SOCIAL MEDIA AND THE MILITARY: HOW THE FIELD GRADE LEADER SHOULD UNDERSTAND, APPROACH, AND CONTROL SOCIAL MEDIA WARFARE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

KYLE M. DEEM, MAJOR, U.S. AIR FORCE
B.A., Virginia Military Institute, Lexington, Virginia, 2006

Fort Leavenworth, Kansas
2020

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE (DD-MM-YYYY) 12-06-2020	**2. REPORT TYPE** Master’s Thesis	**3. DATES COVERED** ***(From - To)*** AUG 2019 – JUN 2020

4. TITLE AND SUBTITLE Social Media and the Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Kyle M. Deem	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR’S ACRONYM(S)** **11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis analyzed the implications of social media throughout the modern military. The results of this research are intended to inform a field grade leader without a cyber or information warfare background of the benefits and concerns regarding social media and its presence in military operations and daily life. The case study methodology was utilized to identify the vast realm of social media impacts, both abroad and at home. The results made it clear that social media plays a major impact in the gray space of conflict, both shaping and reacting to the informational battlefield. But that impact can be limited through education and counter-disinformation. Furthermore, individual actions on social media do have an effect on military operations as well as civil confidence, but the true impact may be exaggerated. These results should provide field grade officers with a basic understanding of social media risk management.

15. SUBJECT TERMS

Social media, cyber warfare, Russia, Ukraine, ISIS, leadership, information warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** ***(include area code)***
(U)	(U)	(U)	(U)	67	

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Kyle M. Deem

Thesis Title: Social Media and the Military: How the Field Grade Leader Should Understand, Approach, and Control Social Media Warfare

Approved by:

____, Thesis Committee Chair
Lieutenant Commander Jerry B. Tuck, M.E.

____, Member
Gates M. Brown, Ph.D.

____, Member
Lieutenant Colonel Cathy L. Massey, M.S.

Accepted this 12th day of June 2020 by:

____, Director, Office of Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SOCIAL MEDIA AND THE MILITARY: HOW THE FIELD GRADE LEADER SHOULD UNDERSTAND, APPROACH, AND CONTROL SOCIAL MEDIA WARFARE, by Kyle M. Deem, 67 pages.

This thesis analyzed the implications of social media throughout the modern military. The results of this research are intended to inform a field grade leader without a cyber or information warfare background of the benefits and concerns regarding social media and its presence in military operations and daily life. The case study methodology was utilized to identify the vast realm of social media impacts, both abroad and at home. The results made it clear that social media plays a major impact in the gray space of conflict, both shaping and reacting to the informational battlefield. But that impact can be limited through education and counter-disinformation. Furthermore, individual actions on social media do have an effect on military operations as well as civil confidence, but the true impact may be exaggerated. These results should provide field grade officers with a basic understanding of social media risk management.

ACKNOWLEDGMENTS

Thank you to my committee, Lieutenant Commander Jerry Tuck, Dr. Gates Brown, and Lieutenant Colonel Cathy Massey. Your wisdom, time, and guidance made this project possible.

Thank you to my wife and sons for your patience and support, even throughout a pandemic. It is the reason this project was successful.

TABLE OF CONTENTS

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> Humans are wired to believe.
>
> —Glenda Jakubowski, "What's Not to Like: Social Media as an Information Operations Force Multiplier"

Overview

Technological innovations of the twentieth and twenty-first century have rapidly changed the global communications landscape. Recognized nations and rogue groups alike possess previously unattainable capabilities. The development of the internet has enabled the near-instantaneous connection of societies for networking and knowledge. However, this technology can equally prove to be divisive. Governments and societies now embrace the internet as a revolutionary form of social language. Likewise, armed competitors, spanning from established state militaries to terrorist organizations, are using the internet as a proving ground to accomplish objectives from the tactical to strategic levels of warfare.

One of the most noticeable products of the internet-era is the emergence of social media sites. A Merriam-Webster dictionary search defines as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)". The boundaries of social media are vague, the players are seemingly limitless, and the capabilities are vast. In short, anyone can say or broadcast anything to anyone at any time. Such a concept stands in stark contrast to the cultures of structured and disciplined militaries. In those structures, there are clear hierarchical authorities entrusted to disseminate orders that are expected to be followed. Although independent thought in many militaries is mostly accepted and encouraged, subordinates are generally required to be respectful, obey superiors, and execute orders regardless of personal feelings. Social media not only enables but often promotes the opposite.

The digital age of the twenty-first century has opened new possibilities for the military, but likewise created difficulties. Although advances in communication are not new, social media presents an emergent challenge based its size and speed. Positively, the military can use social media to attract the proper recruits, disseminate critical information rapidly, and provide a positive transparency to the public. Just as easily, however, social media can expedite the dissemination of world-wide propaganda, provide global reach to recruit and indoctrinate new fighters, compromise operations and personnel, and serve as a basis for scandals that can be as detrimental as fratricide.

Problem Statement

The impact of social media on warfare is a relatively new field of study. Over two decades of implementation from both state and non-state actors has provided a foundation for study, but long-term strategy remains unclear. The United States (U.S.) military must examine adversarial actions as well as internal culture to ensure success in the continuing emergence of the cyber domain of warfare.

The Research Question

Research Question One: How should the U.S. military embrace social media as a means to achieve military objectives?

Research Question Two: Is social media a weapon of war?

Research Question Three: Do domestic social media scandals of the U.S. military have strategic implications?

Significance of Study

The significance of this research project is to better understand an emerging domain of the present battlefield. This battlefield is fused through Multi-Domain Operations (MDO), utilizing land, sea, air, cyber, and space to achieve the desired effects. Informational warfare, equally as important in many historical cases, has gained a marked advantage with the advent of the internet. Future American dominance across the information spectrum is not assured as smaller groups of belligerents take advantage of increased battlespace, making it more difficult for large nation-states to impose their will in a technologically complex environment.[1] Likewise, near-peer threat Russia has found social media as an ample new host for old Soviet propaganda doctrine. The intent of the research is to study this domain in order to provide insight toward future operations across the realm of social media.

The focus of this study centers on field-grade leadership. The researcher holds no bias and has no background in cyber operations. It is the intent of this study to provide a broad assessment of what the average field-grade leader should know about social media and the military, both at home and abroad.

[1] U.S. Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 6, 2018), 6.

The manner in which social media can be employed requires analysis. The term weapon can be defined many different ways. Cyber warfare expert Thomas Rid defines a weapon as "a tool that is used, or designated to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things".[2] Merriam-Webster's Dictionary is less verbose, describing it as "something (such as a club, knife, or gun) used to injure, defeat, or destroy, a means of contending against another".[3] The Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower, more commonly known as the JFIRE, does not define a weapon, but all references to weapons are physical, lethal means such as a Cluster Bomb Unit (CBU) or Joint Direct Attack Munition (JDAM).[4]

Social media can be used to actively conduct psychological warfare through messaging campaigns. As Beata Bialy of the Cyber Defense Review states, social media can be utilized "as the channel for disseminating messages whose objective is to influence (change) target audiences' opinions, beliefs, perceptions, and behaviors. It means achieving some military effect in the cognitive domain using misinformation (including disinformation) and propaganda."[5] Likewise, it can be used offensively to

[2] Thomas Rid, "Cyber Weapons," *The RUSI Journal* 157, no. 1 (2012): 7.

[3] Merriam-Webster, "Weapon," accessed October 15, 2019, https://www.merriam-webster.com/dictionary/weapon.

[4] Army, Marine Corps, Navy, Air Force, Air Force Tactics, Techniques and Procedures Publication 3-2.6, *JFIRE: Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower* (Joint Base Langley-Eustis, VA: Air Land Sea Application Center, October 2019), 154.

[5] Beata Bialy, "Social Media: From Social Exchange to Battlefield," *Cyber Defense Review* 2, no. 2 (Summer 2017): 78.

promote and encourage direct physical harm to an enemy. The Islamic State of Iraq and Syria (ISIS) engineered a massive social media campaign against the West which translated into kinetic action. For example, a company in Garland, Texas created a competition to draw a cartoon image of Mohammed. Immediately, ISIS sympathizers bombarded Twitter with pleas for sympathetic attacks. Within days two operatives were killed attempting an assault on the Texas Company.[6] This is one of many examples where social media was used to incite physical violence against citizens of the U.S.

By contrast, social media can be used to passively collect information, data, monitor people and/or groups, and defend against threats. Such intelligence can be used to gather target audience data or provide critical data for determining kinetic targets.[7] This is, essentially, an emergent source for the intelligence community. The sociological structures that social media collects form a vast map of both human and cyber intelligence.

Finally, social media is a double-edged sword capable of weakening our force from within. Scandals, regrettable digital footprints, and participation in immoral online activities are just a few examples of these issues. Such events can lead to investigations that are costly in terms of both finance and manpower, but most importantly they erode public trust in an institution that serves citizens and is charged with their protection.

[6] Levi J. West, "#jihad: Understanding Social Media as a Weapon," *Security Challenges* 12, no. 2 (2016): 21.

[7] Bialy, "Social Media: From Social Exchange to Battlefield," 76.

Limitations and Delimitations

This section covers the scope of research for this project, including both limitations and delimitations. The limitations described in this section are factors which the researcher could not control. Delimitations are areas in which the researcher constrained their efforts for the sake of the output.

This project was limited by time and physical space. The schedule for the U.S. Army's Command and General Staff College generally restricts travel for further research and is limited to eleven months. Additionally, language was a limiting factor regarding research of the Ukraine-Russia conflict. Many websites are published in Russian or Ukrainian with no option for English language text. The researcher has no linguistic background in either language and therefore some first-hand blogs and state websites were unfortunately off-limits.

Furthermore, the COVID-19 Coronavirus pandemic became an unexpected limitation. In March 2020, the Command and General Staff College closed its doors to in-person instruction. The Combined Arms Research Library (CARL), Fort Leavenworth's principal research facility, was also closed except for limited access under specific requests. Beginning in March, the researcher conducted all further activity on this project from his own personal residence. Although the internet and use of digital CARL research tools remained an asset, scholarly review and journal database access was limited following the pandemic outbreak.

The scope of research was set to examine the impact of social media practices in regard to military operations, understandable to someone outside of cyber operations. However, effects on diplomacy, economic strategy, and informational programs were examined as well, as these instruments of power are greatly affected by social media. Additionally, research was conducted to analyze the impact of individual military members' social media activities. The overall intent was to broadly assess modern social media impacts to the military. As a result, the researcher chose for this paper to remain unclassified. Therefore, classified cyber operations will not be examined. Finally, the researcher chose not to conduct an in-depth analysis of the likely possibility that internet networks will be destroyed, shut down, or jammed during large scale combat operations. Although it can be assumed there will be network degradation in major combat operations, the researcher is conducting the study through the lens of ongoing issues for the military and social media today.

Summary

The accessibility and versatility of social media has created an open door for warfare. This research project aims to explore the "how" of social media relations across the military, followed up with "so what?" How should American forces and allies successfully apply it as a means to achieve an end? Likewise, how are adversaries using it against the U.S.? How do the actions of those we are entrusted to lead impact our force, and at what level does it truly matter? The results of this research hope to shed light on the impacts of the military-social media relations and serve as a knowledge base for future leaders across all branches of service.

CHAPTER 2

LITERATURE REVIEW

Introduction

This chapter examines publications across the social media spectrum, ranging from military action to individual conduct. The literature was chosen for four primary reasons. First, it provides background and understanding to the current social media environment. Second, it describes social media actions in the recent Russia-Ukraine conflict. Next, it provides depth to the level of social media operations by examining tactics in other conflicts. Finally, it defines US military social media guidance and policies. It is important to review US military individual social media guidance in order to provide a field grade leader with a holistic understanding of social media. Additionally, publication date is worth noting. Many of the journal articles were produced following conflicts in the Libya, the rise of ISIS, and the Russian-Ukrainian conflict. However, books are becoming more prevalent in recent years. Most of the literature has been produced in the past decade and continues to increase.

Social Media Principles

In Countering Online Propaganda and Extremism: The Dark Side of Diplomacy, Corneliu Bjola and James Pamment provide a collection of essays connecting western diplomacy and the challenges it faces through modern social media propaganda.[8] The

[8] Corneliu Bjola and James Pamment, *Countering Online Propaganda and Extremism: The Dark Side of Diplomacy* (London: Routledge, 2019).

book is an excellent starting place to understand how social media is utilized internationally, particularly how data is mined and controlled by interested parties. In particular, the book studies two western foes, Russia and Violent Extremist Organizations (VEO). The authors paint a relatively bleak picture of the current geo-political environment as one that threatens democracy and potentially may only be changed with societal reformation.

The authors introduce the term strategic communication. Strategic communication is a relatively new way to describe a "more structured and goal-oriented form of public response and engagement".[9] Bjola and Pamment continue, "Strategic communication has promised to create a more conducive environment for reaching out and engaging target audiences in a more coordinated, consistent, and effective manner."[10] The use of social media is an essential tool in the effort to utilize, and possibly propagandize, strategic communication.

In order to better understand strategic communication, it is essential to study the theory of reflexive control. Reflexive control is the effort to understand the thinking process of an opponent in order to steer them into taking actions desirable to the controlling side.[11] Essentially, if one can predict a person or organization's actions, they can induce variables which force that person or group to make a decision favorable to the

[9] Bjola and Pamment, *Countering Online Propaganda and Extremism*, 4.

[10] Ibid.

[11] Corneliu Bjola, "Propaganda as Reflexive Control: The Digital Dimension," in *Countering Online Propaganda and Extremism: The Dark Side of Diplomacy,* ed. Corneliu Bjola and James Pamment (London: Routledge, 2019), 15.

other person. Soviet military researcher Dr. Vladimir A. Lefebvre introduced this theory in a book published in the 1960's.[12]

There are two outcomes of reflexive control; constructive and destructive. Constructive output is when an opponent willfully makes a decision favorable to the controlling side.[13] Destructive output is when the opponent is prevented from or negatively influenced away from an outcome unfavorable to the controlling side.[14] Russian interference of a U.S. election campaign to shape the outcome for a favorable candidate is an example of constructive reflexive control. ISIS beheadings to deter further coalition raids in Syria highlight an attempt at destructive reflexive control output. Overall, reflexive control is most successful when the opponent is unaware that they are being influenced.[15] Once they are aware of an external influence, they will adjust their decisions to deter or shape outcomes against the controlling side.[16]

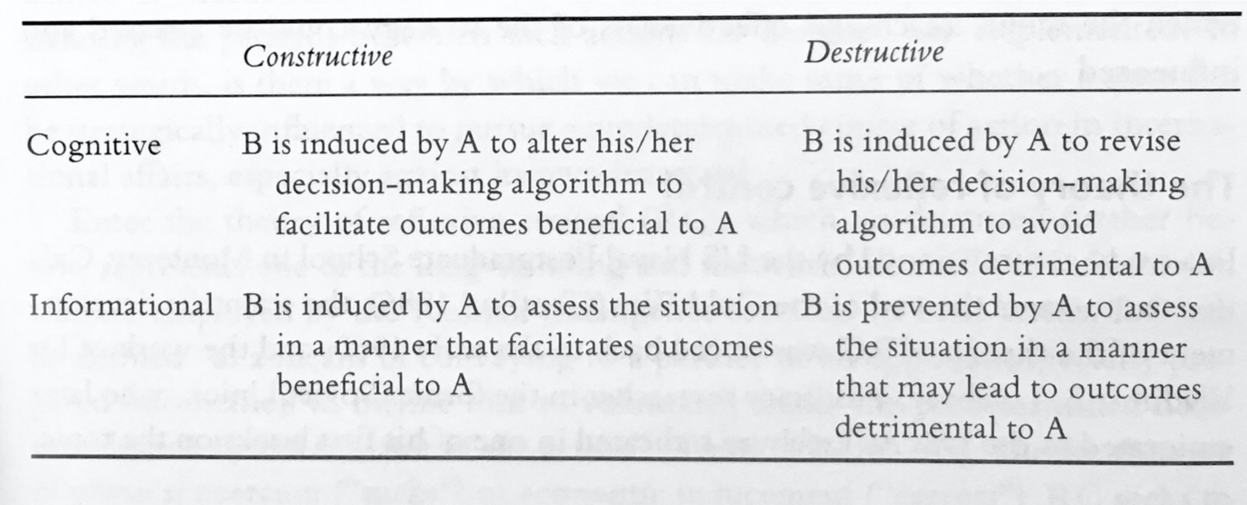
[12] Bjola, "Propaganda as Reflexive Control: The Digital Dimension," 15.

[13] Ibid.

[14] Ibid.

[15] Ibid., 18.

[16] Ibid.



	Constructive	*Destructive*
Cognitive	B is induced by A to alter his/her decision-making algorithm to facilitate outcomes beneficial to A	B is induced by A to revise his/her decision-making algorithm to avoid outcomes detrimental to A
Informational	B is induced by A to assess the situation in a manner that facilitates outcomes beneficial to A	B is prevented by A to assess the situation in a manner that may lead to outcomes detrimental to A

Figure 1. Processes and Outcomes of Reflexive Control

Source: Corneliu Bjola and James Pamment, *Countering Online Propaganda and Extremism: The Dark Side of Diplomacy* (London: Routledge, 2019), 16.

Bjola makes the connection of reflexive control to the digital age. With 3.2 billion people using social media in 2018 alone, a mountain of social, cultural, and economic data exists in unstructured format.[17] He goes on to state that "the data generated online can be theoretically used to build detailed cognitive profiles of target individuals and groups with potentially strong implications for political behavioral prediction".[18] This is done through the use of four filters:

1. Conversation Filter: basic level analysis, hashtags, trends, likes. Used to build thematic profiles, such as topics of conversation.[19]

[17] Bjola, "Propaganda as Reflexive Control: The Digital Dimension," 19.

[18] Ibid.

[19] Ibid., 20.

2. Network Filter: analyzes information flow, notes who people interact with regularly. This paints a picture of how members of a group interact with each other and other groups.[20]
3. Demographic Filter: groups together socio-economic characteristics such as age, gender, education, and occupation. Provides demographic criteria for target audiences.[21]
4. Psychographic Filter: uses sites such as *Google, Facebook,* and *Twitter* to measure psychological attributes. This filter provides the most complex and detailed understanding of an opponent's thinking process but is the hardest to create.[22]

In "Social Media – From Social Exchange to Battlefield", Beata Bialy covers the transformation of social media from simple programs into a weapon.[23] The origins of social media began in the 1980s with a program called Bulletin Board Systems.[24] Two decades passed until Friendster became the first large audience community with over three million users.[25] Shortly after, Facebook, Twitter, Google+, YouTube, Instagram, and Snapchat emerged to create the familiar social media landscape of today. Bialy

[20] Bjola, "Propaganda as Reflexive Control: The Digital Dimension," 20.

[21] Ibid., 20-21.

[22] Ibid.

[23] Bialy, "Social Media: From Social Exchange to Battlefield," 69-90.

[24] Ibid., 69.

[25] Ibid.

explores the gravity and depth of social media, in particular the dependency it brings for many people, regardless of validity. This is where "social cyberattacks" occur, and consequently the weaponization of social media.[26] She explains how ISIS manipulated social media to their advantage, stating that "one of the most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency, and availability 24/7."[27] For example, in 2016 ISIS created a broadcast app for Android that extended outside of their geographical sphere of influence.[28] It was created to teach children the alphabet, but instead made numerous references to jihad and weapons.[29] Bialy concludes by providing five suggestions to counter such activities.

1. Be present on social media with attractive, well-tailored content.
2. Use what technology offers.
3. Advance your own narrative and develop attractive branding.
4. Build your brand and narrative advocacy.
5. Immunize your audience against psychological operations.[30]

Bialy's suggestions are good proposals for individual actions on social media. However, Russia's recent actions in the Ukraine spark an academic debate centered

[26] Bialy, "Social Media: From Social Exchange to Battlefield," 75.

[27] Ibid., 82.

[28] Ibid.

[29] Ibid., 82-83.

[30] Ibid., 87.

around who actually plays a more critical role in social media operations, the state or the individual?

Russia-Ukraine

In "State, Media and Civil Society in the Information Warfare Over Ukraine: Citizen Curators of Digital Disinformation," authors Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Alder-Nissen study the disinformation and counter-disinformation campaign between Russia, Ukraine, and the west surrounding the downing of Malaysian Airlines Flight 17 (MH17).[31] The authors examine 950,000 tweets, focusing on nearly 2,500 active users.[32] The focus of this study is on the role of the individual and the power held by ordinary citizens in social media information operations.

Disinformation, the authors describe, is an intentional effort to deceive, whereas misinformation is erroneous or accidental.[33] They go on to explain that information warfare campaigns, actively spreading disinformation, are targeting ordinary citizens by using information as a weapon and the mind as a battlefield.[34] It is this point that highlights the importance of the potential weaponization of social media. The concept of information and battling for control of the mind is not new, but the reach and speed that

[31] Yevgeniy Golovchenko, Mareike Hartman, and Rebecca Alder-Nissen, "State, Media and Civil Society in the Information Warfare Over Ukraine: Citizen Curators of Digital Disinformation," *International Affairs* 94, no. 5 (September 2018): 975-994.

[32] Ibid., 978.

[33] Ibid., 975.

[34] Ibid., 976.

social media provides changes the game. The content, or payload, of that weapon, however, is important. For example, when Sohaib Athar unknowingly tweeted to the world about the Osama bin Laden raid in his back yard, it took 14 hours to spread globally. However, the Harry Styles' announcement of the break-up of pop band One Direction took about 15 seconds to be seen around the world.[35] The point being, in order for disinformation to be effective it must reach a certain number of audiences in a certain time. This is where tactics come into play.

Furthermore, Golovchenko, Hartman, and Alder-Nissen's discuss curation.[36] Essentially, the role an individual plays in world events is amplified by social media. Much like a museum curator, the individual collects and presents information, rather than artifacts, in an agreeable way to their personal preference. This process of curation is most important at the individual level, where access to information is routinely questioned. The importance is that an individual becomes the owner of state-sponsored information and becomes critical to the dissemination process.[37] This is validated by their findings, which shows that 39 or the 50 most influential MH17 disinformation profiles were citizens.[38] Although their study validates the individual's role in disinformation spreading, state sponsorships continue to feed the machine.

[35] Damon Beres, "Watch the Amazing Way Information Spreads on Twitter," *HuffPost*, last modified March 20, 2016, https://www.huffpost.com/entry/how-twitter-works.

[36] Golovchenko, Hartman, and Alder-Nissen, "State, Media and Civil Society in the Information Warfare Over Ukraine: Citizen Curators of Digital Disinformation," 981.

[37] Ibid., 982.

[38] Ibid., 990.

Maria Snegovaya reviews the Russian machine in "Putin's Information Warfare in Ukraine."[39] Her journal discusses how Russia has centered information operations on reflexive control and how that process adapted over the last few decades. In particular, Russia relies heavily on information operations because it is a cost-effective approach. In the early 2000's, Russia was relying heavily on Soviet era weapons backed by a weak economy.[40] The principles of reflexive control enable Russia to pursue their objectives through western action, or in the case of Crimea, inaction. Additionally, disinformation campaigns enable swift military action by achieving surprise. The minimal Russian casualties in Crimea highlight such success.[41] As a result, Snegovaya believes these developments will reduce Russian military spending.[42]

Additionally, Snegovaya argues that a new cyber approach does not represent new doctrine rather that it relies on Soviet era tactics utilizing new means.[43] While some argue that Russian behavior has shifted since the Cold War, Snegovaya does not agree. Russian information operations, she believes, do not attempt to popularize a new world view, but rather create chaos, misunderstanding, and distrust.[44] She points out that both

[39] Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War, September 2015, https://www.jstor.org/stable/resrep07921.1.

[40] Ibid., 9-10.

[41] Ibid., 17.

[42] Ibid.

[43] Ibid., 7.

[44] Ibid., 14.

the Soviet-era KGB and current Russian trolls and bots disseminate similar styles of disinformation to achieve this effect.[45]

The literature raises interesting points regarding the center of gravity of cyber disinformation. Both the individual citizen and the state play a critical role in its success or failure. However, reflexive control relies upon the actions of the state. Snegovaya correctly points out that western nations must develop theory and doctrine to counter Russian reflexive control through cyber means.[46] As society becomes more educated and suspicious of social media information, the actions of the state will speak louder.

Social Media Operations in the Middle East

Russian operations in Ukraine demonstrate the strategies at play. It is important to examine recent operations in the Middle East to understand the tactics. Adam Segal's book *The Hacked World Order* takes a look at how nations maintain, or upset, the global balance of power in the digital age.[47] Although Segal looks at the broader picture of cyber power and trade, he provides a strong analysis of digital conflict and the role of social media. Segal takes a look at social media usage during Operation Cast Lead, an Israeli offensive against Gaza-based Hamas fighters in 2008. Israeli attempts to control the narrative ultimately backfired. They kept foreign journalists out of Gaza, instead

[45] Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," 14.

[46] Ibid., 21.

[47] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate, in the Digital Age* (New York, NY: Hachette Book Group, 2017).

providing updates through their own YouTube channel and Twitter feed.[48] The videos that were disseminated messaged Israeli self-restraint. One such video showed a helicopter altering the flight path of a missile to avoid hitting civilians that just entered the area.[49] Sympathetic bloggers were allowed early access to material to help spread messaging. A US advocacy group funded training for volunteers across six different languages in an effort to flood Facebook and Twitter with pro-Israeli messages.[50] Teams posted thousands of positive images such as solar farms and female IDF soldiers so that Google search of "Gaza" would not show as many pictures of devastation.[51]

Despite their efforts, the Israeli social media campaign was not well executed. As Segal states, "it was ad hoc and failed to exploit the full potential of the new tools".[52] For example, the accounts were created just prior to the Gaza invasion which did nothing to dispel accusations of propaganda.[53] Their Twitter account, full of military jargon, did not respond to comments and was stale for 179 days following the cease-fire.[54] Most importantly, the Israeli narrative was one of morality and self-restraint. But the 2009 UN Goldstone Report contradicted that by stating it was Israel's policy to target civilians.[55]

[48] Segal, *The Hacked World Order*, 207.

[49] Ibid., 208.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid., 209.

[55] Ibid.

Furthermore, pictures of the destruction in Gaza resonated more powerfully than Israeli YouTube videos.[56] Shortly after, Israel created the New Media Desk in order to correct such missteps and specialize in social media messaging throughout conflict. [57]

Israel learned the hard lesson that a social media campaign can be successful but must be executed with meticulous detail. Flaws in the dissemination of online narratives immediately reduce any credibility. Five years later, the Islamic State in Iraq and Syria (ISIS) set the gold standard for social media messaging. With almost 40,000 tweets in one day alone, ISIS flooded the internet with flags and messages warning Baghdad residents of their impending slaughter.[58] The group developed an app which, once downloaded, gave ISIS the freedom to access and utilize the owner's Twitter account as one of their own.[59] Segal says, "Brutality and barbarism, packaged with sophisticated production techniques, became integral to ISIS's social media campaigns".[60] The videos of savage beheadings and torturous murders struck fear across the world. The group, however, also used social media to portray a lighter side of life, as normal fun-loving people eating Nutella and playing with kittens.[61] Recruitment numbers from 2014 to 2015 paint a successful picture for ISIS's social media campaign. In 2014 approximately

[56] Segal, *The Hacked World Order*, 209.

[57] Ibid.

[58] Ibid., 218.

[59] Ibid., 219.

[60] Ibid.

[61] Ibid.

3,000 Westerners and 12 Americans had gone to fight in Iraq and Syria, by 2015 the numbers spiked to 4,500 and 250, respectively.[62]

ISIS, however, became a victim of their own success. The magnitude of violence, coupled with mass public dissemination, created a global outcry. President Barack Obama addressed the nation, and a poll revealed that 94 percent of Americans said they were following the news of journalists' beheadings.[63] With such a large percentage of America tuned in to the brutality, it was only a matter of time before that led to a call for action. Perhaps most importantly, Segal points out that their "brutality also managed to accomplish what nothing else has: to unite Egypt, the Gulf States, Iran, Iraq, the Kurds, Saudi Arabia, Syria, Turkey, and the U.S. in destroying a common enemy."[64]

In "#jihad: Understanding Social Media as a Weapon", Levi J. West takes a close look at how the Islamic State dominated messaging through social media.[65] He studies how ISIS developed a "system of social media jihad" and why it often resulted in action.[66] West explains that communication is central to terrorism, resulting in the maxim of "propaganda of the deed".[67]

[62] Segal, *The Hacked World Order*, 221-222.

[63] Ibid., 221.

[64] Ibid.

[65] West, "#jihad: Understanding Social Media as a Weapon," 9-26.

[66] Ibid., 10.

[67] Ibid., 11.

West examines Abu Mus'ab al-Suri's strategic theory of a decentralized system of jihad that can be disseminated through social media.[68] The red-haired Syrian published many works on Islamic ideology and tactics which still influence jihadists today. Al-Suri pushed two major points of instruction. Organizationally, al-Suri dismissed traditional pyramid leadership structures for truly independent small-cell operations.[69] Second, he believed in the education and empowerment of the operatives within those cells.[70] Simply put, al-Suri's intentions were to have like-minded people with little to no organizational ties conducting operations world-wide to achieve the same strategic objectives. West summarizes how social media enables such a theory:

> Social media – as a platform for the dissemination of propaganda and education in jihad; as a recruitment platform for drawing participants into jihad; and to facilitate and motivate those seeking to participate in individual and small cell operations, particularly within Western jurisdictions – is unique in its scope and reach.[71]

West concludes with the reminder that propaganda distribution by terror organizations is not a revolutionary concept, but social media provides the means for permanent and continuous distribution of such content.[72] It is his belief that the weaponization of social media is a success and warns that attacks will only continue to increase.[73]

[68] West, "#jihad: Understanding Social Media as a Weapon," 14.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid., 16.

[73] Ibid., 26.

Tim Ripley's article "War of Words – Social Media as a Weapon in Libya's Conflict" takes a close look at some of the early social media tactics employed by fighters in Libya.[74] With social media, Ripley points out, a private citizen now has access to military intelligence, can disseminate counterintelligence, overcome digital barricades, and can real-time open source track military units.[75] Libyan rebels utilizing social media proved adept at all of those functions. After the fall of Benghazi, regime personnel shut down Libya's 3G network, including all internet, mobile data services, short message service (SMS) texting, and telephones.[76] In reaction, rebel forces maintained communications with satellite phones while, simultaneously, their members successfully tapped into the national cellular network and regained access. Once access to functional internet was regained opposition members sent target coordinates to NATO via Twitter, encouraging kinetic strikes.[77] The adaptability of rebel forces to turn a social media site into a call-for-fire mission caused many nations to take note, but Ripley argues that a mentality shift is required to break free from traditional intelligence collection processes.[78] He concludes by saying that "until militaries can produce a strategy to protect sensitive operations from social media scrutiny and put mechanisms in place to

[74] Tim Ripley, "War of Words – Social Media as a Weapon in Libya's Conflict," *Jane's Intelligence Review* 23, no. 9 (Summer 2011): 16-19.

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] Ibid.

monitor the vast streams of social media discussion, the growing availability of open source information is likely to prove more of a hindrance than a help."[79]

Social Media at Home

As online tactics, techniques, and procedures are refined across the spectrum of global conflict, there is another important aspect that must be examined to fully understand the impact of social media. What are the effects of social media conduct of individual members of the armed forces? The impacts of this truly unique aspect of modern civil-military relations are difficult to quantify but certainly have an impact.

In 2017, it was uncovered that the Facebook group "Marines United" contained a large collection of photographs involving nude female service members. The group, which had upwards of 50,000 members, was part of a broader investigation by the Naval Criminal Intelligence Service, analyzing over 131,000 images across 168 social media platforms.[80] Currently, 101 prosecutions have been completed, resulting in 11 courts-martials, 16 non-judicial punishments, 8 administrative separations, and 29 adverse administrative actions.[81] The Marine Corps scandal, although large in scale, highlights how seemingly simple an individual's choices and actions can become detrimental at a national level.

[79] Ripley, "War of Words – Social Media as a Weapon in Libya's Conflict," 16-19.

[80] Hope Hodge Seck, "11 Troops Kicked Out After Court-Martial in Wake of Marines United Scandal," Military.com, September 13, 2018, https://www.military.com/daily-news/2018/09/13/11-troops-kicked-out-after-court-martial-wake-marines-united-scandal.html.

[81] Ibid.

Furthermore, home-station social media use can be exploited operationally. H.I. Sutton's "Social Media Posts Reveal Submarine Deployments" shows how social media analysis can provide details for even the most covert activities. For example, when an open source intelligence (OSINT) analyst discovers a submariner on social media they can immediately exploit that profile to draw further intelligence. Simple online interactions, such as liking or commenting on an image, create social media patterns of life.[82] Friend lists can be exploited, especially in close-knit communities like submarine crews, to find further members.[83] When those patterns of life go silent, it can be deduced that the crew is underway. Online activity from different regions or ports provide geographical intelligence while length of inactivity can provide evidence of crew experience.[84] Although the intelligence collected demands a high level of scrutinization, it is valuable enough that nations are willing to dedicate the assets required.

Kathryn Coronges, Evan Szablowski, and Chris Arney look at the positives of a social media savvy military in "Generation 2.0:: Social Media and the Future of the Army".[85] Their article examines how a younger generation of soldiers use social media and, most importantly, that they provide fresh experiences and intelligence regarding social media. Younger soldiers are indoctrinated with social media as part of their daily

[82] H. I. Sutton, "Social Media Posts Reveal Submarine Deployments," *Jane's Intelligence Review* (2017): 4.

[83] Ibid., 5.

[84] Ibid., 4.

[85] Kathryn Coronges, Evan Szablowski, and Chris Arney, "Generation 2.0: Social Media and the Future of the Army," *Phalanx* 45, no. 1 (March 2012): 27-29.

lives. They expect when they join the military that they will work with premier technology, yet this is not always the case.[86] The authors believe the military would be wise to analyze how a younger generation utilizes social media platforms to communicate.[87] Simply put, new soldiers are a relatively untapped resource of tactics and intelligence. The article alludes to the cultural differences of military society and online society, cautioning that social media communication is horizontal, as opposed to the vertical communication utilized in Unity of Command.[88] According to Coronges, Szablowski, and Arney, there are five effects of social media:

1. Interactive experiences, the ability to report and respond to events as they unfold.
2. Integration of information, from news to friend activity.
3. Widespread audience, exchanges with entire groups at once.
4. Data immediacy have access to information in real time.
5. Usability, logical and simple computer interfaces.[89]

These effects have potentially positive outcomes with regards to military operations. However, the authors counter with five fundamental issues with social media.

1. Quantity of information.
2. Open access to secure information.
3. Validation of information.

[86] Coronges, Szablowski, and Arney, "Generation 2.0: Social Media and the Future of the Army," 27.

[87] Ibid.

[88] Ibid., 28.

[89] Ibid., 27.

4. Speed of exchanges.
5. Security.[90]

The article concludes by embracing social media as a means for revolutionary communication and proposes that communicating differently enables thinking differently.[91]

Each branch of service within the Department of Defense provides public social media guidance. These are formatted differently across each service but provide very similar messages. Whether the guidance comes in the form of a regulation or a handbook, the primary theme is individual online conduct.

As the Marine Corps scandal shows, the modern individual soldier is capable of damaging the image of the US military. Public perceptions can be warped through improper or immature posts. Carelessness with social media posting or privacy settings could be exploited by enemy forces. Therefore, the services have placed heavy emphasis in online conduct.

Currently, the Army has the most modern, user-friendly social media guidance available. Previously a PDF, the Army switched to a website format in 2016.[92] The website provides hyperlinks to the following policies and guidance:

1. ALARACT 058/2018 – Professionalization of Online Conduct

[90] Coronges, Szablowski, and Arney, "Generation 2.0: Social Media and the Future of the Army," 28.

[91] Ibid., 29.

[92] U.S. Army, "Army Social Media: Policies and Resources," accessed January 24, 2019, https://www.army.mil/socialmedia/?from=st2.

2. HASC Hearing on Social Media Policies
3. Tri-signed Letter: Online Conduct
4. Social Media and the Hatch Act
5. DODI 8550.01 – DOD Internet Services and Internet-based Capabilities
6. Disposition of Official Social Media Accounts
7. Secretary of the Army Memo – Delegation of Authority Approval of External Official Presences
8. DOD 1344.10 – Political Activities by Members of the Armed Forces
9. AR 600-20 – Army Command Policy
10. DODI 1300.18 – Personnel Casualty Matters, Policies, and Procedures

Guidance on Transition and Archiving of Official Social Media Accounts

Additionally, there is mandatory online training on securing and online identity and maintaining OPSEC, as well as frequently asked questions and other resources.[93]

The Air Force published a formal regulation, Air Force Instruction (AFI) 35-107 "Public Web and Social Communication". The AFI is a regulatory document which details social media conduct for airmen. Much of the AFI includes approval authorities and guidance for organizational webpages. Chapter 4, "Organizational Social Media Guidance", gives commanders left and right limits for creating their own unit social media pages. Of note, the Air Force permits social media pages at the wing, typically the

[93] U.S. Army, "Army Social Media: Policies and Resources."

installation-level organization, and above. Groups and squadrons must demonstrate a requirement to the Public Affairs office for a need to have a social media page.[94]

Chapter 5, "Personal Use Social Media Guidance", addresses the individual's roles and responsibilities. The chapter is only one and a half pages and includes generic information about online conduct. For example, airmen are reminded not to post hateful or defamatory comments. However, no specific guidance is given in chapter 5 about how to manage your digital footprint or how to ensure location services on specific means are disabled.[95]

The Marine Corps provides a large document titled "Marine Corps Social Media Principles". Although extensive and detailed, this publication avoids the formality of the AFI and the savviness of the multi-linked Army webpage. Although the similar principles of online conduct are covered, the Marine Corps guide gives the reader meticulous instructions for specific social media forums. For example, a list of online applications which access and share your personal data is provided.[96] Additionally, the Marines give a thorough description of Facebook tracking, how to set your privacy, and how to review and manage photo tags on the social media site.[97]

[94] Secretary of the Air Force, Air Force Instruction 35-107, *Public Web and Social Communication* (Washington, DC: Department of the Air Force, March 15, 2017), 21.

[95] Ibid., 27-28.

[96] U.S. Navy Office of Information, Chief of Information, "The Social Corps: The U.S.M.C. Social Page," U.S. Navy, accessed January 8, 2020, https://www.navy.mil/ah_online/opsec/docs/Policy/Marines-Social-Media-Handbook.pdf, 9.

[97] Ibid., 12-13.

The Navy combines the webpage approach of the Army along with a handbook published in 2019. The handbook is very detailed, providing guidance on social media accounts and OPSEC for leaders, sailors, families, ombudsmen, and civilians.[98] The webpage has a link to the handbook, as well as training and reporting procedures.[99]

The differences in delivery of social media education is noteworthy, but not overly significant. Each service has their own culture, and different forums are necessary to reach different members. What is worth noting, however, is the level of information provided in the basic documents or home pages. In this case, the Marine Corps sets the standard for simple and direct communications for conducting online activities.

Conclusion

The literature concerning social media is vast and connectable to military operations, functions, and culture at almost any point. Operations in Israel, Libya, Iraq and Syria, Ukraine, and Russia have exposed the great significance of this relationship. Additionally, Operational Security (OPSEC) compromises, scandals, and misuse across social media are an issue the military cannot ignore. Finally, there is an emerging call for embracing social media, especially with younger generations. The last point requires a serious look at the culture of the U.S. military. Regardless of the specific topic, literature regarding military operations and social media continues to expand.

[98] U.S. Navy Office of Information, Chief of Information, "The Navy Social Media Handbook," U.S. Navy, last modified March 2019, https://www.navy.mil/ah_online/opsec/docs/Policy/Navy_Social_Media_Handbook_2019.pdf.

[99] Ibid.

CHAPTER 3

RESEARCH METHODOLOGY

Research Design and Methods

The primary methodology conducted in this project is qualitative research analysis through the use of two case studies. Much of the qualitative analysis is broken down into content analysis, comparative study, and historical investigation. Unlike in some historical studies, there are no shortage of observers regarding this topic. For example, any military member or citizen who watched the news or read about ISIS could be regarded as a passive observer. Likewise, any military member with a social media account is in some ways an observing participant.

Analysis for this research is centered across two case studies. The case studies were selected specifically because they cover the effects of the broad social media spectrum. While both case studies detail social media conflict, the difference is where it originates, either foreign or domestic. The first case study is the Russian-Ukrainian conflict of 2013 to 2015. What started as student protests in November 2013 eroded into violence over the next year and half. Originally, students were protesting to force Ukrainian President Viktor Yanukovych and Prime Minister Mykola Azarov to sign an association agreement with the European Union.[100] The protests turned violent, and eventually led to Russian offensive action to annex Crimea and subversion in the eastern

[100] Andrey Kurkov, "Ukraine's Revolution: Making Sense of a Year of Chaos," *BBC News*, last modified November 21, 2014, https://www.bbc.com/news/world-europe-30131108.

Ukrainian region of Donbas. Social media, utilized by Ukrainians, Russians, and pro-Western forces, played a critical role within a very large information warfare campaign throughout the conflict. Russia's actions across this social media campaign were tactical, operational, and strategic. This case study is important because it provides a recent example of how social media can be utilized by a peer threat to inflict damage upon an enemy.

Equally as important as understanding how enemies can inflict damage upon the U.S., it is important to understand how self-inflicted wounds can occur due to social media. The second case study looks at the U.S. military and how social media can be detrimental to organizational trust. This study will look at multiple examples of miscues by military members on social media. The researcher chose to analyze more than one event in order to show a more complete picture of the impact.

In summary, the case studies highlight how an adversary can create effects through social media, and how a weapon as unique as social media can be used as a double-edged sword.

Data Gathering and Analysis

Social media is a vast realm of seemingly limitless data. Therefore, the researcher chose to focus primarily on two social media sites: Twitter and Facebook. Facebook continues to globally expand despite scandals throughout its past. In 2018, it was revealed that Facebook had shared unauthorized data from over 50 million individual profiles to Cambridge Analytica.[101] Some of this data was sold to Russia and used to

[101] The Guardian, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," accessed December 12, 2019,

target political audiences for the 2016 Presidential Election and the United Kingdom's Brexit referendum.[102] Although the scandal was a blow to Facebook's image, it did not hinder its popularity. As such, by the end of 2019 the number of Facebook users stands at nearly 2.5 billion.[103]

Twitter, by comparison, is much smaller with just 330 million users.[104] But Twitter is appealing for two reasons. First, Twitter disseminates information more rapidly. The average Twitter user spends 3.39 minutes per session as opposed to the nearly 5 minutes someone spends on Facebook.[105] Second, the majority of Twitter users are between the ages of 35 and 65.[106] This points to a target audience that is more mature and quite possibly in managerial or decision-making positions.

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[102] Ibid.

[103] J. Clement, "Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019," Statista, last modified January 30, 2020, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[104] Ying Lin, "10 Twitter Statistics Every Marketer Should Know in 2020," *Oberlo*, last modified November 30, 2019, https://www.oberlo.com/blog/twitter-statistics.

[105] Ibid.

[106] Ibid.

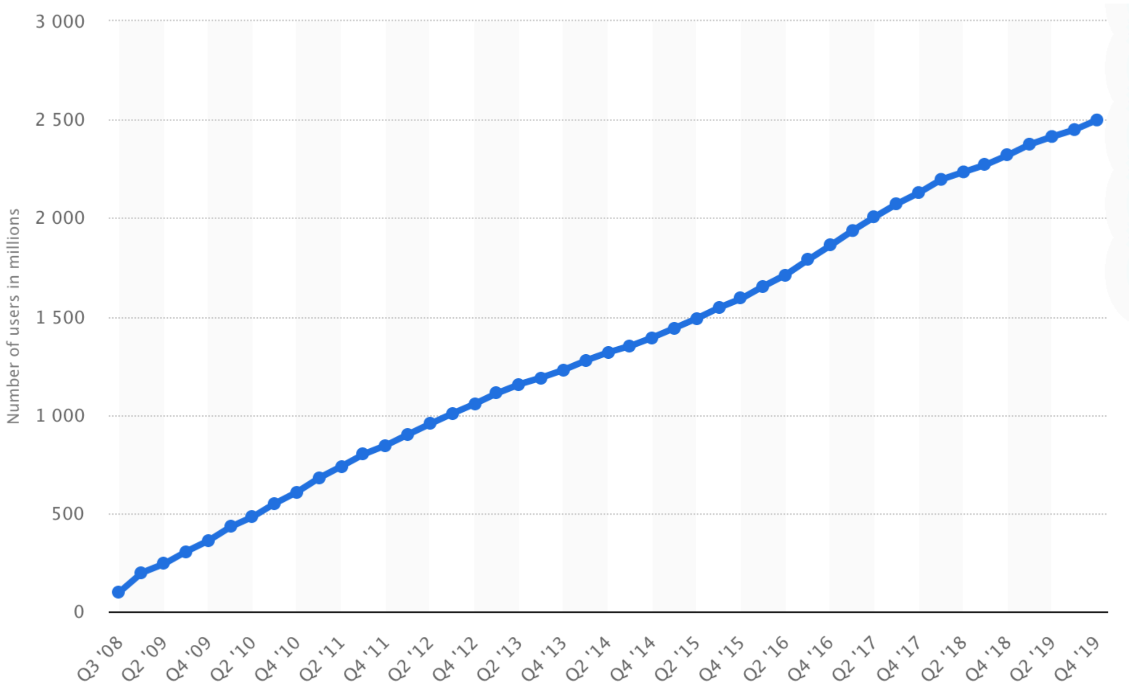


Figure 2. Facebook Users Worldwide as of 4th Quarter 2019

Source: J. Clement, "Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019," Statista, last modified January 30, 2020, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Conclusion

Due to the sheer size of the data available, much of the research is conducted through comparative analysis of professional studies and reports as applied to each case study. Analytical research teams provide published quantitative data available in print and online. However, raw data from Twitter and Facebook can also be analyzed. The goal of the analysis in chapter four is to synthesize that data into factual conclusions and recommendations.

CHAPTER 4

ANALYSIS

Case Study One – Ukraine

The history between Ukraine and Russia is significant. Over a thousand years ago Kiev stood as the capital of the first East Slavic state. The Mongol invasion of 1240 witnessed the destruction of Kiev and transplantation of the capital to Moscow. For centuries following, Ukrainian lands passed through foreign rulers such as Lithuania, Poland, and the Austro-Hungarian Empire.[107] After World War One, Ukraine declared itself an independent state. However, the Soviet Union incorporated Ukraine in 1922. The next few decades witnessed much suffering in Ukraine. Josef Stalin murdered Ukrainians who would not farm collectively.[108] The German invasion during World War Two was initially greeted with praise by Ukrainians, but was followed by massacres at the hands of both the Nazis and the Soviets, where an estimated 5.3 million Ukrainians died.[109] In 1991, Ukraine achieved its independence after the fall of the Soviet Union. Tensions, however, persist for many reasons. Economically, Ukraine has fertile farmland and is a big market for Russian natural gas exports, there are 7.5 million ethnic Russians living in

[107] Theunis Bates, "Ukraine's Fraught Relationship with Russia: A Brief History," *The Week*, last modified March 8, 2014, https://theweek.com/articles/449691/ukraines-fraught-relationship-russia-brief-history.

[108] Ibid.

[109] Ibid.

Ukraine, and geographically, the plains of Ukraine are a gateway to Europe and the Black Sea.[110]

In November 2013, civilian protests erupted in Kiev when President Viktor Yanukovych denied an opportunity for increased economic integration with the European Union. Yanukovych's security forces responded violently, emboldening the protestors and achieving the unintended effect of escalating the conflict.[111] As the protests continued, Russia exploited the all too convenient opportunity. Arguing the need to protect Russian speakers and Russian citizens in Ukraine, Russia seized Ukrainian sovereign territory on the Crimean Peninsula in the Black Sea. Furthermore, Russia supported, incited, and participated in rebel activities in the eastern provinces of Donetsk and Luhansk. The bloody conflict continues today, bearing witness to massive artillery bombardments in eastern Ukraine and the downing of a civilian airliner that killed 298 innocent civilians. Current Ukrainian estimates state 10,300 people killed with 24,000 injured.[112] The conflict in Ukraine has played out over social media in many different ways. It provides an excellent opportunity for analysis of social media conflict in the twenty first century.

A core theory taught at the Russian Military Institute of Foreign Languages known as *spetspropaganda* (special propaganda) was removed from the curriculum

[110] Bates, "Ukraine's Fraught Relationship with Russia: A Brief History."

[111] Global Conflict Tracker, "Conflict in Ukraine," Council on Foreign Relations, accessed February 12, 2020, https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-ukraine.

[112] Ibid.

following the collapse of the Soviet Union.[113] As the internet became more common following the turn of the millennium, *spetspropaganda* was reintroduced as a subject. [114] Igor Panarin, a diplomatic professor at the Institute, teaches the new Russian doctrine. He believes that Russia was truly created in 1999 by Vladimir Putin under a new ideological triad of spiritual, state, and cyber sovereignty.[115] It is his belief that the American-British Empire is failing and should be counter-balanced through a new Eurasian-Ruthenia empire stretching from Egypt to China, with Russia at the center.[116]

At the ideological center of Russian information warfare is the concept of netcode. Netcode is an information management process of certain groups, such as ethnicities or nationalities, to effect conflict favorable to their own cause.[117] Although the terminology is different, Russian doctrine is centered upon the theory of reflexive control.

Still, Ukraine stands as a significant object in the way of the Eurasian dominance Russia seeks. Aleksandr Dugin states that "cultural differences do not always coincide with territorial divisions; in this case the division line will cut through the territory, the land. We have always wanted this line to run as close to the west as possible, while the geopoliticians in Washington are trying to find a way to push it as much to the east as

[113] Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View* 42, (May 2014): 9, https://www.osw.waw.pl/sites/default/files/the_anatomy_of_ russian_information_warfare.pdf.

[114] Ibid.

[115] Ibid., 19.

[116] Ibid., 17.

[117] Ibid., 19-20.

possible. This is what the Ukrainian issue is like. Anyone who says it is not like this is either being diplomatic or is not sufficiently informed."[118] Dugin outlines three scenarios for Ukraine. The first is an east-west divided Ukraine caused by a civil war. The second scenario preys on a Ukraine that is struggling, either politically, socially, or economically, and that has a government in-place favorable to joining with Russia to achieve better conditions. The final scenario is a Ukraine that can be willingly convinced to join Russia by appealing to Ukrainian nationalists as an ally rather than a foe.[119] All of these scenarios are easily exploitable through information warfare. The reemergence of *spetspropaganda*, especially through social media, ensures this domain of battle.

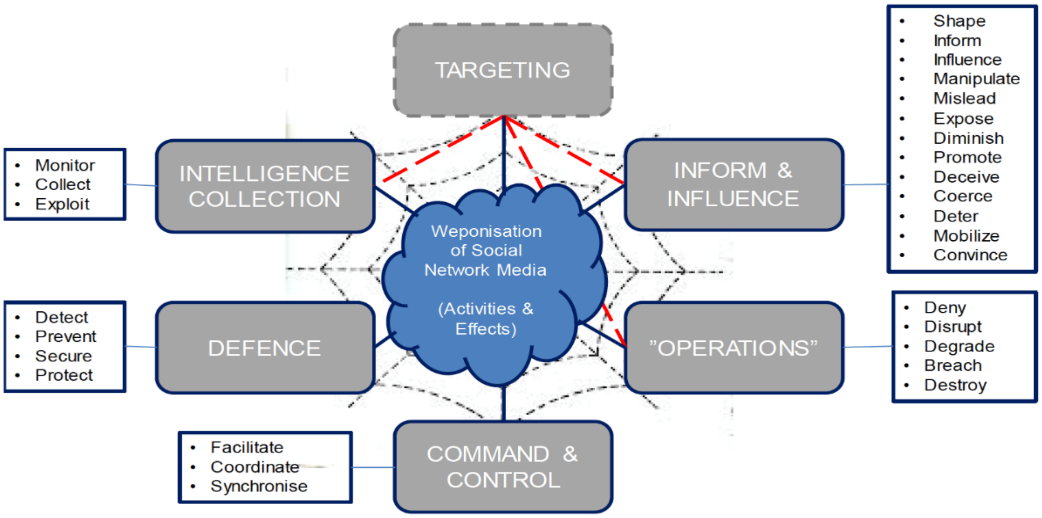


Figure 3. Activities and Effects Framework by T. E. Nissen

Source: Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare* (Riga, Latvia: NATO Strategic Communication Center of Excellence, May 2016), 11.

[118] Darczewska, "The Anatomy of Russian Information Warfare," 21.

[119] Ibid., 21-22.

Social media represents a revolutionary new tool to conduct information warfare. The internet is a willing host for Russian operations across Ukraine. Social media, however, is a double-edged sword. Dugin is one of many actors in charge of a multitude of pro-Kremlin websites and social media teams employing internet swarm tactics across websites such as http://ruxpert.ru, http://kontra20.ru, http://odna-ko.org, http://ruska-prawda.com, http://politrash.ru.[120] In Russia, where the state controls the media, this is easy to coordinate. But the internet is a mechanism where both sides are afforded equal exploitation. Therefore, after years of Russian information warfare in Ukraine, the November 2013 protests opened up a new battleground.

Twitter and Facebook became the two primary resources for information during the protests. The main protest hashtags, as tracked by New York University, captured 3.6 million tweets within the first three months alone, whereas the main protest Facebook page had been liked over a million times.[121] By comparison, the population of Kiev is 2.9 million.[122] Although all the "likes" probably did not come from Kiev alone, the figure still represents that a population one-third the size of the entire city had actively professed support through social media.

[120] Darczewska, "The Anatomy of Russian Information Warfare," 30.

[121] Megan Metzger and Pablo Barbera, "SMaPP Lab Data Report: Ukraine Protests 2013-2014" (New York University, New York, NY, 2014), https://wp.nyu.edu/smapp/wp-content/uploads/sites/1693/2016/04/Ukraine_Data_Report.pdf, 1-2.

[122] Central Intelligence Agency, "The World Factbook: Kiev," accessed February 18, 2020, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/up.html.

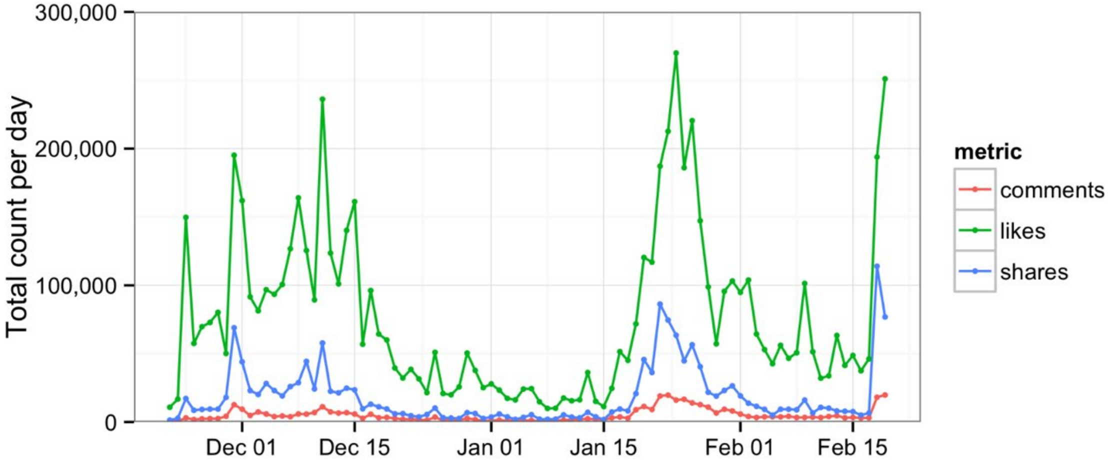


Figure 4. Facebook Activity through February 20th

Source: Megan Metzger and Pablo Barbera, “SMaPP Lab Data Report: Ukraine Protests 2013-2014” (New York University, New York, NY, 2014), https://wp.nyu.edu/smapp/wp-content/uploads/sites/1693/2016/04/Ukraine_Data_Report.pdf, 3.

The languages used on social media paint a picture of the means used to achieve the end state. The main protest Facebook page communicated in Ukrainian. It appears that Facebook was used as a domestic messaging system, providing alerts, information, maps, and warnings to protestors.[123] Twitter, on the other hand, witnessed much more disparity in language usage. Figure 5 and Figure 6 display languages used on Twitter for the first week of protests compared to the next three months.

[123] Metzger and Barbera, “SMaPP Lab Data Report: Ukraine Protests 2013-2014,” 2-4.

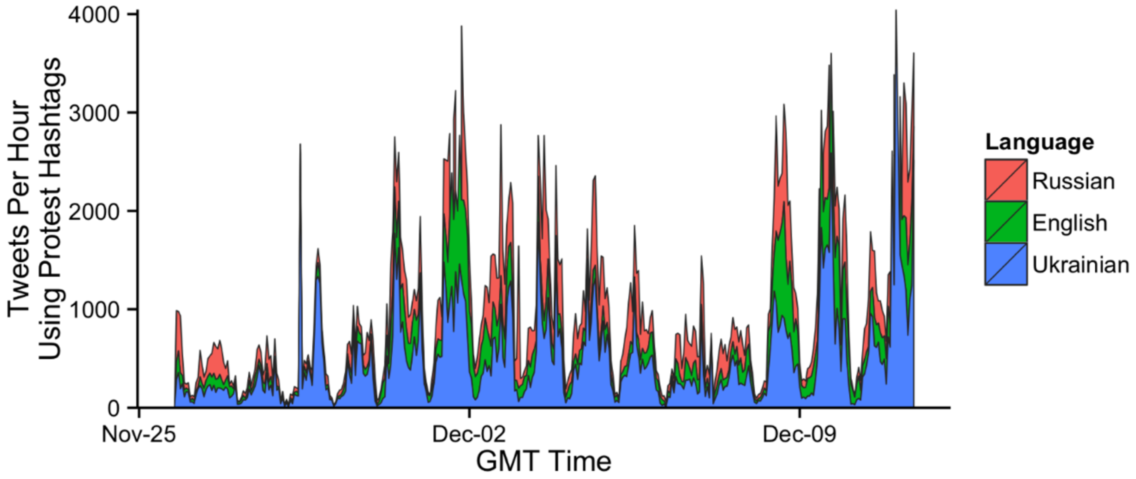


Figure 5. Linguistic Distribution of Tweets through December 11th

Source: Megan Metzger and Pablo Barbera, "SMaPP Lab Data Report: Ukraine Protests 2013-2014" (New York University, New York, NY, 2014), https://wp.nyu.edu/smapp/wp-content/uploads/sites/1693/2016/04/Ukraine_Data_Report.pdf, 5.

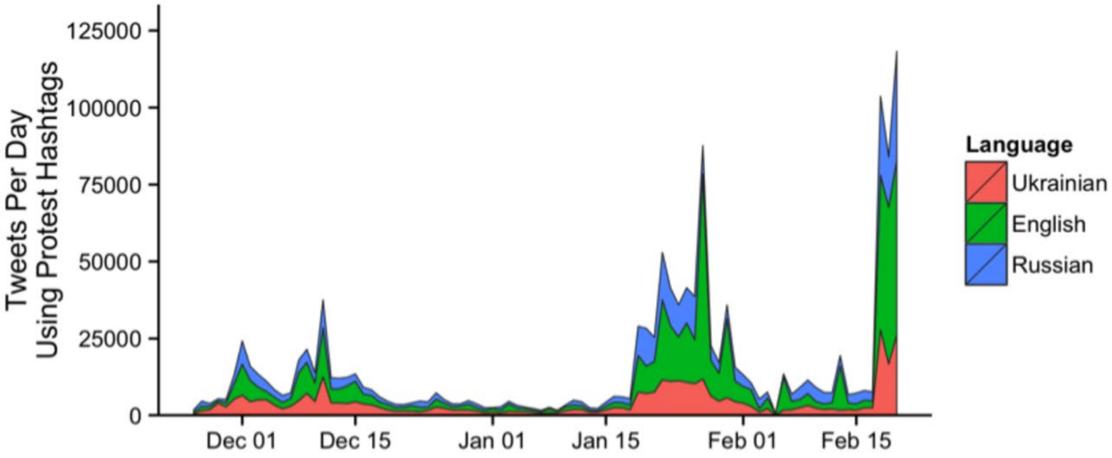


Figure 6. Linguistic Distribution of Tweets through February 21st

Source: Megan Metzger and Pablo Barbera, "SMaPP Lab Data Report: Ukraine Protests 2013-2014" (New York University, New York, NY, 2014), https://wp.nyu.edu/smapp/wp-content/uploads/sites/1693/2016/04/Ukraine_Data_Report.pdf, 7.

The comparison shows that as the protests grew, the international audience became more involved. Spikes in Russian tweets are often countered with spikes in English tweets. Although it is likely that this is evidence of international support, it is also possible that Ukrainians were tweeting in English as an appeal to western audiences.[124] Nearly 70 percent of Ukrainians speak Ukrainian, as opposed to 30 percent speaking Russian.[125] Therefore, the charts also highlight an unbalanced number of Russian tweets during peak events in the uprising.

The charts are essentially a map of a digital battlefield. There is clear evidence of a heavy Russian Twitter presence, shortly countered by Western information warriors. The data also shows that Twitter is a more conducive environment for a digital battle than Facebook. Twitter is a relatively open, unchecked forum with a free-fire zone of hashtags. Although Facebook is fair game, especially to point/counter-point arguments, owners of groups have more control over security and privacy settings, essentially screening involvement to more of a degree than Twitter.

Case Study Two – Domestic Social Media Impact

One of the most dangerous scenarios for military aviators is conducting evasive maneuvers at low altitude. When bullets or missiles are projecting towards an aircraft that is flying in its maximum performance envelope in close proximity to the ground, crews

[124] Metzger and Barbera, “SMaPP Lab Data Report: Ukraine Protests 2013-2014,” 6.

[125] Central Intelligence Agency, “The World Factbook: Ukraine,” accessed February 18, 2020, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/up.html.

must remember that although the enemy weapons are a threat, the ground carries a probability of kill (Pk) of 1. Simply put, if the aircraft smashes into the ground, the crew just completed the enemy's task for them. Social media carries similar risks across the information battlespace. Whether it is to be considered fratricide or a self-inflicted wound, the domestic activities of military members can achieve the same effects that the enemy desires.

Polish researcher Jolanta Darczewska describes Russian information warfare doctrine as "an old product in new packaging".[126] He goes on to explain that the Russian propaganda machine is an incredible system utilizing Soviet tactics applied to modern networks. "Propaganda", he says, "remains the key instrument of information warfare. Its distinctive features are language (the language of emotions and judgments, and not of facts), content (compliance with the Kremlin's official propaganda) and function (discrediting the opponent)."[127] Social media can rapidly deliver all of these distinctive features, but it doesn't necessarily require Russian teams to employ.

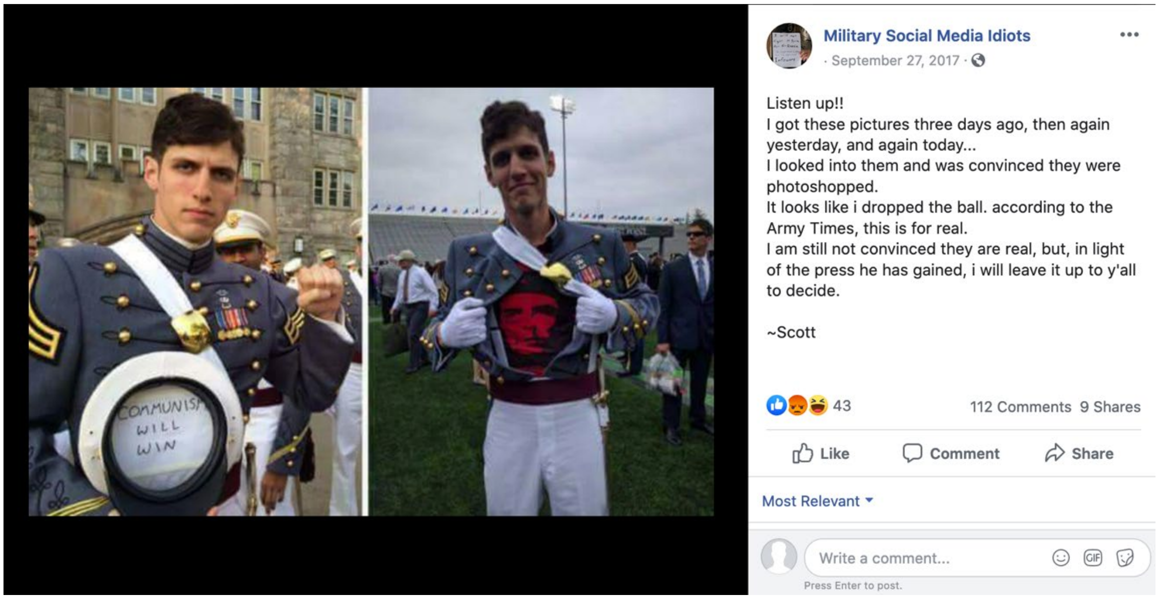
Spenser Rapone delivered for Russia when he graduated from the U.S. Military Academy at West Point in 2016. Rapone posted pro-communism photos at graduation, such as wearing a Che Guevara shirt under his uniform. An investigation soon followed and Rapone received another-than-honorable discharge from the army in 2018.[128] Prior

[126] Darczewska, "The Anatomy of Russian Information Warfare," 34.

[127] Ibid.

[128] Alex Horton, "A West Point Grad Wrote Communism Will Win in His Cap. The Army Kicked Him Out," *The Washington Post*, accessed March 13, 2020, https://www.washingtonpost.com/news/checkpoint/wp/2018/06/19/a-west-point-grad-wrote-communism-will-win-in-his-cap-the-army-kicked-him-out/.

to social media, it is imaginable that this story would have barely made news. But with the advent of social media, it went viral. The effect plays to the emotions of Russian strategy and discredits the image of the U.S. military as unified.



Military Social Media Idiots
· September 27, 2017 ·

Listen up!!
I got these pictures three days ago, then again yesterday, and again today...
I looked into them and was convinced they were photoshopped.
It looks like i dropped the ball. according to the Army Times, this is for real.
I am still not convinced they are real, but, in light of the press he has gained, i will leave it up to y'all to decide.

~Scott

Figure 7. Spenser Rapone on the "Military Social Media Idiots" Page of Facebook

Source: Military Social Media Idiots, Facebook, September 27, 2017, https://www.facebook.com/Military-Social-Media-Idiots-1448783588687036/.

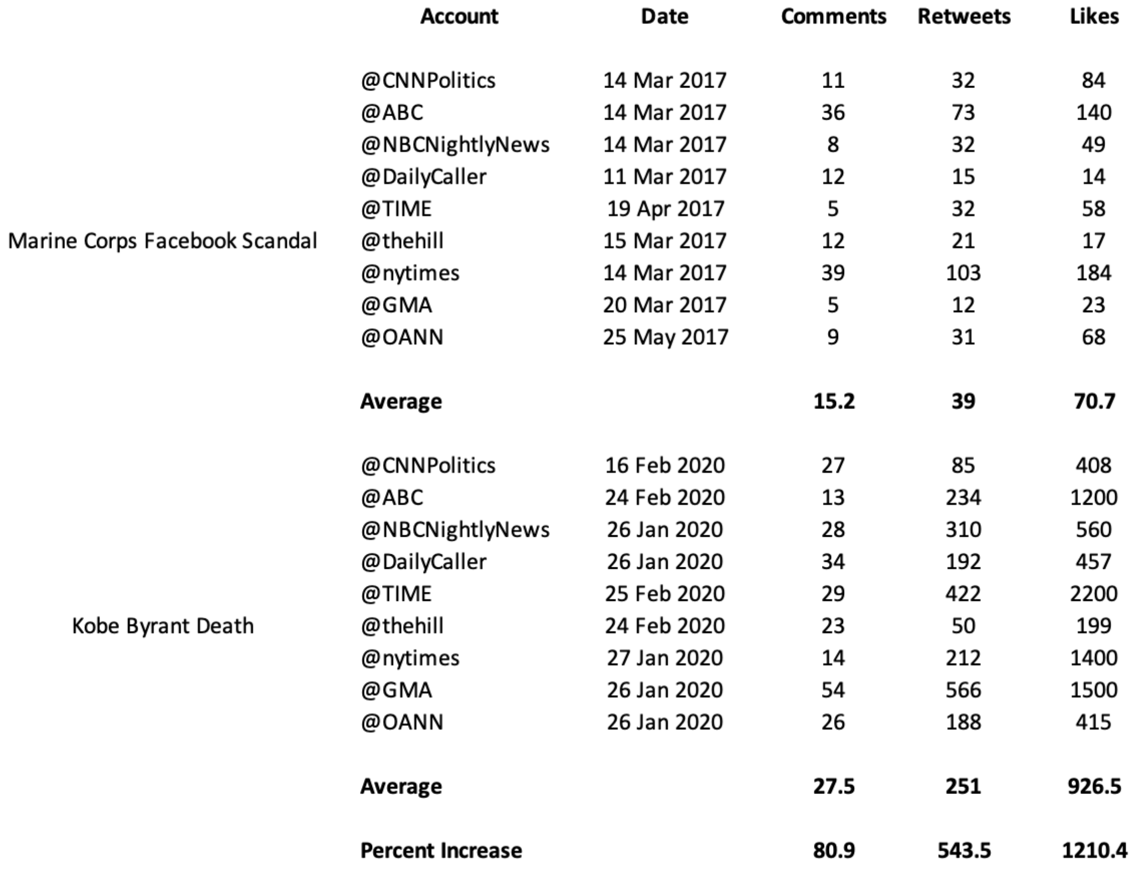
Furthermore, the court of public opinion often utilizes social media to channelize and project those emotions. Simply put, social media is the barometer that measures the effect. As evidence, the Facebook page "Military Social Media Idiots" has 22,165 followers and 22,605 likes.[129] Comparatively on Facebook, "Military Social Media

[129] Military Social Media Idiots, Facebook, September 27, 2017, https://www.facebook.com/Military-Social-Media-Idiots-1448783588687036/.

Heroes" has 2,294 followers and 2,314 likes.[130] While the numbers of followers is significant, it pales in comparison to the size of the user population on Facebook.

Rapone's actions garnered national attention, but he could be dismissed as one bad apple. The sheer size of the Marine Corps Facebook scandal potentially exposed a larger cultural problem within the service. Accordingly, the story attracted more attention than Rapone's. A Twitter search of "marine corps scandal" returns many articles as well as Senator Kirsten Gillibrand's grilling of General Robert Neller, Commandant of the Marine Corps. Retweets and Likes on Twitter can also help measure the impact of a story. The chart below compares Twitter activity from the Marine Corps Facebook scandal to Tweets surrounding the death of basketball star Kobe Bryant. News sources were selected for consistency in audiences. Sports accounts, such as ESPN, generated much higher interest in the Kobe Bryant news and generally do not address military social media activity.

[130] Military Social Media Heroes, Facebook, https://www.facebook.com/Military-Social-Media-Heroes-1380467095561943/.



	Account	Date	Comments	Retweets	Likes
Marine Corps Facebook Scandal	@CNNPolitics	14 Mar 2017	11	32	84
	@ABC	14 Mar 2017	36	73	140
	@NBCNightlyNews	14 Mar 2017	8	32	49
	@DailyCaller	11 Mar 2017	12	15	14
	@TIME	19 Apr 2017	5	32	58
	@thehill	15 Mar 2017	12	21	17
	@nytimes	14 Mar 2017	39	103	184
	@GMA	20 Mar 2017	5	12	23
	@OANN	25 May 2017	9	31	68
	Average		**15.2**	**39**	**70.7**
Kobe Byrant Death	@CNNPolitics	16 Feb 2020	27	85	408
	@ABC	24 Feb 2020	13	234	1200
	@NBCNightlyNews	26 Jan 2020	28	310	560
	@DailyCaller	26 Jan 2020	34	192	457
	@TIME	25 Feb 2020	29	422	2200
	@thehill	24 Feb 2020	23	50	199
	@nytimes	27 Jan 2020	14	212	1400
	@GMA	26 Jan 2020	54	566	1500
	@OANN	26 Jan 2020	26	188	415
	Average		**27.5**	**251**	**926.5**
	Percent Increase		**80.9**	**543.5**	**1210.4**

Figure 8. Twitter Comparative Analysis of News Stories

Source: Created by author.

The table shows significantly more interest in the Kobe Bryant story compared to the Marine Facebook scandal. It is important to note that the events took place three years apart, and Twitter's usage has grown since 2017. However, the data still provides a measure of which event was followed more closely.

Conclusion

Evidence clearly demonstrates significant social media interconnectivity with today's military. The Ukraine case study highlights the usage of social media across all instruments of national power in an attempt to affect outcomes. This campaign plays out from the tactical to the strategic level. The actions of military members on social media also have an impact. However, evidence suggests that the level of impact may not be as deep as is often portrayed. Regardless, the data highlights a growing reliance on social media and commanders must accept its emerging capabilities as a standard.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

Modern conflict exists throughout social media. Information warfare is conducted across various means of social media prior to any shots being fired. Battlespace is shaped, lines are drawn, and passions are exploited twenty-four hours a day. The power that social media yields must not only be accounted for but utilized and exploited.

Because social media can be viewed as a continual, uninterrupted information operations tool, it is easy to relegate social media to the gray space of conflict. Dr. Frank Hoffman describes the gray zone as “deliberate multidimensional activities by a state actor just below the threshold of aggressive use of military forces. In such conflicts, adversaries employ an integrated suite of national and subnational instruments of power in an ambiguous war to gain specified strategic objectives without crossing the threshold of overt conflict.”[131] Without a doubt, social media is active in the gray space of conflict. But what makes social media unique is its ability to transcend the full spectrum of conflict.

[131] Frank Hoffman, “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War,” in *Index of Military Strength: Assessing America’s Ability to Provide for the Common Defense,* ed. Dakota L. Wood (Washington, DC: The Heritage Foundation, 2016), 26, https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf.

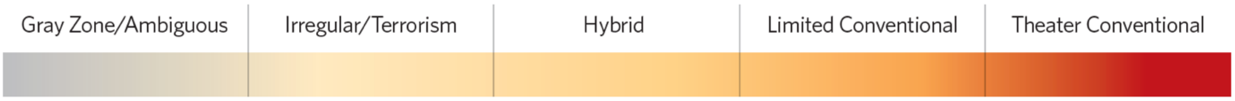


Figure 9. Spectrum of Unconventional Warfare

Source: Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in *Index of Military Strength: Assessing America's Ability to Provide for the Common Defense,* ed. Dakota L. Wood (Washington, DC: The Heritage Foundation, 2016), https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf, 29.

According to Figure 8, the gray zone is only one end of the spectrum. The research has shown that social media is a factor across the entire spectrum. It is true that the impacts of social media will vary in different types of conflict. For example, theater conventional war between two world powers could expect major disruption to internet accessibility. But the Libyan rebels showed the adaptability of social media even in the face of connectivity restrictions. Likewise, day to day counterinsurgency operations in eastern Afghanistan might appear to have little reliance on social media. However, the rise of ISIS throughout the region is partially attributed to a social media campaign.

Furthermore, social media blurs the lines between the instruments of national power. It is conceivable that social media should be categorized with information operations. But the messaging and influencing on social media effects diplomacy, economic actions, and military power. It is now more imperative than ever that all four instruments work in conjunction with one another to achieve objectives.

The literature of chapter two and analysis of data in chapter four made some conclusions very clear while others maintain a certain level of ambiguity. The topic of social media, cyber warfare, and online information operations has exploded over the last decade. The conclusions below are intended to provide a field grade leader without a cyber operations background with some basic knowledge of social media's role in the modern military.

The Research Questions

Research Question One: How should the U.S. military embrace social media as a means to achieve military objectives?

Social media is a dynamic tool that can assist in the support of military objectives at all levels. In its most simple form, social media is an efficient, cheap, and broad way to communicate. In garrison, social media should be utilized routinely to facilitate open communication with local communities. Twitter and Facebook have become a language of their own, and it is a language that spans generations as well as ethnicities and backgrounds. The military needs to speak this language better. The Israeli example in Chapter 2 highlights the potential destruction of using it as a tool but not understanding the audience or potential consequences.

Furthermore, social media is a recruiting tool. As the military emerges from decades of counterinsurgency and focuses on large scale combat, the size of the force will be assessed and, according to many, should be increased. Recruiting the right people starts with social media. A new generation is entering the force. This generation grew up with social media as a part of their lives from the start. They speak the digital language and understand its importance. Not only is social media an effective recruiting tool, but it can attract the types of people the military wants for the next generation fight.

In order for the recruiting and communication piece to be fully successful, the military must loosen the reigns and allow commanders at the O-5 level and below to have their own organizational Twitter, Facebook, and Instagram accounts. The current Air Force policy of wing level and above is too restrictive. Squadrons, battalions, and other organizations are entrusted with multi-million-dollar budgets and large amounts of manpower and equipment. A younger generation of leaders is more than capable of posting daily training photos to Instagram. This level of dissemination takes away from the stiff, hierarchical messaging of senior-level accounts and enables genuine, honest posting. The reward for this delegation outweighs the risk. Social media is most effective in the gray space of conflict. The gray space could include home station operations as well as international exercises. Therefore, service guidance must be tailored for flexibility while being more specific.

During war, the social media tool is exceptionally useful for information gathering. That being said, the average operational major or lieutenant colonel is not focusing their efforts on Twitter during combat operations. Just as reasonable, localized information passed across social media is not likely to reach the lower echelon units that it will affect. Therefore, squadron and battalion intelligence units should employ a social media analyst. This position should be fielded by a social media savvy analyst who is capable of adapting to the mission of the unit. Furthermore, there are many examples of social media compromising military units. Differing standards across individual units have enabled this issue. The Department of Defense need not apply one directive to the whole force, but service chiefs must provide clear guidance. For example, submariners do not take cell phones while underway, but many aircrews fly with phones as a potential rescue device. Setting a standard for organizations within each department of service would help avoid potentially costly errors.

The U.S. military seems to value the importance of social media. But current guidance does not channel its effectiveness. The following recommendations should be considered:

1. Official social media accounts should not be restricted to the O-6 level. Embrace O-5 and below usage of Instagram and Facebook for home station/garrison operations.
2. During international exercises and non-combat deployments, social media posts must be approved by unit social media analyst.
3. During combat deployments, social media usage is not allowed except for social media analysts and cyber warfare experts.

Research Question Two: Is social media a weapon of war?

Yes. Social media is a modern weapon used to achieve results across all spectrums of conflict. The results can be tactical, such as coercing individuals to induce physical harm in forms of terrorism or subversive attacks. The results can be operational, such as tweeting coordinates to NATO to entice airstrikes. The results can be strategic or even national, such as influencing democratic elections through the use of purchased or stolen data. Social media does not fit the traditional sense of a weapon. The argument could be made that a Harris PRC-152 radio is not a weapon, or that communication nodes are targets, but not weapons. But social media does something that a cell phone tower or field radio does not; it plays to the emotions of people. Logic and reason need not be present on social media, but people can and will act upon the pathos provided by social media.

Another issue is the lack of distinction between social media platforms. Much as a Barrett .50 caliber rifle has a different effect than a Beretta 9-millimeter pistol, social media platforms are likewise unique. Facebook is a closed-door information forum. Its effects include networking and information sharing. Twitter is the massive central communication node with few restrictions, leveraging near-instantaneous worldwide information sharing. Instagram satisfies the sense of vision, making true the old saying "every picture is worth a thousand words". Guidelines should delineate specific social media platforms.

Defeating this weapon is not easily done at the military level. Certainly, internet infrastructure would be likely early targets in any large-scale combat operation. But Libyan rebels proved that even system shutdowns can be sidestepped. The answer lies within societies themselves: education. The best way to defeat online disinformation and belligerence is by educating the society.

Finland has been successful against Russian propaganda. Their education system, which is ranked number one worldwide, enhances critical thinking skills.[132] It's the ability to think critically, rather than passively accepting what is seen or heard, that destroys the Russian disinformation game plan. It is important to note that Finland's other main advantage is the homogeneity of their society, which is staunchly anti-Russian.[133] This presents more of a challenge for a diverse U.S. It is that diversity that makes it so vulnerable to online attacks. Russia targeted racial and social issues as well as other hot-

[132] Glenda Jakubowski, "What's Not to Like: Social Media as an Information Operations Force Multiplier," *Joint Forces Quarterly* 94 (3rd Quarter 2019): 13.

[133] Ibid.

button topics prior to the 2016 presidential election.[134] Other deployable countermeasures are tracking false news, working with social media sites to eliminate false advertisements and restrict user data, legal measures, and diplomacy.[135]

All of these measures are necessary to hold ground in a digital battle. However, the education of the society coupled with honest, upfront messaging from leadership will enable the critical thinking and trust required to overcome disinformation.

Recommendations:

1. The U.S. spends 5 percent GDP on education. This ranks 64 out of 175 countries.[136] The U.S. needs to invest more heavily in education in order to broaden critical thinking skills and counter online susceptibility in order to defeat reflexive control measures.
2. The U.S. government is obligated to protect its citizens from online attacks. Stricter legislation must be imposed to protect user data.

Research Question Three: Do domestic social media scandals of the U.S. military have strategic implications?

The Twitter and Facebook analysis of social media "black eyes" for the military revealed surprisingly low interest. Individuals will continue to embarrass themselves online, whether intentionally or not. The levels of public interest will vary based on the

[134] Jakubowski, "What's Not to Like: Social Media as an Information Operations Force Multiplier," 15.

[135] Ibid., 13-14.

[136] Central Intelligence Agency, "The World Factbook: United States," accessed February 18, 2020, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/us.html.

severity of the action, number of people involved, and who or what rank was involved. These unfortunate incidents are the exception rather than the norm. Most service members are doing the right thing on social media. The services have barraged young recruits with training and those efforts appear to be paying off. The mandatory classes and online training are having a positive effect, but more importantly there is a generation of young service members who have grown up understanding the consequences of social media.

These actions can still be detrimental to the service, but the data suggests that the level of impact is not as powerful as is sometimes suggested. Certainly, Russian propagandists rejoiced at the sight of a West Point cadet holding a sign saying that communism will win. But in the digital age attention spans are short. Surely, many Americans have no idea who Spenser Rapone is anymore.

What makes this topic pertinent is that leaders at all levels have an impact on individual actions of social media. The average field grade officer has little influence on strategic information warfare campaigns throughout the internet. However, a company or battalion commander who has a base of knowledge regarding social media and its impact can train, educate, and guide their soldiers to make smart decisions on social media. Regardless of regulations, young service members must be instructed about smart practice of social media at home. More importantly, leaders must take it upon to themselves to ensure smart practice during exercises and deployments. For example, disabling location services and leaving cell phones behind should be standard operating procedure for most combat organizations. The field grade leader cannot control what Russia disseminates on Facebook, but they can lead a group of intelligent and responsible troops. It is the researcher's opinion that current service guidance regarding home station social media usage is sufficient and does not require additional recommendations.

Recommendations for Further Study

This research project was conducted through a broad lens. It was essentially broken down into two parts, social media usage of our adversaries, and social media usage of individual service members. Each topic could be broken down and researched further.

The social media actions of our adversaries are as calculated and specific as they are dynamic. Further examination should be conducted on Soviet propaganda principles and how they are reappearing in modern Russia. The reemergence of these beliefs correlates directly to the application of social media. Additionally, the entire Ukrainian Euromaden conflict stands as an excellent example of modern hybrid warfare with a heavy emphasis on social media and information battles. Finally, social media is only as valuable as the connectivity upon which it relies. Researching contested/degraded operations (CDO) and how the future battlefield might look with degraded and jammed systems and equipment would be valuable. This topic, as well as social media and further propaganda warfare, would also be very useful in a classified format.

The issue of social media scandals at home ties directly with leadership studies. There is no shortage of case studies for moral and ethical leadership dilemmas, but what this study shows is that the world is digitally connected, and online verdicts are swift and brutal. It would be interesting to study the metrics of successful social media accounts of military leaders. For example, a successful page could be judged by how many likes, shares, and followers as well as how much information is passed. But furthermore, why?

Is it the background of the leader or the age? What is their target audience? This information could be used to assess who should be utilizing social media more heavily and who could pass.

Finally, as social media plays more of a role in conflict it will be important to define its status in the Law of Armed Conflict (LOAC). A further study could be conducted to help understand where social media fits in the LOAC. To what level do, or can, we destroy a nation's internet infrastructure both physically and through online attacks? This information would help define the left and right limits of campaign planners.

Conclusion

Social media is not simply an innocent social networking forum. Nor is it a digital devil which should be avoided at all costs. It is a staple of communication in the modern connected world. It will continue to play a pivotal role in our society and therefore the military must embrace its possibilities. The common theme throughout this research is education. Our service members must be educated by their leaders on social media conduct and consequences, both at home and abroad. Our leaders must be educated on our adversaries' capabilities and intentions through social media. But most importantly, Americans as a society must prioritize education. A more intelligent society, capable of applying critical thinking, will not take things at face value, but will study, compare, and understand the world better. That alone is the strongest weapon against social media warfare.

BIBLIOGRAPHY

Army, Marine Corps, Navy, Air Force. Air Force Tactics, Techniques and Procedures Publication 3-2.6, *JFIRE: Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower.* Joint Base Langley-Eustis, VA: Air Land Sea Application Center, October 2019.

Bates, Theunis. “Ukraine’s Fraught Relationship with Russia: A Brief History.” *The Week.* Last modified March 8, 2014. https://theweek.com/articles/449691/ukraines-fraught-relationship-russia-brief-history.

Beres, Damon. “Watch the Amazing Way Information Spreads on Twitter.” *HuffPost.* Last modified March 20, 2016. https://www.huffpost.com/entry/how-twitter-works.

Bialy, Beata. “Social Media: From Social Exchange to Battlefield.” *Cyber Defense Review* 2, no. 2 (Summer 2017): 69-90.

Bjola, Corneliu, and James Pamment. *Countering Online Propaganda and Extremism: The Dark Side of Diplomacy*. London: Routledge, 2019.

Brooking, Emerson T., and P. W. Singer. “War Goes Viral: How Social Media is being Weaponized.” *The Atlantic* (November 2016): 70-83.

Central Intelligence Agency. “The World Factbook.” Accessed February 18, 2020, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/up.html.

Chivvis, Christopher S. “Hybrid War: Russian Contemporary Political Warfare.” *Bulletin of the Atomic Scientists* 73, no. 5 (2017): 316-321.

Clement, J. “Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2019.” Statista. Last modified January 30, 2020. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Coronges, Kathryn, Evan Szablowski and Chris Arney. “Generation 2.0: Social Media and the Future of the Army.” *Phalanx* 45, no. 1 (March 2012): 27-29.

Darczewska, Jolanta. “The Anatomy of Russian Information Warfare,” *Point of View* 42, (May 2014). https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

Global Conflict Tracker. “Conflict in Ukraine.” Council on Foreign Relations. Accessed February 12, 2020. https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-ukraine.

Golovchenko, Yevgeniy, Mareike Hartman, and Rebecca Alder-Nissen. “State, Media and Civil Society in the Information Warfare Over Ukraine: Citizen Curators of Digital Disinformation.” *International Affairs* 94, no. 5 (September 2018): 975-994.

The Guardian. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” Accessed December 12, 2019. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Hoffman, Frank. “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War.” In *Index of Military Strength: Assessing America’s Ability to Provide for the Common Defense,* edited by Dakota L. Wood, 25-36. Washington, DC: The Heritage Foundation, 2016. https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf.

Horton, Alex. “A West Point Grad Wrote Communism Will Win in His Cap. The Army Kicked Him Out.” *The Washington Post,* June 19, 2018. https://www.washingtonpost.com/news/checkpoint/wp/2018/06/19/a-west-point-grad-wrote-communism-will-win-in-his-cap-the-army-kicked-him-out/.

Jakubowski, Glenda. “What’s Not to Like: Social Media as an Information Operations Force Multiplier,” *Joint Forces Quarterly* 94 (3rd Quarter 2019): 8-17.

Kurkov, Andrey. “Ukraine’s Revolution: Making Sense of a Year of Chaos.” *BBC News.* Last modified November 21, 2014. https://www.bbc.com/news/world-europe-30131108.

Lin, Ying. “10 Twitter Statistics Every Marketer Should Know in 2020.” *Oberlo*. Last modified November 30, 2019. https://www.oberlo.com/blog/twitter-statistics.

Merriam-Webster. “Weapon.” Accessed October 15, 2019. https://www.merriam-webster.com/dictionary/weapon.

Metzger, Megan, and Pablo Barbera. SMaPP Lab Data Report: Ukraine Protests 2013-2014.” New York University, New York, NY, 2014. https://wp.nyu.edu/smapp/wp-content/uploads/sites/1693/2016/04/Ukraine_Data_Report.pdf.

Military Social Media Heroes. Facebook. https://www.facebook.com/Military-Social-Media-Heroes-1380467095561943/.

Military Social Media Idiots. Facebook. September 27, 2017. https://www.facebook.com/Military-Social-Media-Idiots-1448783588687036/.

Reynolds, Anna, ed. *Social Media as a Tool of Hybrid Warfare.* Riga, Latvia: NATO Strategic Communication Center of Excellence, May 2016.

Rid, Thomas. "Cyber Weapons." *The RUSI Journal* 157, no. 1 (2012): 6-13.

Ripley, Tim. "War of Words – Social Media as a Weapon in Libya's Conflict." *Jane's Intelligence Review* 23, no. 9 (Summer 2011): 16-19.

Seck, Hope Hodge. "11 Troops Kicked Out After Court-Martial in Wake of Marines United Scandal." Military.com. September 13, 2018. https://www.military.com/daily-news/2018/09/13/11-troops-kicked-out-after-court-martial-wake-marines-united-scandal.html.

Secretary of the Air Force. Air Force Instruction 35-107, *Public Web and Social Communication.* Washington, DC: Department of the Air Force, March 15, 2017.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate, in the Digital Age.* New York, NY: Hachette Book Group, 2017.

Snegovaya, Maria. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare." Institute for the Study of War*,* September 2015. https://www.jstor.org/stable/resrep07921.1.

Sutton, H. I. "Social Media Posts Reveal Submarine Deployments." *Jane's Intelligence Review* (December 2017). https://janes-ihs-com.lumen.cgsccarl.com/Janes/Display/FG_693303-JIR.

U.S. Army. "Army Social Media: Policies and Resources." https://www.army.mil/socialmedia/?from=st2.

U.S. Army Training and Doctrine Command (TRADOC). TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028.* Fort Eustis, VA: TRADOC, December 6, 2018.

U.S. Navy Office of Information, Chief of Information. "The Navy Social Media Handbook." U.S. Navy. Last modified March 2019. https://www.navy.mil/ah_online/opsec/docs/Policy/Navy_Social_Media_Handbook_2019.pdf.

U.S. Navy Office of Information, Chief of Information. "The Social Corps: The U.S.M.C. Social Page." U.S. Navy. https://www.navy.mil/ah_online/opsec/docs/Policy/Marines-Social-Media-Handbook.pdf.

West, Levi J. "#jihad: Understanding Social Media as a Weapon." *Security Challenges* 12, no. 2 (2016): 9-26.