REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
24-03-2016	Master of Military Studies	SEP 2015 – APR 2016

4. TITLE AND SUBTITLE
Virtual Camouflage: Social Media and a New Operating Environment in the 21st Century

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Cahill, Jeffrey, J., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Matthew J. Flynn

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The communication strategies implemented by the Islamic State have been effective, and it can be assumed that future groups, who wish to disseminate messages of violence to achieve their political end state, will emulate, implement, and adapt the information strategies used by ISIS and its support network. With an obsolete framework to fully measure the social complexity of insurgent messaging and social influence, the immediate Western reaction to IS success has been the classic default response of targeted kinetic military action against a perceived distinguishable enemy. While kinetic engagements have been unyielding, the objectives of a counterinsurgency are rarely reconciled by the decisive military battle. Within the virtual operating environment, the capacity to influence change and disseminate a grievance narrative has become as powerful as ever. The Islamic State's proven online tactics, techniques, and procedures (TTPs) will enable future non-state actors and underground insurgencies to more effectively disseminate their objectives, propaganda messages, and grievance narratives through the technologies and tools of the internet.

15. SUBJECT TERMS
ISIS; Islamic State; counterinsurgency; COIN; social media; internet

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	37	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Virtual Camouflage: Social Media and a New Operating Environment in the 21st Century

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

AUTHOR:
Major Jeffrey J. Cahill, USMC

AY 15-16

Mentor and Oral Defense Committee Member: MATTHEW FLYNN
Approved: _____
Date: 3/24/16

Oral Defense Committee Member: J.W. Gordon
Approved: _____
Date: 3/24/16

R.S. DiMAIO
R S DiMaio 24MAR16

Executive Summary

Title: Virtual Camouflage: Social Media and a New Operating Environment in the 21st Century

Author: Major Jeffrey J. Cahill, United States Marine Corps

Thesis: The introduction and accessibility of social media and the internet has changed the means and ways by which insurgent actors are able to achieve their political ends. Insurgent leaders have historically adopted an irregular, operational approach because they have recognized their organization's relative inferiority as compared to the traditional capabilities of the adversary. The proliferation and accessibility of the internet and digital technology have become a force multiplier for the decentralized networks of insurgent strategy, creating an information advantage for an otherwise inferior insurgent force.

Discussion: The counterinsurgency (COIN) lessons-learned from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), which were validated after a decade of US combat operations in theatre, lose relevance unless they are supplemented with a profound understanding of the social and psychological insurgent narratives now easily distributed by the internet. The communication strategies implemented by the Islamic State have been effective, and it can be assumed that future groups, who wish to disseminate messages of violence to achieve their political end state, will emulate, implement, and adapt the information strategies used by ISIS and its support network. With an obsolete framework to fully measure the social complexity of insurgent messaging and social influence, the immediate Western reaction to IS success has been the classic default response of targeted kinetic military action against a perceived distinguishable enemy. While kinetic engagements have been unyielding, the objectives of a counterinsurgency are rarely reconciled by the decisive military battle. Within the virtual operating environment, the capacity to influence change and disseminate a grievance narrative has become as powerful as ever. The Islamic State's proven online tactics, techniques, and procedures (TTPs) will enable future non-state actors and underground insurgencies to more effectively disseminate their objectives, propaganda messages, and grievance narratives through the technologies and tools of the internet.

Conclusion: The US approach to defeating the Islamic State is flawed, for it fails to highlight and address the changing sociological characteristics of insurgent doctrine perpetuated by the influence of internet communication. The Islamic State of Iraq and al-Sham has survived in large part because of its dynamic and innovative utilization of the internet and social media as an uncontested sanctuary to disseminate an ideological narrative. The Islamic State has effectively exploited the expansive reach of the virtual environment, the vulnerabilities of social human behavior, and the infallibility of the internet to plan and organize operations, maintain and finance its organization, and attract and inspire new followers.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

Preface

Earning the trust and commitment of the civilian population is critical in successful counterinsurgency operations. Equally important is the ability of the counterinsurgency to isolate the civilian population from the support and solicitations of the insurgency, and disconnect the population from the insurgent narrative. The proliferation of technology, the infallibility of the internet, and a decentralized release architecture, which enables an insurgent actor to quickly deliver a narrative to his audience, have caused a superior US force to relinquish the advantage to the insurgent. The goal of this paper is to address the shortfalls of current literature and doctrine regarding the complimentary relationship between social media and COIN, and then bridge the widening gap between population-centric COIN strategy, the complex and mobilizing influence of social media, and the rapidly changing character of the virtual operating environment. The speed at which technology is able to reach the open market and strengthen the influence of non-state actors is occurring at a faster pace than that which US strategists and leaders can respond with thoughtful and timely tactics, techniques and procedures.

I would like to thank my wife, Molly, for her enduring support during this Academic Year. Her commitment, understanding, and self-sacrifice over the last nine months in allowing me to reach my academic goals has been boundless. I would also like to thank Professor Matthew J. Flynn and Lieutenant Colonel Jeffrey A. Vandaveer. Their encouragement, guidance, and support were instrumental in the development of this essay. Also, a special thanks to the Ladies at the Marine Corps University Leadership Communication Skills Center.

Virtual Camouflage:
Social Media and a New Operating Environment in the 21st Century

"It is the people who figure out how to work simply in the present, rather than the people who mastered the complexities of the past, who get to say what happens in the future."

– Clay Shirky, Adjunct Professor at New York University's graduate Interactive Telecommunication Program (ITP), where he teaches courses on the interrelated effects of social and technological network topology and how its networks shape culture[1]

INTRODUCTION

Each insurgency is an amalgamation of enduring political strife and evolving character. While the nature of an insurgency has remained relatively unchanged, which is the "organized use of violence to seize, nullify, or change political control of a region," the fundamentals of its sociological character have evolved with the mobilizing influences of social media and the infallibility of internet content.[2] The introduction and accessibility of social media and the internet has changed the means and ways by which insurgent actors are able to achieve their political ends. Insurgent leaders have historically adopted an irregular, operational approach because they have recognized their organization's relative inferiority as compared to the traditional capabilities of the adversary. The proliferation and accessibility of the internet and digital technology have become a force multiplier for the decentralized networks of insurgent strategy, creating an information advantage for an otherwise inferior insurgent force.

When assessing the information war of any conflict, labels become blurred. Labelling a collective body as a terrorist organization, transnational violent extremist group, insurgency, jihadist, belligerent, or guerrilla force becomes less important than recognizing and addressing the integrated communication advancements and social mobilizing strategies validated by the adversary, such as the Islamic State (IS). The Islamic State's proven online tactics, techniques, and procedures (TTPs) will enable future non-state actors and underground insurgencies to more effectively disseminate their objectives, propaganda messages, and grievance narratives through the technologies and tools of the internet. The Islamic State's successes will be adopted by

future non-state actors, as "it should come as no surprise that terrorists tend to study other terrorists – they do it vertically (through the study of historical narratives and evidence) as well as horizontally (by studying the tactics and strategies of contemporaneous groups)."[3] The reach of the internet has had an exponential effect on the capacity to translate influence into action, and challenges current counterinsurgency (COIN) core principles, which necessitate the isolation and protection of the population from the insurgency.

The anonymity of the internet allows a cyber insurgent to deliver his message and establish a connection with a population while concealing his identity under the camouflage of an online pseudonym or persona. The capacity to exploit such a permissive environment is derived from a term, coined by the author of this paper, called virtual camouflage. Virtual camouflage is the disguise that allows one to freely operate in the non-physical domain of the virtual environment by exploiting the sanctuary provided by the anonymity of the internet. Given the huge amount of digital information constantly flowing across the internet, "it is difficult for security forces to distinguish between serious threats and trivial ones. This lack of clarity affords insurgents a degree of protection."[4]

This study identifies a new virtual operating environment created by the internet and social media in which insurgents can collectively leverage asymmetric, catalyzing mediums of influence to exploit the infallibility of the internet and target the vulnerabilities of social human behavior. While the population-centric nature of counterinsurgency operations remains enduring, the accessibility and proliferation of information, through the internet and various social media platforms, has codified a virtual sector of the Operating Environment (OE), altered the available channels and communication drivers of social influence, and facilitated the emergence of virtual social identities based on a shared interest to promote violence. These

changes in social influence and behavior have expanded the reach of insurgent narratives and challenge the population-centric principles of published COIN doctrine. The internet has revolutionized the military operating environment, galvanized the virtual community, and forever-changed the methods by which insurgents can communicate, cooperate, and organize to achieve their objectives. The communication strategies implemented by organizations such as the Islamic State have been popular and effective in exposing the general population to its political message. Historical experience suggests that there is little hope of destroying a revolutionary guerilla movement after it has acquired the sympathetic support of a significant segment of the population.[5] Aspiring groups, who desire to mobilize a population to achieve a political objective, will emulate, implement, and adapt the proven strategies engineered by the Islamic State and its support network.

LITERATURE REVIEW

Sources for this paper were compiled from a variety of doctrinal publications, literature sources, and online video clips. The publications referenced include journal articles, Armed Forces of the United States Service and Joint Doctrine, and scholarly books, which discuss the mobilizing influences of social media and the authoritative guidance designed to prepare the joint force and other government agencies in the conduct of COIN operations. The goal of this paper is to address the shortfalls of current literature and doctrine regarding the complimentary relationship between social media and COIN, and then bridge the widening gap between population-centric COIN strategy, the complex and mobilizing influence of social media, and the rapidly changing character of the virtual operating environment. The speed at which technology is able to reach the open market and strengthen the influence of non-state actors is occurring at a faster pace than that which US strategists and leaders can respond with thoughtful and timely

tactics, techniques and procedures. Steven Metz, in his 2012 article, "The Internet, New Media, and the Evolution of Insurgency," believes that:

> Today's technology is capable of supporting an ever-expanding information flow. It has also reduced transmission times and cost, allowing dispersed units or organizations to communicate, coordinate, and swarm, either to targets or to successful narratives. By acting with some degree of effectiveness, even without central command and control, insurgencies as a movement are more survivable because they are not vulnerable to decapitation of their leadership.[6]

Although Metz's article is more than three years old, his argument remains relevant. Organizations like IS will retain an advantage in the information environment as long as they are able to control the narrative and exploit the concept of decentralized release authority. Like other authors, he argues that insurgencies employing these techniques cannot be defeated, only managed.

Governmental publications provide the fundamental framework for the conduct of counterinsurgency operations. Joint Publication 3-24, *Counterinsurgency*, which was modified and released in November 2013, and Army Field Manual 3-24.2 (2009), are the two principle publications designed to assist American forces in the planning, execution and assessment of counterinsurgency operations. Both publications place the physical, psychological, political, and social isolation of the population from the insurgency as essential elements of COIN strategy – and both publications highlight the relevance of the information environment and the narrative. Unfortunately, the cycle at which these publications are updated and distributed is not able to keep pace with the speed at which technology and information are effecting the operating environment. JP 3-24, which is the most recent joint doctrine publication on COIN, is already over two years old. The messaging strategies of the Islamic State did not become available on

the internet and social media until the summer of 2014. Thus, current COIN doctrine, as it applies to the adaptive TTPs of ISIS and information operations, is obsolete.

On February 25, 2015, FBI Director James Comey delivered a speech at the National Association of the Attorneys General. In his speech, titled *ISIS is a Top Priority*, Director Comey paints a very clear picture of the ISIS social media strategy. He states, "ISIL is putting out a siren song through their slick propaganda…through social media that goes like this – troubled soul, come to the caliphate…you will live a life of glory; these are the apocalyptic end times. You will find a life of meaning here fighting for our so-called caliphate."[7] Director Comey's expression reflects the themes of many authors, who in their articles, analyze the dissemination of the ISIS narrative, through internet mediums such as Twitter, Facebook, and YouTube, and argue that the Islamic rationale used by the Islamic State to recruit and sustain its members is a violation of basic Islamic principles. David Sorenson, a Professor of International Security Studies at the US Air War College, proposes a US led, but not owned, counter-ISIS information campaign designed to "challenge the veracity of ISIS thought and action."[8] In Professor Sorenson's article *Confronting the "Islamic State,"* he cites the work of Peter Krause and Stephen Van Evera, who defend that a campaign should be designed to "evoke dialogue over monologue by encouraging Muslims to discuss and implement religious prohibitions on ISIS ideations."[9] The United States has the technology, intelligence, and media experience to identify pertinent communities, craft messages, and to deliver these messages. But the strategy has to be more sophisticated than the simple argument that "ISIS is bad" or "ISIS is not Islam."

Within the last three months, the US Government has added a branch to its strategy to defeat ISIS. The Obama Administration has become much more outspoken about the importance of a sophisticated strategy that incorporates information operations. Thus far, the strategy has

been dominated by kinetic engagements. In an article published by Gardiner Harris in January 2016, Harris cites multiple statements by the White House Press Secretary, Josh Earnest, who acknowledges that the White House has failed to develop a strategy to counter extremist recruitment and exhortations of violence on social media. The State Department, Department of Justice, and Department of Homeland Security, with the assistance of the private sector, have begun to implement tools that "effectively counter the austere and apocalyptic pronouncements of Islamic extremists, improve responses to jihadist propaganda, and counter the disinformation from extremist groups by highlighting their misdeeds and creating positive images of the West."[10] An approach that attacks the human cognitive dimension is manpower intensive and will require a large coalition to marginalize the Islamic State online: from governments and companies to non-profits and international organizations.[11]

Ultimately, this paper identifies an emerging topic, gives it a name, and provides key means of analysis that have otherwise been absent in current literature and military doctrine. The effectiveness of future counterinsurgency strategy in the new virtual operating environment is contingent upon the capacity and desire of Western governments to develop and implement tangible countermeasures that restrict freedom of movement online and degrade the protective concealment of virtual camouflage.

BACKGROUND

The accessibility to the internet has become a force-multiplier for insurgent groups that were historically quelled by the traditional confines of expensive communication strategies and sophisticated technological mediums. The United States Government, Department of Defense, and Joint Force no longer retain an advantage as it applies to employing the traditional security methods used to isolate a population from an insurgency, as "the operating environment is

increasingly enabled by technology, which provides the types of capabilities once largely limited to major powers to a broad range of actors."[12] Insurgent groups have changed the status quo of the operating environment through the use of social media and the internet to establish virtual social identity connections with their sympathizers. Virtual connections have redefined the operational environment and challenged the capacity of COIN forces to isolate the population from insurgent forces.

The Joint Army-Marine Corps counterinsurgency publication, FM 3-24 *Counterinsurgency*, is universally accepted as the most up-to-date, "coherent and insightful publication on the subject since the Marine Corps Small Wars Manual of 1940."[13] This COIN publication, along with other service-specific doctrinal manuals, combine the lessons learned from historic counterinsurgencies and current operations with the realities of today's operational environment. Although valuable lessons have been learned from past experiences, the US analysis of counterinsurgency remains concerned more with "perfecting the minutiae of tactics, techniques, and procedures" than with understanding and preparing for the ensuing sociological dynamics enabled by the social influence of the internet and social media.[14] The COIN lessons-learned from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), which were validated after a decade of US combat operations in theatre, lose relevance unless they are supplemented with a profound understanding of the social and psychological insurgent narratives now easily distributed by the internet.

At its core, "a counterinsurgency is an armed struggle for the support of the population."[15] Retired United States Army Lieutenant Colonel John A. Nagl is a counterinsurgency expert who has argued for a "push" methodology during COIN operations, which is designed to push the insurgent from the population and focuses on dividing the people

from the insurgents.[16] But how does a COIN force isolate an insurgency from its popular support and restrict its contact with outside sympathizers when the ability to connect and share information is limitless in the new virtual environment created by the internet? Insurgent forces now, more than ever, possess the capacity to exploit the connectivity of the global network landscape to codify shared grievances.

A group perpetrating organized violence to achieve political goals against a recognized state authority within a nation is known as an insurgency. An insurgency has enduring requirements, such as the need to recruit additional members, acquire financial resources, and maintain operational safe havens. The internet and social media provide the platforms to fulfill these requirements. YouTube and Twitter enable the dissemination of real-time video and propaganda tweets to attract additional members. Video-sharing and photo-sharing websites also display examples of efficacy to potential donors sympathetic to a group's narrative. And the virtual and anonymous nature of the internet provides insurgents a safe haven from government and institutional policing. As nation-states struggle to establish legitimacy and stability, dissatisfied members of the population will blend alternative methods of social influence and religious fundamentalism to establish a shared identity with other dissatisfied sympathizers. JP 3-24.2 states that "there are three prerequisites for an insurgency to be successful in an area – a vulnerable population, leadership available for direction, and lack of government control."[17] An additional prerequisite – an easily accessible, instantaneous and infallible medium to disseminate a solution to popular dissatisfaction – has now become a prerequisite to implementing a successful resistance campaign.

With an obsolete framework to fully measure the social complexity of insurgent messaging and social influence, the immediate Western reaction to insurgent success has been

the classic default response of targeted kinetic military action against a perceived distinguishable enemy. While kinetic engagements are unyielding, the objectives of a counterinsurgency are rarely reconciled by the decisive military battle. Rather, a re-engineered system that adapts and understands the evolving, online-focused, and population-centric character of COIN will assist in achieving the doctrinal objective of the civilian population assenting to Host Nation (HN) governance. The effectiveness of the long-term, intensive, and expensive whole-of-government counterinsurgency system has been challenged by the opportune, cursory, and low-cost information war that the internet can leverage.

Units conducting COIN perform offensive operations in order to achieve three fundamental objectives: secure the populace continuously; isolate the insurgency from the populace; and destroy, disrupt, interdict, deny or neutralize elements of the insurgency.[18] The majority of insurgencies have been limited to local regions and constrained within the boundaries of individual nation-states. However, the exponential influence and instantaneous communication of social media has nurtured an environment where insurgent groups and leaders retain unrestricted, worldwide capacity to garner support for their cause and to support causes they view as compatible with their own goals. Insurgents manage perceptions through propaganda and their narrative. In technologically advanced insurgencies, "filming an attack may be as important as the attack itself," and the influence of such an act becomes systemic.[19] While current doctrine captures the protractive nature of COIN, its analysis lacks substantive comprehension regarding the relationships between social media influence, social identity development, the power of virtual communities and each's capacity to desirably shape a targeted population. A core principle of COIN doctrine is to isolate and protect the civilian population

from the insurgency. The virtual character and accessibility of the internet challenges the achievement of this objective.

THE NEW OPERATING ENVIRONMENT

A military force is trained for conventional warfare, but many current and future conflicts require and will require a new strategy that moves beyond conventional military action, as the advent of faster and greater capacity-carrying information networks have transformed the operating environment. According to an article published in *The Economist* in January 2013, "between 1775 and 1945, only about a quarter of insurgencies achieved most or all of their aims. But since 1945, that number has risen to 40%."[20] The improved success, specifically in the last decade, has been a direct reflection of the improvements made to mass media and technology. The centers of gravity have changed, and the role of synchronized communication has evolved. In the battle to publicize the narrative, insurgents have many more weapons at their disposal to employ against what has traditionally been considered a superior adversary. Post-World War II, "the spread of democracy, education, mass media, and the concept of international law have all conspired to sap the will of states engaged in protracted counter-insurgencies."[21] The system is no longer linear. Mass media and basic communication capabilities, once only accessible to technologically-advanced societies, have connected the global majority to the virtual enterprise. New technological mediums, which allow users to interface globally with anyone able to access a computer, tablet, or cellular phone, have forever-changed the way information is exchanged. Example of information-exchanging domains include the internet, e-mail, text-messaging, social networking (Facebook, Twitter, and Snapchat), chat rooms, blogs, file-sharing (Google Docs) and video-sharing (YouTube). Information strategy is about identifying and exploiting the

instruments that capture the audience's attention, shape its behavior, and translate attitudes and opinions into tangible action.

On June 29, 2014, the Islamic State of Iraq and al-Sham (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL), a Sunni jihadist insurgent group composed of paramilitary personnel and captured Iraqi Army equipment and weapons, began an organized movement of armed conflict designed to overthrow the constituted government of Iraq and establish an Islamic State. Initially comprised of 10,000 militants, the group took territory and began to expand their influence in the Middle East region.[22] The deterioration of the Syrian and Iraqi states further enabled ISIS's expansion of power, control, and legitimacy. Combining innovative technological strategies with strong force, intimidation, and financial resources, ISIS has been successful in projecting power. ISIS has become quite sophisticated in its use of propaganda and social media messaging, as it maintains an organized and well-coordinated online network that inflates and promotes its violent extremist messages. Building on techniques pioneered by other terrorist organizations, such as Al Qaeda in the Arabian Peninsula (AQAP) and Al Shabaab, ISIS not only employs social media to spread its messages and recruit followers, but also to empower its supporters to take part in the process.[23] Beginning in July 2014, the Al-Hayat Media Center, which serves as the distributor for new ISIS media, initiated the release of videos, mujatweets, and the online English-language magazine *Dabiq* as a stepping-stone to project strength and promote engagement online.

One of ISIS's more successful mediums is the Arabic-language Twitter application called the *The Dawn of Glad Tidings*, or just *Dawn*. The application instantly connects to the latest links, hashtags, and images about the jihadi group. Another application ISIS uses to magnify its message are organized hashtag campaigns, in which the group enlists hundreds and sometimes

thousands of activists to repetitively tweet hashtags at certain times of the day, causing them to spike and trend within social media. As a result of these strategies, ISIS is able to project strength and promote engagement online. Systematically, the world is witness "to the emergence of a visually-oriented, ideologically impulsive Internet culture with the means to rapidly and collectively plan and act."[24] While the dissemination of published material is not a new concept, the key change is online exposure to such publications.

The communication strategies implemented by the Islamic State have been effective, and it can be assumed that future groups, who wish to disseminate messages of violence to achieve their political end state, will emulate, implement, and adapt the information strategies used by ISIS and its support network. ISIS has proven that "electronic narratives are so pervasive that they generate actions before ideologies are considered. With greater emphasis on building a narrative and less on ideology, social media offers an alternative to the historical, linear progression of developing a resistance storyline."[25]

Earning the trust and commitment of the civilian population is critical in successful counterinsurgency operations. Isolating the civilian population from the support and solicitations of the insurgency disconnects the population from the insurgent narrative. According to COIN doctrine, the Small Wars Manual, and Joint Publication 3-24, "the strength and success of an insurgency depends in large part on its ability to shape the behavior of its ranks and the population whose compliance and outright support it requires."[26] The proliferation of internet technology and the low cost of digital devices have made COIN isolation strategies that much more challenging. The focus of USG COIN strategy in Iraq and Afghanistan during the first decade of the 21st century was focused on the physical security of the population and isolation from the insurgents. Physical isolation was effective, as network devices and communication

networks were in their infancy in these regions and only a small percentage of the population and insurgency possessed a technological capability. However, internet and telecommunication usage has soared in Africa and the Middle East since 2000. According to Internet World Stats, as of 30 November 2015, there were 331,000,000 people in Africa and 123,000,000 people in the Middle East with internet access. From 2000-2015, these regions experienced a growth in internet usage of 3,650% and 7,231%, respectively. By comparison, North America saw a 190% growth in internet usage during the same time period.[27]

The influence of transnational organizations on insurgent activities has added to the complexity of defining the OE. However, the term transnational assumes that the existence of borders and boundaries is universal. In the virtual world of the internet and social media, information and violent narratives are able to freely permeate national borders and regional boundaries. As was demonstrated during the Arab Spring in 2011, the freedom to operate in the cyber domain has caused the border construct to become futile. Populations who were once divided by the borders that defined their national identity, culture and governance, have become blurred with the evolution of a new virtual culture. Brian Petit, in his article *Social Media and UW*, references a new dimension in unconventional warfare by which the user can instantly connect, communicate and act in this borderless space. Better known as "swarming," users can operate in a "coordinated strategic way to strike from all directions. Swarming in the digital domain can easily span time zones, geography, economic and cultural barriers."[28] The Revolution in Egypt, which was mobilized at least in part by a Facebook page that read, "We are all Khaled Said," publicized the wrongful death of an Egyptian businessman. The Facebook page became a modern example of swarming, for it enabled unity through the instantaneous mobilization of mass. The social media campaign illustrated a new capability to instantaneously

mobilize a regional Muslim population. While there were other drivers of change in Egypt that lead to President Hosni Mubarak's eventual removal from power, specifically demographic conflict, foreign policy issues, and challenges to the legitimacy of the state, social media tools, such as Facebook and Twitter, did "speed up the process by helping to organize the revolutionaries, transmit their message to the world and galvanize international support."[29] A revolution had been building for years. But it was the accessibility and global reach of social media that allowed the marginalized activists in Egypt to mobilize the population and effectively disseminate their message. Ideas disseminated in Egypt during the Arab Spring validated the concept that "social media [outlets] had become the pamphlets of the 21st century – a way that people who are frustrated with the status quo can organize themselves and coordinate protest," which could then lead to a global revolution.[30] In a fact sheet released by the US Department of State in March, 2012, it was identified that both traditional journalists and bloggers played critical roles reporting on the events of the January 2011 Revolution, organized heavily through social media tools such as Facebook and Twitter.[31] In today's context, the capacity to influence change and disseminate a grievance narrative is as powerful as ever. Insurgents are unlimited in their capacity to exploit the transparencies of social media and magnify the vulnerabilities of weak and failing governments.

SOCIAL INFLUENCE IN THE VIRTUAL COMMUNITY

Insurgents are able to boost their social influence and reputation in the virtual community by disseminating propaganda and making it accessible to anyone attracted to it. They adapt their message to the audience, implement marketing techniques like those of large corporations, and disseminate a communication campaign designed to attract customers to its brand. According to Rheingold in *Virtual Social Identity and Consumer Behavior*, "a virtual community is an

association of like-minded individuals who maintain extended discussions mixed with enough feeling to develop deeper relationships online."[32] For those individuals who possess minimal interest in the insurgent propaganda machine, its message stagnates in the ether. However, for those individuals who seek to discover a message of violence through the virtual landscape of the internet, the message is easily accessible and influential. This delivery method constructed by ISIS works in similar fashion to a corporate creative marketing strategy. When an effective social influence campaign is well designed and executed, its brand possesses the capacity to flourish. Anthony Pratkanis, in his "Winning Hearts and Minds: A Social Influence Analysis," defines social influence as "any technique, device, procedure, or manipulation on the social-psychological nature of human beings as the means for creating or changing the belief or behavior of the target."[33]

The internet and social media generate an ability to produce bonds between people who have never and would never have met if it were not for the computer-linked global social connections facilitated by the efficacy of the internet. Whether native or foreign-born, the great majority of radicals today are converted not by someone they know or by an imam in a mosque but over the internet, which serves as the most powerful tool that has ever existed for promoting ideas.[34] And the opportunity to influence continues to rise with a substantial shift in the capacity to mobilize online. As of April 2011, the Middle East constituted a region of the world with the largest amount of new Facebook users. Facebook's mobile users "exceeded 250 million subscribers and Twitter users exceeded 200 million users" in the Middle East, according to the Arab Social Media Report.[35] Collectively, the 200 million Twitter users tweet about 4 billion tweets a month.[36] And in nations like Egypt, where a relatively low percentage of the population uses Facebook (5.5%), the translation amounts to 6 million users in a national population of over

120 million.[37] Those 6 million users are connected to a much larger community of social contacts who, even without access to social media, can be influenced by the messages posted to this virtual landscape.

The rise of the Islamic State of Iraq and al-Sham, and its increasingly sophisticated social media communication and recruitment strategies have influenced a diverse group of people from around the world. ISIS's far-reaching propaganda machine, accelerated by ease-of-access to the internet and social media outlets, has attracted thousands of recruits to the contested region. According to the International Center for the Study of Radicalization and Political Violence (ICSR), the number of foreign fighters that have joined the Sunni militant organization in Syria and Iraq continues to rise. As of 2015, "the estimated worldwide total of foreign fighters was 20,730. This makes the conflict in Syria and Iraq the largest mobilization of foreigner fighters in Muslim majority countries since 1945. It now surpasses the Afghanistan conflict in the 1980s, which is thought to have attracted up to 20,000 foreigners."[38] ISIS has transformed the way terrorist groups and their supporters reach, influence and recruit followers around the world by developing an aggressive social media strategy. This approach enables ISIS to employ tactics that empower individual supporters to take part in creating and distributing its narrative.[39]

The Yale Model, developed by psychologist Carl Hovland and his colleagues during and after World War II, is a simple, yet effective framework that can be used to dissect and examine how ISIS has capitalized upon the infinite reach of the internet to harness social influence, persuasion techniques, and brand management. The model is designed to look at the process of social influence through six stages: exposure, attention, comprehension, acceptance, retention, and translation that must be navigated to successfully persuade a target audience.[40] Through this model, one can begin to conceptualize the power of the internet to build linkages, leverage

narratives, and mobilize sympathizers. The ultimate objective is target audience persuasion, connection, and action.

The first step in disseminating a message that connects a leader with a prospective follower in the virtual community is presentation and exposure. The IS communication strategy represents an effective utilization of propaganda and recruitment. Historically, jihadist movements adopted video content as an important part of their strategy – "ISIS's embrace of social media and youth culture gave these videos a new videogame-like quality. As with Twitter, ISIS uses YouTube and other video platforms to spread visual and often graphic messages of intimidation, religious justification, and recruitment."[41] These repeated images do nothing but glorify ISIS's brutal acts, helping to make the group more appealing to younger people through skillfully applied editing and production techniques. According to Jack Dickey, author of the *Time* magazine article "The Antisocial Network:"

> Current neuroscientific research suggests that teenager's brains are wired differently than those of adults, as younger people lack the adult capacity for complex reasoning and are thus more susceptible to emotional appeals. Similarly, teenager frontal lobes, the position of the brain responsible for measuring consequences and morality of choices, do not fully form until one's 20s.[42]

When exposed to graphic videos and images that depict death, destruction and the perception of justice to Islamist enemies, younger people lack the reasoning capacity to distinguish right from wrong and thus are a more susceptible audience to the ISIS narrative and violence brand.

In the second stage, the goal is to capture the audience's attention. Even if the message is transmitted through easily accessible means, there must be a driver that causes the audience to gravitate towards it. Aside from long-form propaganda videos, the al-Hayat Media Center

creates the "increasingly popular spate of short propaganda videos, called "mujatweets." These high-quality morsels average around a minute in length and aim to portray the softer side of ISIS. One video depicts ISIS fighters handing out ice cream and candy to overjoyed children."[43] Other videos depict foreign fighters from the West inviting others to join ISIS. The videos are short and deliver a persuasive message, which is to identify with the Islamic State and oppose injustices created by Western influence. In addition to appealing to Westerners for recruitment reasons, the "mujatweets" also serve to represent the "caliphate's stability, prosperity, and strength of leadership."[44]

The third stage, which is comprehension, maintains that an influence campaign must "ensure that the intended audience understands the persuasive communication."[45] The target audience must not only comprehend the message, but also accept it. As a tool to persuade acceptance, ISIS uses the social photo-sharing platform, Instagram, as a means to boost its image and share visually its message of injustice and jihad with the world. These Instagram users, who post photos to social media and narrate personal stories of victory, represent the success that ISIS seeks to glamorize. The expectation is that the opportunity to achieve success in the name of jihad will become infectious. Successful comprehension and identification with the message increases the potential of a previous fence-sitter to reject internal feelings of apprehension. The adoption of a persuasive narrative sets the preconditions for acceptance.

During the fourth stage and fifth stages, which are acceptance and retention, "the target audience must not only comprehend the message, but also accept it; and it must have a durable effect on the target audience(s)."[46] Because social media can only serve as the initiator of change, the catalyst for influence relies on a communication strategy where the audience accepts the message and is prepared to mobilize based on their own acceptance.

"Cognitive change, leading to behavioral change, or the translation of perception into action" occurs during the sixth and final stage.[47] Relationships developed online can be as mobilizing as those made face-to-face, resulting in extreme group behavior. Translation of perception into action through online relationships began to reveal itself in the early 2000s through a phenomenon known as "web suicide pacts." According to BBC News, in Japan in 2005, "91 people died in suicide pacts" that were initiated and coordinated through internet communication forums.[48] An increasing number of young people in Japan, feeling alienated by the stresses of modern life and in search of other like-minded individuals, used the expansive reach of the internet to connect with others who shared a common interest of suicide. The article highlights how suicide pacts become appealing for those in fear of dying alone. Membership, influenced by the power of community, provided a tangible mechanism to enable action.

VIRTUAL SOCIAL IDENTITY PHENOMENON

One of the strengths of the ISIS propaganda campaign created through online virtual interaction and information sharing has been the establishment of a collective social identity phenomenon, where individuals intentionally choose to align themselves with a violent, yet justified grievance narrative against the West. The concept of a collective social identity refers to an individual's sense of belonging to the group or collective. For the individual, the identity derived from the collective shapes a part of his or her personal identity. The internet has transformed the global nature of community and identity. Along with other groups, this unbounded medium has provided ISIS the cohesiveness needed to disseminate its violent message. Through online media forums, ISIS has been able to invoke strong social connections with its global audience. These social connections have created a collective social identity that

trumps the other aspects of the person's personal identity. Individuals gain an immediate sense of belonging and identity that transcends the individual.

Social media tools merge online and offline identities. It is the ability to establish a virtual social identity connection with its followers that further galvanizes individuals sympathetic to a violent, counter-HN governance grievance narrative. This virtual social identity, which exploits uncontested social media channels that serve as a catalyst for its far-reaching propaganda machine, has become the core of the insurgent strategic communication campaign. Per JP 3-24, "narratives are central to representing collective/group identities, particularly the collective identity of religious sects, ethnic groupings, and tribal elements…insurgents will exploit populations whose social narrative and norms are similar to or can be manipulated by the insurgent group."[49] The emergence of virtual communities have expanded the reach of insurgent narratives. The internet and proliferation of social media outlets have dramatically changed the exposure to grievance narratives by facilitating expansive networks that connect the individual with a virtual community. Internet-driven insurgencies are able to attract recruits and support from around the world, "particularly if the instigators use transnational ideologies rather than purely local or nationalistic ones."[50] Internet access has become commonplace and its accessibility provides a bridge between emotionally-driven individuals and the insurgent narrative. Because of its virtual nature, the internet community has no concrete counterpart and becomes idealized in the imagination of its users. In the case of a message that promotes violence, the fundamentals of jihad become attractive to young, alienated individuals, who are vulnerable and sympathetic to the global grievance message and in search of a new sense of community that will ease their loneliness through a connection to other people who perceive to share similar strife.[51]

Online social networks can contribute to the development of an individual's self-esteem and the positive reinforcement experienced when sharing in the identity and success of a particular group. Social identity theory has "strongly incorporated self-esteem as a motivator for outcomes. It has been shown that group memberships are often a source of self-esteem. This is particularly true for those who not only classify themselves as members, but who are also accepted by others as members."[52] According to Korina Korostelina, author of *Social Identity and Conflict*, "social identity includes a feeling of belonging to a social group, as a strong connection with a social category, and as an important part of our mind that affects our social perceptions and behaviors."[53] Individuals from distinct cultures may feel particularly motivated to distinguish themselves from other groups when their distinctiveness or identity is perceived as threatened, challenged, or salient.[54] Insurgencies, such as IS, strive to validate this perception through polarizing rhetoric and internet propaganda tactics that support their narrative. This strategy captures an emotional response from the population through the exploitation of media outlets that are effectively able to communicate images and messages inciting anti-Western aggression. Anger and resentment become the driving force, rather than the ideology. Young, impressionable individuals are driven to believe that the West is threatening to their social identity. This social identity propaganda encourages individuals, who may feel disenfranchised by the West, to identify with an organization, such as IS, with whom they share a more familiar ideology, coupled with the anger towards another group. Even though the Islamic State demonstrates a violent and radical ideology, an individual's sensitivity and resistance to violent extremism is diminished when he is persuaded to believe that his Muslim identity is in jeopardy. Therefore, it is reasonable to expect that an individual watching a successful jihadist image or video on social media that counters perceived Western aggression, in order to protect the

threatened identity of all Muslims, will lead to immediate sympathy towards the goals of ISIS and its jihadi brand.[55] The internet is a tool that can leverage the power of an ideology through the influence of media. Ideologies that were once restricted to the populations with which they were physically co-located have now become tangible mobilizers to the near and far sympathizer.

The freedom to disseminate materials and develop relationships over the internet has led to a thriving radical culture. Natalie Wood, in the book, *Virtual Social Identity and Consumer Behavior*, argues, "as the world shifts into new expanses of communicative ability, led by the ever-evolving force of technology, the opportunity to seek and attain knowledge and understanding expands as well."[56] The virtual nature of the internet provides a medium for insurgents to actively engage in social communication and interaction with the population while also achieving the benefits of virtual anonymity. Much like an insurgent or guerilla who uses the camouflage of the population to escape identification and capture, the anonymity of the internet allows a cyber insurgent to deliver his message while benefiting from the virtual camouflage that cyberspace provides. The insurgent "claims the honors while rejecting the same obligations. His kind of organization permits him to escape the police…and the army cannot use the power of its weapons against him because he hides himself permanently within the midst of the population going about its peaceful pursuits."[57] One of the greatest weapons an insurgent has is the concealment provided by the local population.

A grievance narrative, when properly constructed, has the capacity to shape and reinforce the malleable characteristics and sensitivities of an individual's social identity. An immediate connection occurs between the individual and the narrative based on a pre-existing social identity and then builds on those convictions. With the proliferation of internet media

outlets that publicize anonymous postings, where the source and content cannot and do not need to be verified before release, insurgents are able to freely disseminate vexatious propaganda without having to provide a clear source, context, or complete storyline. There is no credibility requirement and the insurgents capitalize on the vulnerability of the system and their audience. According to Steven Metz, "the internet, information and ideas move with such rapidity and in such complex ways, that it is impossible to identify or gauge the authority of a given source. Information may have been passed through hundreds, thousands, or even millions of individuals and locations…no one will able to identify its origin."[58] Credibility is based on appeal and speed, and "the criterion for credibility thus becomes the inherent receptivity of the receiver."[59] The insurgent grievance narrative, regardless of credibility, targets a sympathetic audience based on religion or ethnicity, and uses a shared common social identity to build an immediate connection and compassion with the insurgency.

CONCLUSION

The 2015 National Military Strategy addresses the requirement to counter non-state actors who are undermining transregional security and threatening US national interests. This study has argued that the US approach to defeating such adversaries is flawed, for it fails to highlight and address the changing sociological characteristics of insurgent doctrine perpetuated by the influence of internet communication. The Islamic State of Iraq and al-Sham has survived in large part because of its dynamic and innovative utilization of the internet and social media as an uncontested sanctuary to disseminate an ideological narrative. Although it has acquired weapons, equipment and resources, mainly from the struggling states of Iraq and Syria, ISIS lacks the infrastructure of a traditional state. In order to successfully offset these strategic shortfalls, the Islamic State has effectively exploited the expansive reach of the virtual

environment, the vulnerabilities of social human behavior, and the infallibility of the internet and its content to plan and organize operations, maintain and finance its organization, and attract and inspire new followers.

Some strategists will argue that the only way to defeat belligerent non-state actors, such as the Islamic State, is through an intensive bombing campaign or a sophisticated and enduring cyber network attack. While focused and deliberate, attempting to shut down the insidious messages of Western adversaries and contesting their internet presence is nearly impossible because of the instantaneous delivery methods and anonymous nature of the cyber operating environment. Video-sharing and social media platforms require minimal personal information to register and are able to solicit interest under the protection of virtual camouflage, which is the disguise that allows one to freely operate in the non-physical domain of the virtual environment while exploiting the sanctuary provided by the anonymity of the internet.

While these strategies, and others that might follow could temporarily paralyze the targeted organization, these measures fail to address the galvanizing and mobilizing driver that has fostered IS's global growth – which is exploiting the infallibility of the internet to generate a powerful human behavioral connection between its caliphate narrative and its audience.

Insurgencies have been a part of history ever since the establishment of the state. What has changed over the last three to five years is the global accessibility of grievance narratives and propaganda messaging. Grievances that were traditionally restricted by state boundaries and imperfect communication mediums, are now able to easily circulate through the low-cost and easily-accessible pathways of the internet. Beyond the accessibility of the internet are the virtual communities created by social media platforms that initiate communication and encourage like-minded individuals to interact based on the perception of shared interests.

The West faces a challenge online from these groups, a challenge that contests the very premise of population-centric COIN. Winning hearts and minds, the central tenet to waging a successful counterinsurgency, now entails a difficult pursuit in advancing a narrative that overcomes its counterpoint online. In short, the accessibility and proliferation of online technology threatens to undo the foundation of US COIN strategy, which starts and ends with the acceptance that preserving the will of the people is essential to successful COIN operations. As this analysis clearly points out, addressing this challenge should be the most essential aspect of US military thinking when looking to regain the advantage in COIN strategy.

[1] http://www.bloomberg.com/research/stocks/private/person.asp?personId=25574469&privcapId=32946925&previousCapId=91996&previousTitle=Index%20Ventures

[2] Joint Staff, *Counterinsurgency*, Joint Publication 3-24 (Washington DC: Joint Staff, November 22, 2013), I-1.

[3] Paul J. Smith, *The Terrorism Ahead: Confronting Transnational Violence in the Twenty-First Century*, (New York: Routledge, 2015), 17.

[4] Steven Metz, "The Internet, New Media, and the Evolution of Insurgency," *Parameters* (Autumn 2012): 85.

[5] Headquarters of the Marine Corps, *Mao Tse-tung on Guerilla Warfare*, FMFRP 12-18 (Washington, DC: US Marine Corps, April 5, 1989), 27.

[6] Steven Metz, "The Internet, New Media, and the Evolution of Insurgency," *Parameters* (Autumn 2012): 86.

[7] James Comey, "ISIS is a Top Priority," video, 2:12, address at the National Association of the Attorney's General on February 25, 2015, https://www.youtube.com/ watch?v=YgMebzDi328.

[8] David S. Sorenson, "Confronting the "Islamic State"," *Parameter*s, (Autumn 2014): 25.

[9] Ibid, 34.

[10] Gardiner Harris and Cecilia Kang, "Obama Shifts Online Strategy on ISIS," *New York Times* (January 8, 2016).

[11] Jared Cohen, "Digital Insurgency: How to Marginalize the Islamic State Online," *Foreign Affairs*, (November-December 2015): 55.

[12] US Department of Defense, *2014 Quadrennial Defense Review* (Washington, DC, March 4, 2014).

[13] William Rosenau, "Counterinsurgency: Lessons from Iraq and Afghanistan," *Harvard International Review 31.1*, (Spring 2009): 52.

[14] Ibid, 53.

[15] Headquarters Department of the Army, *Tactics in Counterinsurgency*, FM 3-24.2 (Washington, DC: US Army, April 21, 2009), ix.

[16] John A. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*, (Chicago: University of Chicago Press, 2005), 28.

[17] Headquarters Department of the Army, *Tactics in Counterinsurgency*, FM 3-24.2 (Washington, DC: US Army, April 21, 2009), 1-16.

[18] Ibid, 5-1.

[19] Ibid, 4-11.

[20] Max Boot, "How the Weak Vanquish the Strong." *The Economist*, January 19, 2013.

[21] Ibid.

[22] Heather Marie Vitale, "A Time to Tweet, as well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria," *Defense Horizons* (October 2014), 2.

[23] "The Social Influence of ISIS Beheadings," Kathe Kollwitz, *The Parents*, https://medium.com/homeland-security/the-social-influence-of-isis-beheadings-9fce5c8ceb40#.

[24] Brian Petit, "Social Media and UW," *Special Warfare* 25, no. 2 (April-June 2012): 26, http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html.

[25] Brian Petit, "Social Media and UW," *Special Warfare* 25, no. 2 (April-June 2012): 27, http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html.

[26] Joint Staff, *Counterinsurgency*, Joint Publication 3-24 (Washington DC: Joint Staff, November 22, 2013), xi.

[27] "World Internet Usage and Population Statistics, November 30, 2015," Miniwatts Marketing Group, *Internet World Stats*, last updated January 7, 2016, http://www.internetworldstats.com/stats.htm

[28] Brian Petit, "Social Media and UW," *Special Warfare* 25, no. 2 (April-June 2012): 26, http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html.

[29] Sam Gustin, "Social Media Sparked, Accelerated Egypt's Revolutionary Fire," *Wired*, February 2011, http://www.wired.com/2011/02/egypts-revolutionary-fire.

[30] Ibid.

[31] US Department of State, "The Arab Spring in Egypt: Revolution at Tahrir Square," March 19, 2012, http://www.state.gov/outofdate/bgn/egypt/196332.htm.

[32] Natalie T. Wood and Michael R. Solomon, ed. *Virtual Social Identity and Consumer Behavior* (New York, Routledge, 2009), 139.

[33] "The Social Influence of ISIS Beheadings," Kathe Kollwitz, *The Parents*, https://medium.com/homeland-security/the-social-influence-of-isis-beheadings-9fce5c8ceb40#.

[34] Margot Patterson, "Seduced by ISIS," *America*, March 30, 2015, 12, http://americamagazine.org/sites/default/files/issues/2015/pdfs/03-30-15web.pdf.

[35] "Civil Movements: The Impact of Facebook and Twitter," Racha Mourtada and Fadi Salem, *Arab Social Media Report* vol. 1, no. 2 (May 2011), 1.

[36] Ibid, 2.

[37] Ibib, 5.

[38] "Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s," Peter R. Neumann, *International Center for the Study of Radicalization and Political Violence*, last modified January 25, 2015, http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s.

[39] Anti-Defamation League, "Homegrown Islamic Extremism in 2014: The Rise of ISIS and Sustained Online Recruitment," *Imagine a World Without Hate*, April, 2015, http://www.adl.org/assets/pdf/combating-hate/homegrown-islamic-extremism-in-2014-the-rise-of-isis-and-sustained-online-recruitment.pdf.

[40] "The Social Influence of ISIS Beheadings," Kathe Kollwitz, *The Parents*, https://medium.com/homeland-security/the-social-influence-of-isis-beheadings-9fce5c8ceb40#.

[41] Heather Marie Vitale, "A Time to Tweet, as well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria," *Defense Horizons* (October 2014), 5.

[42] Ibid, 5.

[43] Ibid, 3.

[44] Ibid, 4.

[45] "The Social Influence of ISIS Beheadings," Kathe Kollwitz, *The Parents*, https://medium.com/homeland-security/the-social-influence-of-isis-beheadings-9fce5c8ceb40#.

[46] Ibid.

[47] Ibid.

[48] "Web Suicide Pacts Surge in Japan," *BBC News*, last modified February 9, 2006, http://news.bbc.co.uk/2/hi/asia-pacific/4695864.stm.

[49] Joint Staff, *Counterinsurgency*, Joint Publication 3-24. (Washington DC. Joint Staff, November 22, 2013), I-7.

[50] Steven Metz, "The Internet, New Media, and the Evolution of Insurgency," *Parameters* (Autumn 2012), 85.

[51] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 161.

[52] Peter J. Burke and Jan E. Stets, "Identity Theory and Social Identity Theory," In *Social Psychology Section Session on Theoretical Frameworks at the Annual Meetings of the American Sociological Association*, San Francisco, 1998.

[53] Korina V. Korostelina, *Social Identity and Conflict: Structure, Dynamics, and Implications* (United Kingdom: Palgrave MacMillan, 2007), 15.

[54] Natalie T. Wood and Michael R. Solomon, ed. *Virtual Social Identity and Consumer Behavior* (New York, Routledge, 2009), 319.

[55] Natalie T. Wood and Michael R. Solomon, ed. *Virtual Social Identity and Consumer Behavior* (New York, Routledge, 2009), 319.

[56] Ibid, 135.

[57] Roger Trinquier. *Modern Warfare: A French View of Counterinsurgency*. Translated by Daniel Lee. London: Pall Mall Press, 1964, 13.

[58] Steven Metz, "The Internet, New Media, and the Evolution of Insurgency," *Parameters* (Autumn 2012), 84.

[59] Ibid, 84.

Bibliography

Headquarters Department of the Army. *Tactics in Counterinsurgency*, FM 3-24.2. Washington, DC: Headquarters US Army, April 21, 2009.

Headquarters of the Marine Corps. *Mao Tse-tung on Guerilla Warfare*. FMFRP 12-18. Washington, DC: US Marine Corps, April 5, 1989.

Joint Staff. *Counterinsurgency*. Joint Publication 3-24. Washington DC. Joint Staff, November 22, 2013.

US Department of Defense. *2014 Quadrennial Defense Review*. Washington, DC, March 4, 2014.

Ahuja, Manju K., and Kathleen M. Carley. "Network Structure in Virtual Organizations." Organization Science, Vol. 10, no. 6 (November-December 1999): 741-757. http://www.jstor.org/.

Benson, David C. "Why the Internet is Not Increasing Terrorism." *Security Studies* (May 16, 2014): 293-328.

Boot, Max. "How the Weak Vanquish the Strong." *The Economist*, January 19, 2013.

Burke, Peter J. and Jan E. Stets. "Identity Theory and Social Identity Theory." In *Social Psychology Section Session on Theoretical Frameworks at the Annual Meetings of the American Sociological Association*, San Francisco, 1998.

Cohen, Jared. "Digital Counterinsurgency: How to Marginalize the Islamic State Online." *Foreign Affairs* (November/December 2015): 52-58.

Corman, Steven R., Angela Trethewey, and H.L. Goodall, Jr., ed. *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism.* New York: Peter Lang, 2008.

Cunningham, Daniel, Sean F. Everton, Robert Schroeder. "Social Media and the ISIS Narrative." Department of Defense Analysis, Naval Postgraduate School, 2015.

Eder, Mari K. *Leading the Narrative: The Case for Strategic Communication*. Annapolis, MD: Naval Institute Press, 2011.

Gustin, Sam. "Social Media Sparked, Accelerated Egypt's Revolutionary Fire." *Wired*, February 2011, http://www.wired.com/2011/02/egypts-revolutionary-fire.

Hafez, Kai, ed. *Mass Media, Politics & Society in the Middle East*. New Jersey: Hampton Press, 2001.

Harris, Gardiner and Cecilia Kang. "Obama Shifts Online Strategy on ISIS." *New York Times*, January 8, 2016.

Hudson, Rex A. *Who Becomes a Terrorist and Why: The 1999 Government Report on Profiling Terrorists*. Guilford, CT: The Lyons Press, 1999.

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence*. Berkeley: University of California Press, 2003.

Kahn, Marty Z. "Strategic Communication with the Islamic World." *The Quarterly Journal* (Summer 2012): 41-51.

Korostelina, Korina V. *Social Identity and Conflict: Structure, Dynamics, and Implications*. United Kingdom: Palgrave MacMillan, 2007.

Metz, Steven. "The Internet, New Media, and the Evolution of Insurgency." *Parameters* (Autumn 2012): 80-90.

Mourtada, Racha and Fadi Salem. "Civil Movements: The Impact of Facebook and Twitter." *Arab Social Media Report* vol. 1, no. 2 (May 2011): 1-29.

Nagl, John A. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. Chicago: University of Chicago Press, 2005.

Patterson, Margot. "Seduced by ISIS." *America*, March 30, 2015. 1-39. http://americamagazine.org/sites/default/files/issues/2015/pdfs/03-30-15web.pdf.

Petit, Brian. "Social Media and UW." *Special Warfare* 25, no. 2 (April-June 2012): 25-31.

Rosenau, William. "Counterinsurgency: Lessons from Iraq and Afghanistan." *Harvard International Review 31.1* (Spring 2009): 52-56.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Seul, Jeffrey R. "Ours is the Way of God: Religion, Identity, and Intergroup Conflict." *Journal of Peace Research*, Vol. 36, no. 5 (September 1999): 553-569.

Smith, Paul J. *The Terrorism Ahead: Confronting Transnational Violence in the Twenty-First Century*. (New York: Routledge, 2015.

Sorenson, David S. "Confronting the "Islamic State"." *Parameters* (Autumn 2014): 25-36.

Trinquier, Roger. *Modern Warfare: A French View of Counterinsurgency*. Translated by Daniel Lee. London: Pall Mall Press, 1964.

Van de Velde, James. Crash Their Comms. The American Interest, Vol. 10, no. 6 (June 10, 2015), http://www.the-american-interest.com/2015/06/10/crash-their-comms/

Vitale, Heather Marie. "A Time to Tweet, as well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria." *Defense Horizons* (October 2014): 1-12.

Wellman, Barry, Janet Salaff, Dimitrina Dimitrova, Lauren Garton, Milena Gulia and Caroline Haythornthwaite. "Computer Networks as Social Network: Collaborative Work, Telework, and Virtual Community." *Annual Review of Sociology*, Vol. 22 (1996): 213-238. http://www.jstor.org/

Wood, Natalie T. and Michael R. Solomon, ed. *Virtual Social Identity and Consumer Behavior*. New York: Routledge, 2009.

Zickmund, Susan. "Approaching the Radical Other: The Discursive Culture of Cyberhate." In *Virtual Culture: Identity and Communication in Cybersociety*, edited by Steven G. Jones, 185-205. London: Sage Publications, 1997.