuters.com/article/2012/03/23/us-iran-syria-crackdown-idUSBRE82M18220120323.

Internet World Stats. “World Internet Usage and Population Statistics June 30, 2012.” Accessed March 22, 2013. http://www.internetworldstats.com/stats.htm.

Iran Media Project. “Text Messaging as Iran’s New Filtering Frontier.” April 25, 2013. Accessed May 2, 2013. http://www.iranmediaresearch.org/en/blog/227/13/04/25/1360.

Kendzior, Sarah and Katy Pearce. “How Azerbaijan Demonizes the Internet to Keep Citizens Offline.” *Slate.com*, May 11, 2012. Accessed April 10, 2013. http://www.slate.com/blogs/future_tense/2012/05/11/azerbaijan_eurovision_song_contest_and_keeping_activists_and_citizens_off_the_Internet_.html.

King, Gary. “China’s ‘Internet Police’ Targets Collective Action.” *National Public Radio*, August 8, 2012. Accessed September 6, 2012. http://www.npr.org/2012/08/08/158448847/chinas-Internet-police-targets-collective-action.

Klandermans, Bert. “Mobilization and Participation: Social-Psychological Expansions of Resource Mobilization Theory.” *American Sociological Review* 42 (1984): 583–600.

Kramer, Andrew. “Russians Selectively Blocking Internet.” *The New York Times*, March 31, 2013. Accessed April 12, 2013. http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-Internet-content.html?_r=0.

Kreutz, Christian. “Mobile Activism in Africa: Future Trends and Software Developments.” In *SMS Uprising: Mobile Activism in Africa*, edited by Sokari Ekine, 17–31. Oxford: Pambazuka Press, 2010.

Langlie, Emily. “Seattle Area Man Who Fled to Mexico, Sentenced for Bank Fraud in ‘Lies for Loans’ Scheme Defendant Defrauded Credit Unions with Phony Purchase Orders for Luxury Cars.” The United States Attorney’s Office Western District of Washington, August 9, 2010. Accessed September 2, 2012. http://www.justice.gov/usao/waw/press/2010/aug/sopo.html.

Laudon, Kenneth and Carol Traver. *E-Commerce: Business, Technology, Society*, 7th ed. Upper Saddle River, NJ: Prentice Hall, 2011.

Lee, Doowan. “A Social Movement Approach to Unconventional Warfare,” *Special Warfare Magazine* 27, No.1 (2013).

Lucente, Seth, Greg Wilson, Rob Schroeder, and Gregory Freeman. “Crossing the Red Line.” *From the CORE: Common Operational Research Environment Quarterly Newsletter* 3 (2013): 2–5.

Mann, Jim. “Tape Recording the Modern Medium of Dissent.” *The Los Angeles Times*, Jaunary 11, 1987. (Accessed April 13, 2013). http://articles.latimes.com/1987–01–11/opinion/op-3795_1_democratic-progressive-party.

Martin, Rachel. “CIA Tracks Public Information for the Private Eye.” National Public Radio, January 22, 2012. Accessed September 1, 2012. http://www.npr.org/2012/01/22/145587161/cia-tracks-public-information-for-the-private-eye.

Mayfield, Thomas. “A Commander’s Strategy for Social Media.” *Joint Forces Quarterly* 60 (2011): 79-83. Accessed May 3, 2013. http://www.ndu.edu/press/commanders-strategy-social-media.html.

McAdam, Doug. *Political Process and the Development of Black Insurgency, 1930–1970*, 2nd ed. Chicago: The University of Chicago Press, 1999.

———. “Micromobilization Contexts and Recruitment to Activism,” *International Social Movement Research* 1 (1988): 125–154.

McComb, Lindsay. “Social (Media) Revolution: There’s An App for That.” The Metaq.com. Accessed February 20, 1023. http://themetaq.com/articles/social-media-revolution-theres-an-app-for-that.

Meier, Patrick. “PeaceTXT Kenya: Since Wars Begin in Minds of Men.” iRevoluition.net. Accessed May 17, 2013. http://irevolution.net/tag/sms/.

Morozov, Evgeny. “How Dictators Watch Us on the Web.” *Prospect Magazine*, November 18, 2009. Accessed November 21, 2012. http://www.prospectmagazine.co.uk/magazine/how-dictators-watch-us-on-the-web.

———. “Empire-Social Networks, Social Revolution: Interview with Marwan Bishara.” By Marwan Bishara. IITrends. Accessed November 12, 2012. http://www.iitrends.com/2011/03/video-social-networks-social-revolution.html

———. *The Net Delusion*. New York: PublicAffairs, 2011.

Mydans, Seth. “People Power II Doesn’t Give Filipinos the Same Glow.” *The New York Times*, February 5, 2005. Accessed November 15, 2012. http://www.nytimes.com/2001/02/05/world/people-power-ii-doesn-t-give-filipinos-the-same-glow.html.

Ning.com. “14-Day Trial on all Plans.” Accessed March 31, 2013. https://www.ning.com/pricing/.

Norton, Quinn. “Anonymous 101 Part Deux: Morals Triumph Over Lulz.” *Wired Magazine*, December 30, 2011. Accessed January 25, 2013. http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux.

OpenNet Initiative, “Global Internet Filtering Map,” Opennet.net. Accessed December 12, 2013. http://map.opennet.net/filtering-IT.html.

———. “Global Internet Filtering Map.” Opennet.net. Accessed December 12, 2013. http://map.opennet.net/filtering-pol.html.

———. “Global Internet Filtering Map.” Opennet.net. Accessed December 12, 2013. https://opennet.net/research/map/socialmedia.

Orsi, Peter. “Cuba Internet Cable Turned On, Juicing Up Country’s Connection to Outside World.” *The Huffington Post*, January 21, 2013. Accessed February 5, 2013. http://www.huffingtonpost.com/2013/01/22/cuba-Internet-cable_n_2521330.html.

Osa, Maryjane. “Networks in Opposition: Linking Organizations through Activists in the Polish People’s Republic.” In *Social Movements and Networks*, edited by Mario Diani and Doug McAdam, 77–104. New York: Oxford University Press, 2003.

Oweidat, Nadia, Cheryl Benard, Dale Stahl, Walid Kildani, Edward O’Connell, Audra Grant. “The Kefaya Movement.” The RAND Corporation. Accessed January 16, 2013. http://www.rand.org/pubs/monographs/2008/RAND_MG778.pdf.

Passy, Florence. “Social Networks Matter. But How?” In *Social Movements and Networks*, edited by Mario Diani and Doug McAdam, 21–48. Oxford University Press: New York, 2003.

PBS Frontline. “April 6th Youth Movement.” Accessed December 9, 2012. http://www.pbs.org/wgbh/pages/frontline/revolution-in-cairo/inside-april6-movement/.

Petit, Brian. “Social Media and Unconventional Warfare, *Special Warfare Magazine* 25, No. 2 (2012): 20–28.

Piven, Frances and Richard Cloward. *Poor People’s Movements: Why They Succeed, How They Fail*. New York: Vintage Books, 1979.

Polletta, Francesca. “Contending Stories: Narrative in Social Movements,” *Qualitative Sociology* 21, No. 4 (1998): 419–446.

Pop-Eleches, C., H. Thirummurthy, J. P. Habyarimana, J. G. Zivin, M. P. Goldstein, D. de Walque, L. Mackeen, J. Haberer, S. Kimaiyo, J. Sidie, D. Ngare, and D. R. Bangsberg. “Mobile Phone Technologies Improve Adherence to Antiretroviral Treatment in a Resource-Limited Setting: A Randomized Controlled Trial of Text Message Reminders.” The National Center for Biotechnology Information (NCBI). Accessed May 17, 2013. https://www.ncbi.nlm.nih.gov/pubmed/21252632.

Raghavan, Sudarsan. “Powerful Elite Cast a Shadow Over Reforms in Yemen.” *The Guardian*, February 22, 2013. Accessed March 12, 2013. http://www.guardian.co.uk/world/2013/feb/26/yemen-powerful-tribal-families-influence.

Roberts, Hal., Ethan Zuckerman, and John Palfrey. “2007 Circumvention Landscape Report: Methods, Uses, and Tools.” Berkman Center for Internet & Society at Harvard University. Accessed November 10, 2012. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2007_Circumvention_Landscape.pdf.

———. “2011 Circumvention Tool Evaluation.” Berkman Center for Internet & Society at Harvard University. Accessed November 10, 2012. http://cyber.law.harvard.edu/publications/2011/2011_Circumvention_Tool_Evaluation.

Roberts, Hal, Ethan Zuckerman, Julian York, Robert Faris, and John Palfrey. “2010 Circumvention Tool Usage Report.” Berkman Center for Internet & Society at Harvard University. Accessed November 17, 2012. http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage.

———. “International Bloggers and Internet Control.” Berkman Center for Internet & Society at Harvard University. Accessed November 20, 2012. http://cyber.law.harvard.edu/publications/2011/International_Bloggers_Internet_Control .

Roberts, Nancy. “Social Capital.” Lecture given at the Naval Postgraduate School, Monterey, CA, 26 September, 2012.

Ryan, Yasmine. “Tunisia’s Bitter Cyber War.” Aljazeera. January 6, 2011. Accessed December 15, 2012. http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html.

Schmidt, Michael, Keith Bradsher, and Christine Hauser. “U.S. Panel Cites Risks in Chinese Equipment.” *The New York Times*, October 8, 2012. Accessed May 2, 2013. http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all&_r=0.

Shapiro, Samantha. “Revolution, Facebook Style.” *The New York Times*, January 25, 2009. Accessed January 18, 2013. http://www.nytimes.com/2009/01/25/magazine/25bloggers-t.html?_r=0&pagewanted=print.

Shirky, Clay. “The Political Power of Social Media.” *Foreign Affairs* 90, No. 1(2011): 28–41.

Shuster, Mike. “A New Weapon against Nukes: Social Media.” National Public Radio. Accessed September 2, 2012. http://www.npr.org/2012/02/08/146589700/a-new-weapon-against-nukes-social-media.

Siegal, Robert. “How Does the CIA Use Social Media.” National Public Radio. Accessed September 1, 2012. http://www.npr.org/2011/11/07/142111403/how-does-the-cia-use-social-media.

Snow, David and Robert Benford. “Ideology, Frame Resonance, and Participant Mobilization.” *International Social Movement Research* 1, No. 1 (1988): 197–217.

Snow, David, E. Rochford, Jr., Steven Worder, and Robert Benford. “Frame Alignment Processes, Micromobilization, and Movement Participation.” *American Sociological Review* 51, No.2 (1986): 464–481.

Spencer, Richard. “Tunisia Riots: Reform or be Overthrown, U.S. Tells Arab States Amid Fresh Riots.” *The Telegraph*, January 13, 2011. Accessed January 21, 2013. http://www.telegraph.co.uk/news/worldnews/africaandindianocean/tunisia/8258077/Tunisia-riots-Reform-or-be-overthrown-U.S.-tells-Arab-states-amid-fresh-riots.html#mm_hash.

Sutter, John. “Google Reports ‘Alarming’ Rise in Government Censorship Requests.” CNN. Accessed February 13, 2013. http://www.cnn.com/2012/06/18/tech/web/google-transparency-report.

Swaby, Rachel. “7 Massive Ideas that Can Change the World.” *Wired Magazine*, January 17, 2013. Accessed February 10, 2013. http://www.wired.com/business/2013/01/ff-seven-big-ideas/all/.

Tarrow, Sidney. *Power in Movements*. Cambridge: Cambridge University Press, 1998.

Tibken, Shara. "FBI Uses Facebook to Nab NY Terrorist Suspect," CNET.com. Accessed December 21, 2012. http://news.cnet.com/8301–1023_3–57535887–93/fbi-uses-facebook-to-nab-ny-terrorist-suspect/.

Topping, Alexandra. "Fugitive Caught After Updating His Status on Facebook." *The Guardian*, October 14, 2009. Accessed September 1, 2012. http://www.guardian.co.uk/technology/2009/oct/14/mexico-fugitive-facebook-arrest.

Tyson, Jeff. "How Internet Infrastructure Works." How Stuff Works. Accessed February 8, 2013. http://computer.howstuffworks.com/Internet/basics/Internet-infrastructure1.htm.

U.S. Attorney's Office. "New York Man Pleads Guilty to Attempting to Bomb New York Federal Reserve Bank in Lower Manhattan." The FBI New York Field Office. Accessed March 12, 2013. http://www.fbi.gov/newyork/press-releases/2013/new-york-man-pleads-guilty-to-attempting-to-bomb-new-york-federal-reserve-bank-in-lower-manhattan.

United For Iran. "16 Azar Green Routes." Flickr. Accessed May 18, 2013. http://www.flickr.com/photos/united4iran/4165827330/.

United States Special Operations Command. "Special Operations Forces Operating Concept." Accessed May 20, 2013. http://fortunascorner.files.wordpress.com/2013/05/final-low-res-sof-operating-concept-may-2013.pdf.

Vaughan-Nichols, Steven. "How Social Networking Works." *IT World*. Accessed December 12, 2012. http://www.itworld.com/software/91803/how-social-networking-works.

Voss, Bristol. "Governments Shop for Latest Internet Weapons." *Minyanville*, August 28, 2012. Accessed September 6, 2012. http://www.minyanville.com/business-news/politics-and-regulation/articles/Internet-weapons-cyberspace-social-media/8/28/2012/id/43548?page=full.

Walsh, Edward. "Resource Mobilization and Citizen Protest in Communities Around the Three Mile Island." *Social Problems* 29, No. 1(1981): 1-21. As quoted by Doug McAdams. "Micromobilization Contexts and Recruitment to Activism." *International Social Movement Research* 1(1988): 125-154.

Waruzi, Bukeni. "Using Mobile Phones for Monitoring Human Rights Violations in the DRC." In *SMS Uprising: Mobile Activism in Africa*, edited by Sokari Ekine, 138–142. Oxford: Pambazuka Press, 2010.

Williams, Ben. Presentation given at the Naval Postgraduate School, Monterey, CA, October 23, 2012.

Wojcieszak, Magdalena., Briar Smith, and Mahmood Enayat. "Finding a Way: How Iranians Reach for News and Information." The Iran Media Program's 2011–2012 Report on Media Consumption in Iran. Accessed April 12, 2013. http://www.global.asc.upenn.edu/fileLibrary/PDFs/FindingaWay.pdf.

Wong, Edward. "Riots in Western China Amid Ethnic Tensions." *The New York Times*, July 6, 2009. Accessed November 22, 2012. http://www.nytimes.com/2009/07/06/world/asia/06china.html?_r=0&pagewanted=print.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California