REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 20-04-2018	2. REPORT TYPE MASTER'S THESIS	3. DATES COVERED (From - To) 10-09-2017 - 20-04-2018

4. TITLE AND SUBTITLE

OPERATIONALIZING SOCIAL MEDIA: A METHOD FOR INCORPORATING SOCIAL MEDIA IN DEPARTMENT OF DEFENSE PLANS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Allison, Brett, A., LtCol, USMC

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College, Joint Advanced Warfighting School, 7800 Hampton Blvd, Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION 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

Reports of Russia's utilization of social media to influence the 2016 U.S. presidential elections demonstrated the power of social media. They also revealed that the U.S. is behind its adversaries in effective use of social media to influence targeted audiences and help set conditions for future operations. This thesis will examine factors of influence on social media networks and provide strategies for incorporating social media in operational plans. Before assessing potential strategies, the paper will define the social media environment and look at some principles marketers use to exert influence over consumers. Next, it will assess four case studies, two from business and two from adversaries. Finally, from the lessons learned in both marketing and adversarial actions, the paper will develop and demonstrate methods for incorporating social media through the Joint Planning Process using an operational example.

15. SUBJECT TERMS

Social Media, Influence, Information, Information Operations, Information Warfare, Department of Defense Planning, Joint Planning, Operational Environment

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE
U	U	U

17. LIMITATION OF ABSTRACT

SAR

18. NUMBER OF PAGES

42

19a. NAME OF RESPONSIBLE PERSON

LtCol Brett Allison

19b. TELEPHONE NUMBER (Include area code)

757-443-6301

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

OPERATIONALIZING SOCIAL MEDIA: A METHOD FOR INCORPORATING

SOCIAL MEDIA IN DEPARTMENT OF DEFENSE PLANS

by

Brett Allison

LtCol, USMC

BLANK

OPERATIONALIZING SOCIAL MEDIA: A METHOD FOR INCORPORATING

SOCIAL MEDIA IN DEPARTMENT OF DEFENSE PLANS

by
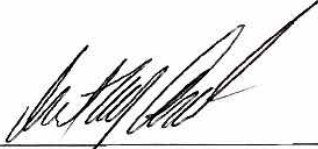
Brett Allison

LtCol, USMC

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: _____

20 April 2018

Thesis Advisor:

Signature: _____
Robert M. Antis, Ph.D.
Professor, Joint Forces Staff College

Approved by:

Signature: _____
Mary S. Bell, Ph.D.
Associate Professor of Practice,
Joint Forces Staff College

Signature: _____
Miguel L. Peko, Captain, US Navy
Director, Joint Advanced Warfighting School

BLANK

ABSTRACT

Reports of Russia's utilization of social media to influence the 2016 U.S. presidential

elections demonstrated the power of social media. They also revealed that the U.S. is

behind its adversaries in effective use of social media to influence targeted audiences and

help set conditions for future operations. This thesis will examine factors of influence on

social media networks and provide strategies for incorporating social media in

operational plans. Before assessing potential strategies, the paper will define the social

media environment and look at some principles marketers use to exert influence over

consumers. Next, it will assess four case studies, two from business and two from non-

state and state actors. Finally, from the lessons learned from marketing, non-state actors,

and state actors, the paper will develop and demonstrate methods for incorporating social

media through the Joint Planning Process using an operational example.

BLANK

<u>DEDICATION</u>

For my wife, Kim…the reason I have a Facebook account and discovered social media.

Table of Contents

BLANK

Introduction:

On January 12, 2012, a video of four Marine Scout Snipers urinating on and desecrating dead Taliban fighters in Afghanistan went viral on YouTube.[1] General Charles Krulak, 31st Commandant of the Marine Corps, coined the term "Strategic Corporal," describing future scenarios where the action of a single Marine "will potentially influence not only the immediate tactical situation, but the operational and strategic levels as well."[2] While former Army psychologist Bret Moore explained that demonstrating disdain for the enemy is normal, the actions of these four Marines were illegal and demonstrated the negative impact a "Strategic Corporal" can have at the operational and strategic levels.[3] Their actions offended not only enemies of the United States in Afghanistan, but also Muslims around the world, damaging relationships with U.S. allies.[4] The role that social media played in this event is significant and demonstrates the influence that social media has on the operational and strategic environment.

According to researchers Andreas Kaplan and Michael Haenlein, social media has been around since the late 1970s, when people shared information electronically through bulletin board systems and open diaries.[5] However, it was not until the early 2000s and

---

[1] Corey Flintoff, "Viral Images, the Military's Recurring Nightmare," National Public Radio, http://www.npr.org/2012/01/12/145117940/viral-images-the-militarys-recurring-nightmare?ps=cprs (accessed October 30, 2017).

[2] Charles Krulak, "The Strategic Corporal: Leadership in the Three Block War," Marine Corps Gazette Vol. 83, No. 1 (January 1999): 21, https://www.mca-marines.org/leatherneck/1999/01/strategic-corporal-leadership-three-block-war (accessed October 30, 2017).

[3] Flintoff.

[4] Ibid.

[5] Andreas M. Kaplan and Michael Haenlein, "Users of the World Unite! The Challenges and Opportunities of Social Media," Business Horizons, Vol. 53, No. 1, (January-February 2010): 60. http://www.sciencedirect.com/journal/business-horizons/vol/53/issue/1 (accessed October 31, 2017).

the creation of applications such as Java, that the collaborative internet world known as Web 2.0 introduced *social media*; media which allows near real-time conversations and collaborative postings.[6] Furthermore, social media applications have expanded beyond computer systems and are now also available in most countries through numerous media devices such as mobile tablets and cellular phones (to include both smart phones and more conventional cellular phones). As of 2009, it was estimated that over 75% of internet users were on social media, with the population of Facebook alone rivaling that of Brazil.[7] Today, one fifth of the world's population uses some form of social media either daily or weekly.[8] The global proliferation of social media technology provides increased connectivity between individuals and organizations.

As a media platform, social media provides unique opportunities for traditional organizations to interact with the private individuals. Businesses leverage social media to gain a better understanding of consumer desires as well as to market their products. Politically, both state and non-state actors have turned social media into a means to shape the environment by building biases and influencing regional populations to act favorably towards meeting their objectives. Extremist organizations have used social media to promote their ideas and recruit new followers, activists have capitalized upon social media's vast networking capabilities to mobilize people into action, and states have used social media to broadcast their messages and gauge popular opinion.

---

[6] Kaplan and Haenlein, 59-60.
[7] Ibid.
[8] Ravi Gupta, and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis: John Wiley & Sons, Inc., 2013), 19.

National leaders recently made two important decisions with regards to how the Department of Defense (DoD) handles information. First, the President of the United States elevated Cyber Command (CYBERCOM) to a separate unified combatant command no longer subordinate to Strategic Command (STRATCOM).[9] Second, the Secretary of Defense determined that *Information* should be a separate Joint Function, thus signaling "a fundamental appreciation for the military role of information at the strategic, operational and tactical levels within today's complex operating environment."[10] The June 2016 DoD Strategy for Operations in the Information Environment (IE) gives the following end state: "Through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations."[11] As the DoD continues to develop policies and procedures with regards to both CYBERCOM and *Information*, serious consideration needs to be given to the role of social media in attaining this end-state. This paper will examine how the Department of Defense may better integrate use of social media into its daily operations and written plans to gain influence and set conditions to increase national security.

There is already a body of literature surrounding social media and its use within the DoD. Many of the existing publications focus on Operational Security measures, to

---

[9] Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," Department of Defense News, https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ (accessed October 16, 2017).

[10] U.S. Secretary of Defense, *Information as a Joint Function,* Memorandum, (Washington DC: Department of Defense, 15 September 2018).

[11] U.S. Department of Defense, *DoD Strategy for Operations in the Information Environment* (Washington DC: Department of Defense, June 13, 2016), 2.

include articles and training found on the DoD's Chief Information Officer website.[12]

Other works discuss potential intelligence opportunities through social media analysis, such as RAND's 2017 study on social media analysis in support of Information Operations.[13] As the RAND study points out, there are legal considerations in conducting intelligence or information operations using social media, specifically the potential to cross between Title 10 (Armed Forces) and Title 50 (Intelligence) activities.[14] While legal considerations need to be more fully explored, they are not the focus of this study. The intent of this paper is to build upon existing ideas for social media strategies and incorporate them into effective use of *Information* focusing on social media to not only analyze online social networks, but also identify ways to exert influence on those networks and develop an overall strategy that uses social media to help set favorable conditions for future operations.

<div align="center">Method</div>

This paper will utilize the Case Study Method, a qualitative method that allows for detailed understanding of a particular case.[15] Four separate cases will be examined: two cases from the business world and two cases from recent events involving a non-state and a state actor, demonstrating both effective and ineffective social media engagements. By

---

[12] Chief Information Officer, "Social Media Education and Training," U.S. Department of Defense, http://dodcio.defense.gov/Social-Media/SMEandT (accessed January 2, 2018).

[13] William Marcellino, Meagan L. Smith, Christopher Paul, and Lauren Skrabala, "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations," (Santa Monica, CA: RAND Corporation, 2017), under "DoD Social Media," https://www.rand.org/pubs/research_reports/RR1742.html (accessed December 20, 2017), 8.

[14] Ibid., 55-57.

[15] Elia Shabani Mligo, *Introduction to Research Methods and Report Writing: A Practical Guide for Students and Researchers in Social Sciences and the Humanities*, (Eugene, OR: Resource Publications, 2016), under "Research Methods," https://ebookcentral.proquest.com/lib/nationaldefense-ebooks/detail.action?docID=4835551 (accessed October 31, 2017): 51.

understanding what is and is not effective in a variety of situations, entities within the DoD will be able to better use social media to inform and persuade its intended audience.

Before examining the case studies, this paper will provide background information on social media. This paper will provide a common definition for social media, describe the social media environment, and discuss influence factors. The background information provides the context for evaluating case studies.

The first two case studies come from business and marketing. Private corporations were some of the first to recognize the value of, and incorporate the use of social media into their strategies to influence consumer decisions. From these private industry cases, the DoD can learn how to better employ effective techniques to develop a better understanding of the market environment, find ways to influence through lessons learned in advertising, and how to better target their desired audience.

The second group of case studies come from recent global events that demonstrated how both a non-state and a state actor employed social media to help shape the environment and attain their goals. A review of both al-Shabaab media usage, and Russian Information Warfare doctrine and its application to recent events, illustrate some effective social media strategies. While not all of these strategies may be applicable to the DoD, it is important for people inside the DoD to understand them and identify ways to combat them.

Once examples of effective business, non-state, and state actor social media strategies have been identified, conclusions will be drawn, identifying principles that the DoD should consider in the development of its social media strategy. This research will illustrate how the DoD may use social media as a viable means to collect open source

information. Through analyzing business models and social media techniques, the paper will demonstrate improved ways the DoD may utilize social media to communicate globally. An operational example will demonstrate practical ways that the lessons learned from business models and our adversaries may be applied to the Joint Planning Process. Finally, this study is intended to generate discussion and encourage the development of network knowledge required to maximize the capabilities social media might offer to the DoD.

Chapter 1: Understanding Social Media

Defining Social Media and the Social Media Environment

In order to understand how to use social media, a user must first understand the meaning of the term social media. Social media is any application that allows global users to create and share information with each other in a virtual space.[1] The critical component of this definition is the ability to create dialogue between various users. Communication via social media is made possible through a variety of device types, to include computers, tablets, gaming devices, smart phones, and even basic cell phones.[2] The components of users, information, and the platforms and devices to share the information, make up the social media environment.

The first step to understanding the social media environment is knowing what devices and platforms are available for social media users within a region. While much of the western world equates social media devices to smart phones, tablets, and computers, the non-Western world relies heavily on "dumb phones," or more traditional cellular phones with limited computing power and functionality.[3] These varying device types will run different applications. For example, "dumb phones" are not capable of running platforms such as Facebook, so they rely more heavily on short messaging service (SMS) platforms such as GroupOn and WhatsApp.[4] Knowing the device types, sites and platforms

---

[1] Gupta and Brooks, 18.
[2] Ibid.
[3] Ibid., 33.
[4] Ibid.

available leads to the second component of social media, the type of information or media available.

Within the social media environment, there are three basic media types: owned, paid, and earned. Owned media is that which is generated or controlled by the marketer, such as a company website or Facebook page.[5] Paid media is bought by the marketer and includes sponsorship or advertising.[6] Paid media could include pop-up ads that sponsor other applications, such as the advertisements sometimes seen on YouTube or Facebook. Earned media is neither controlled nor bought by the marketer, but rather controlled by the consumer, and includes word-of-mouth or viral posts.[7] However, the marketer may help generate earned media through marketing actions.[8] Likewise, earned media may be posted on owned media, such as a consumer providing feedback on a company Facebook page. In most social media platforms there is interplay between the three types of social media. The DoD will primarily work with owned and earned social media types; posting its own content on owned websites or applications which will help generate earned social media from the public.

Within the types of media are several classifications of social media platforms. Blogs are websites maintained by a single individual, posting information chronologically in a

---

[5] Richard Hannah, Andrew Rohm and Victoria L. Crittenden, "We're All Connected: The Power of the Social Media Ecosystem," *Business Horizons* Vol. 54, No. 3 (May-June 2011): 268, http://www.sciencedirect.com/science/article/pii/S0007681311000243?via%3Dihub (accessed September 10, 2017) ; Karen Xie and Young-Jin Lee, "Social Media and Brand Purchase: Quantifying the Effects of Exposures to Earned and Owned Social Media Activities in a Two-Stage Decision Making Model," *Journal of Management Information Systems* Vol. 32, No. 2 (Fall 2015): 205, https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=2ca64ecc-c3a9-4dea-9b22-851610dafb6e%40sessionmgr4010 (accessed December 27, 2017).

[6] Hannah, Rohm, and Crittenden, 268.

[7] Ibid.

[8] Xie and Lee, 205.

manner that allows for interaction through comments on posted material.[9] Social

networking platforms, such as Facebook and Twitter, provide a micro-blog function that

allows multiple users to network with each other and share personal information.[10]

Content platforms such as YouTube, allow sharing of media, to include video, pictures,

audio, and text, between users.[11] Platforms called *collaborative projects*, such as

Wikipedia, use a method in which numerous users may create or edit content.[12] A fifth

type of platform are ones that are location-based. Examples are *Find My Friends,* which

shares a user's location with others; *Yelp*, which utilizes the user's location to provide

specific media to the user; and *Facebook Places,* which uses locations to geo-tag the

user's media.[13] The final type of social media platform is *crowdsourcing*, which focuses

on distributing knowledge between users. An example of crowdsourcing is *Waze*, an

application in which drivers input information such as traffic conditions and road

conditions making that information immediately available to other users.[14]

Crowdsourcing is "the act of influencing, incentivizing, and leveraging crowds through

social media to provide you with information and help you solve problems."[15] While

crowdsourcing platform are relatively new, the concept has already been used in other

platforms such as Facebook, and crowdsourcing provides an active way to foster

---

[9] Kaplan and Haenlein, 63.
[10] Gupta and Brooks, 22; Kaplan and Haenlein, 63.
[11] Ibid., 23; Ibid.
[12] Kaplan and Haenlein 62.
[13] Gupta and Brooks, 26.
[14] Harvard Business School Digital Initiative, "Waze – Crowdsourcing Maps and Traffic Information," Harvard Business School, https://digit.hbs.org/submission/waze-crowdsourcing-maps-and-traffic-information/ (accessed March 30, 2018).
[15] Ibid., 180.

engagement and interaction with populations, thereby opening opportunities to influence those populations.[16]

The last component to the social media environment is the user. Users may be broken down into five categories: creators, critics, collectors, joiners, and spectators.[17] Creators publish, maintain, and upload content, critics comment and rate content; collectors save and share the information; joiners connect other users; and spectators simply read the information without commenting or passing it on.[18] As entities within the DoD develop social media strategies, planners will need to not only identify the various users by studying the networks, but will also need to understand which roles the DoD needs to play within those networks. The roles will change based on varying relationships with other users and the platforms they utilize.

The social media environment is a complex system involving the interactions of users in a virtual world created by the use of electronic devices and site usage. Understanding the environment where the targeted community resides is essential to effective social media strategies. Once the social media environment is defined, organizations and businesses can determine influence factors, marketing, and targeting techniques to reach the desired population. A study of some effective business and marketing strategies will help identify some critical concepts for the DoD to integrate into their own social media strategy.

---

[16] Ibid.
[17] Hannah, Rohm, and Crittenden, 268.
[18] Hannah, Rohm, and Crittenden, 268-269.

Marketing Media

In marketing, social media "moves consumers from awareness [of a company/product] to knowledge, and finally conviction or action [to advocate or purchase]."[19] Effective marketers understand that a social media environment exists, comprised of the interactions between marketers and consumers through both traditional and interactive media.[20] Traditional media includes television, radio, print, and billboard advertising. Interactive media includes primarily social media, but also includes paid advertising on websites allowing consumers to interact through clicking on the advertisement and gaining more information.

It is critical for the marketer to integrate all elements of the social media environment. In order for their message to have impact, marketers must identify their target consumer, determine which traditional and social media platforms the target consumer uses, develop the key message to tell, and broadcast the message throughout the environment.[21] Furthermore, they must use a combination of earned and owned social media content in a way that is complementary and does not diminish the benefit derived from one or the other.[22] For example, a brand could undermine the effect of an associated buzzword on earned social media by creating a new campaign on owned social media such as a Facebook Fan Page. The new owned content should capitalize on existing successful messages and relationships.

---

[19] Xie and Lee, 212; Hannah, Rohm, and Crittenden, 268.
[20] Hannah, Rohm, and Crittenden, 267.
[21] Hannah, Rohm, and Crittenden, 269.
[22] Xie and Lee, 232.

Marketers also use the social media environment to provide a forecast and help

determine future activities a company should take.[23] Due to the interactive nature of

social media, consumers provide regular feedback and build a conversation with the

marketer in the form of clicks, likes, posts/re-posts, and comments.[24] Synthesizing this

feedback provides marketers a forecast of desired products in addition to status of current

products. Once a business understands the social media environment of their target

consumers, they may develop strategies to influence consumers and push them towards

conviction and action.

<center>Influencing an Audience</center>

Dr. Robert Cialdini's six principles of persuasion are widely accepted by marketers in

setting conditions for influencing customers. These principles include reciprocity,

scarcity, authority, consistency, liking, and consensus.[25] When marketing experts began

leveraging social media to improve access to their targeted audience, they found ways to

incorporate these principles into their marketing campaigns.

The principle of reciprocity is the obligation an individual feels to give back to others

for something they have received first.[26] In marketing this principle may be translated

into offering aggressive discounts that might cause a consumer to feel obligated to

purchase the item based on the money they would save.[27] Because social networking is

---

[23] Hannah, Rohm, and Crittenden, 268.

[24] Ibid.

[25] Robert Cialdini, "Science of Persuasion (Video Transcript)", Influence at Work, https://www.influenceatwork.com/principles-of-persuasion (accessed December 27, 2017).

[26] Ibid.

[27] Edward Vukovic, "The Six Principle of Influence and How to Make them Work for You," Digital Actuaries, https://www.actuaries.digital/2015/09/19/the-six-principles-of-influence-and-how-to-make-them-work-for-you (accessed December 27, 2017).

often about the relationships and idea sharing, businesses may push consumers away with aggressive overt advertising. However, by offering no-strings-attached values, such as a discount coupon by joining or liking a Facebook fan page, business begin to build relationships and reciprocity simultaneously.[28]

The principle of scarcity is the principle that people want more of those things that there are fewer of.[29] According to Dr. Cialdini; "It's not enough simply to tell people about the benefits they'll gain if they choose your products or services. You'll also need to point out what is unique about your proposition and what they stand to lose if they fail to consider your proposal." Marketing uses this principle when they offer "hot deals" that tell people they will miss out if they don't act quickly.[30] Less personal, these deals often pop up in social media applications but may be targeted towards specific customers based on preferences, which will be explained in the next section.

Dr. Cialdini's third principle of persuasion is the principle of authority, or the idea that people follow the lead of credible, knowledgeable experts.[31] Celebrity endorsement is a well-known marketing technique and is applicable in social media as much as in traditional media. A 2015 study demonstrated that the strongest influence came from celebrities who are top-experts within domains, such as business, education, media, and entertainment.[32] The study also demonstrated that celebrities in entertainment tend to

---

[28] Jeff Sexton, "6 Powerful Social Media Persuasion Techniques," Social Media Examiner, https://www.socialmediaexaminer.com/6-powerful-social-media-persuasion-techniques (accessed December 27, 2017).

[29] Cialdini.

[30] Manuel Jaeggi, "Use These 6 Principles Behind the Science of Persuasion (or Sicence of Influence) and Start Getting More Customers Before Your Competition Does, Or You May Lose Your Business!" Postcron, https://postcron.com/en/blog/use-6-principles-science-of-persuasion-get-customers (accessed December 27, 2017).

[31] Cialdini.

[32] Wayne Xin Zhao, Jing Liu, Yulan He, Chin-Yew Lin, and Ji-Rong Wen, "A Computational Approach to Measuring The Correlation Between Expertise and Social Media Influence for Celebrities on

exercise the most amount of influence across domains.[33] In addition to celebrity

endorsements, consumers have become key influencers on social media by providing

product testimonials to other consumers within their social networks.[34] By studying and

identifying key influencers within a social network, businesses can target those

individuals who will then have a multiplying affect within their networks.

Consistency is the principle that people like to be consistent with the things they have

previously said or done.[35] Online marketing uses clicks or "likes" to build consistency

and commitment in a consumer's mind.[36] Over time a consumer builds a consistent

message regarding a company or product and will want maintain the appearance of

consistency through product purchase.

The principle of liking is that people tend to say yes to people they like; people who

are similar to them, pay them compliments, or cooperate with them.[37] Kaplan and

Haenlein provide five points for corporations to be effective on social media: be active,

be interesting, be humble, be personal and be honest.[38] Active engagement requires

posting up to date information in new and imaginative ways and regular interaction with

consumers through two-way communications. Two-way communication allows

businesses to better understand consumer preferences, so they may target their messaging

---

Microblogs, *World Wide Web; New York* Vol. 19, No. 5 (September 2016):
867, https://search.proquest.com/docview/1799427794?accountid=12686 (accessed September 10, 2017).

[33] Ibid., 879.

[34] Danny Brown, "Breaking from Tradition: The Four-Ms of Influence Marketing," Convince and Convert, http://www.convinceandconvert.com/social-media-case-studies/breaking-from-tradition-the-four-ms-of-influence-marketing (accessed December 27, 2017).

[35] Cialdini.

[36] Jaeggi.

[37] Cialdini.

[38] Kaplan and Haenlein, 66.

towards certain groups of consumers. Each social networking platform has its own rules of etiquette. Corporations need to maintain humility and stay within the established rules. The concepts of Web 2.0 and User Generated Content imply a lack of professional structure by allowing everyday users to become an active participant. Social media provides corporations an inexpensive means to interact with the customer and brings marketing down to a personal vice professional manner. Honesty ties the other four points together by ensuring corporations understand and abide by the social media rules and norms to build a more personal interaction with the consumer. These five points will increase likeability among consumers.

The final principle is consensus, which states that when uncertain, people will look to the actions of others to determine their own.[39] In marketing, consensus is social proof, or the evidence that something is adequate or not.[40] Social networks give numerous ways to gain social proof, such as likes, ratings, and re-posting/re-tweeting. Corporations that are able to get consumers to give positive feedback via social network platforms will gain greater influence within those networks.

<center>Targeting an Audience</center>

Marketers have several tools available to them to target consumers through online tracking. Each time consumers pulls up a web-page, their browser creates a "cookie" on that device. Cookies are created by either a first-party or third-party. First-party cookies are placed by the site that a consumer visits in order to make their web experience more

---

[39] Cialdini.
[40] Jaeggi.

efficient.[41] Third-party cookies are placed by a partner of the website, such as an advertising network or analytics company.[42] Third-party cookies are designed to monitor behavior over time and allow companies to build a profile on a consumer to better target their interests. First and third-party cookies are only beneficial to marketers if a consumer does not manage their browser setting or clear their browsing history before logging off.

Flash cookies and device fingerprinting provide marketers a means to monitor consumer activity that may not be cleared at the end of a browsing session. A flash cookie is a type of cookie specific to Adobe's Flash player technology. Flash cookies store settings and preferences on the consumer's computer vice the browser, which allows marketers to track consumer history and target advertising for that device.[43] Similarly, device fingerprinting uses a device's browser configuration and settings to create a profile for that device without cookies.[44] Using device fingerprinting, marketers build a profile for that specific device based on the browser settings. Finally, device identifiers provide advertising and analytics companies a method of collecting consumer information through mobile applications. Device identifiers are provided by the operating system and monitor the different applications used on a particular device.[45] While savvy consumers are able to manage device and browser settings to diminish the effectiveness of consumer monitoring, the average consumer will find it challenging to manage settings on all devices and keep up with emerging marketing technologies.

---

[41] Federal Trade Commission, Consumer Information, "Online Tracking," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0042-online-tracking (accessed December 20, 2017).
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.

Chapter 2: Social Media in Business and Marketing

Case Study #1: JPMorgan Chase Fails to Connect on Twitter

In November of 2013, JPMorgan Chase underwrote Twitter in its initial public offering. To promote both the bank and Twitter, JPMorgan launched a social media Question and Answer (Q&A) campaign. The target audience was college students, giving them an opportunity to ask a senior executive career advice. A day prior to the question and answer period the bank canceled the Q&A session.

Why did JPMorgan cancel the Q&A? Primarily due to the negative response from the public reflected in the questions posed. Instead of thoughtful questions from students, they received non-career-related questions aimed at the company's recent failures. Questions such as "What's your favorite type of whale?" referring to the London Whale trading loss two months prior, and "Did you have a specific number of people's lives you needed to ruin before you considered your business model a success?" alluding to the settlement JPMorgan Chase reached the month prior with the US Justice Department for bad mortgage loans, spotlighted corporate blunders.[1] Additionally, some Chase executives were being investigated for manipulating the Foreign Exchange markets at the time.[2] All of these issues resulted in a public relations crisis for the bank.

---

[1] Emily Greenhouse, "JPMorgan's Twitter Mistake," *The New Yorker*, November 16, 2013, under "JPMorgan Twitter Fail," https://www.newyorker.com/business/currency/jpmorgans-twitter-mistake (accessed December 20, 2017); Matt Taibbi, "Chase's Twitter Gambit Devolves into All-Time PR Fiasco," *Rolling Stone*, November 15, 2013, under "JPMorgan Twitter Fail," https://www.rollingstone.com/politics/news/chases-twitter-gambit-devolves-into-all-time-pr-fiasco-20131115 (accessed December 20, 2017).
[2] Taibbi.

JPMorgan's failed attempt to connect with the public is illustrative of a lack of understanding in the social media environment and understanding the platform they were trying to leverage. JPMorgan attempted to target a specific audience with a platform designed to allow any individual to share the same space, attention, and authority as any other individual or group.[3] As such, they were unable to control the conversation on Twitter that ended up encouraging dialog during a controversial time for them.[4] It was a costly mistake. To engage in a successful open dialogue, corporations must first establish a positive relationship with consumers. Due to recent legal and financial misdeals, JPMorgan had eroded the public's trust and undermined existing relationships. To successfully provide a means for consumer input, JPMorgan first needed to listen and regain trust through empathy before posing open-ended questions to the public.[5] For two-way communications to be effective, corporations must have a strong, positive relationship with their consumers.[6]

There are several lessons that the Department of Defense can draw from this example. The first lesson is to know the purpose and functionality of the available social media platforms and what type of audience they reach. Understanding the functionality of various social media platforms available enables the DoD to employ them appropriately. If the intent is to gain information and public opinion, platforms such as Twitter may

---

[3] Greenhouse.

[4] Lina Saigol, Camilla Hall, and Hannah Kuchler, "#AskJPM Underscores Risks of Twitter Engagement," *Financial Times*, November 14, 2013, under "#askjpm," https://www.ft.com/content/def2fd4c-4d2a-11e3-9f40-00144feabdc0 (accessed December 20, 2017).

[5] Saigol, Hall, and Kuchler; Ted Birkhahn, "Here's What You Should Learn from JPMorgan's #disaster," CNBC, https://www.cnbc.com/2013/11/18/six-things-to-learn-from-jpmorgans-mistakes.html (accessed December 20, 2017).

[6] Aaron Taube, "What Banks Can Learn from JPMorgan Twitter Fail," *Business Insider,* November 15, 2013, under "JPMorgan Twitter Fail," http://www.businessinsider.com/what-banks-can-learn-from-jpmorgan-twitter-fail-2013-11 (accessed December 20, 2017).

provide the most information. To build relationships gradually and gain trust, platforms that broadcast information with limited commenting functionality such as Facebook or YouTube would be best.

The DoD must not only understand the functionality, but also what type of audience the platform draws and why people use it. In the case of JPMorgan, they attempted to generate professional dialogue on a general public social media platform, when a platform focusing on professionals, such as LinkedIn, may have been a more appropriate venue. After DoD entities understand the functionality and users of the platforms they can begin developing their desired message to favorably influence and shape their area of operations.

When developing the message, entities within the DoD need to understand the importance of timing and how current events may affect behavior before engaging with an audience. Analysis of popular opinion will give insights to the level of existing relationship with the populace. Precautions must be taken to avoid being perceived as manipulative. By understanding existing relationships and opinions, DoD entities can effectively develop strategic messaging to shape the social media environment to support operations in their area of responsibility.

Case Study #2: Social Media Rebuilds Interest in the Grammy Awards

In 2008, the Recording Academy was facing a decline in viewership of their annual Grammy Awards program on CBS. The number of competing media outlets, such as increased cable networks and online entertainment, provided consumers options that

drew them away from traditional network programs.[7] Additionally, a shift in demographics away from the desired 18-49 year old crowd towards an older female demographic resulted in lost revenues from paid advertisers.[8] In order to boost viewership, the Recording Academy decided to develop a social media strategy.

The Recording Academy hired the TBWA/Chiat/Day advertising agency who took two years to develop a social media strategy before it was fully implemented for the 2010 Grammy Awards. During that time, TBWA/Chiat/Day conducted outreach, studied the social media climate, and determined where its target audience was spending its time online.[9] The Recording Academy also used this time to develop its own presence online and began connecting with consumers.[10] TBWA/Chiat/Day used the Recording Academy's social media presence and the resulting relationships with viewers to launch their 2010 Grammy Awards show advertising campaign.

TBWA/Chiat/Day took a holistic approach to advertising the 2010 Grammy Awards. While social media provided the focal point of their advertising, they used traditional media, such as radio, newspaper, and television, to point consumers to the wereallfans.com, a website designed for the 2010 Grammy Awards.[11] Traditional media advertising combined numerous videos posted to social media by the public to advertise the awards show, encouraging further on-line interaction with the Recording Academy.[12] The website developed by TBWA/Chiat/Day featured interactive software that allowed

---

[7] Hannah, Rohm, and Crittenden, 269.
[8] Ibid.
[9] Christina Warren, "How Social Media is Changing the 2010 Grammys," *Mashable,* January 25, 2010, under "We're All Fans," http://mashable.com/2010/01/25/grammys-2010/#snBycBRCDqqN (accessed December 20, 2017).
[10] Hannah, Rohm, and Crittenden, 270.
[11] Hannah, Rohm, and Crittenden, 270; Warren.
[12] Warren.

viewers to scroll over key words linked to social media content that would then be used

to create collages of popular artists.[13] By increasing the Recording Academy's social

media presence and interaction with a broader consumer base, TBWA/Chiat/Day was

able to generate interest in the 2010 Grammy Awards among the younger demographics,

thereby increasing viewership.

The successful 2010 Grammy Awards social media campaign provides several

lessons learned that may be applicable to the Department of Defense. To be successful,

the Recording Academy had to first do its research. Relatively unfamiliar and

uncomfortable with social media, the Recording Academy hired an expert in the field,

TBWA/Chiat/Day, to do the hard work for them. Experts at TBWA/Chiat/Day developed

interactive software that quickly combed several social media sites for keywords.[14]

Similarly, the DoD should look for opportunities to develop experts in social media

within CYBERCOM who not only understand how to push or pull information, but are

able to develop software that interacts with social media platforms in creative ways.

The 2010 Grammy Awards campaign demonstrates is the importance of

understanding the social media environment. TBWA/Chiat/Day's first challenge was

developing a presence on social media and building an understanding of who was using

the various platforms. As demonstrated in their campaign, this takes time. Furthermore,

the 2010 Grammy Awards campaign illustrates the importance of understanding how

traditional media forms interact with the social media environment. For the DoD to use

social media successfully to shape and influence an area of responsibility to support

---

[13] Hannah, Rohm, and Crittenden, 270.
[14] Warren.

future operations, it must determine what platforms the various demographics in a region

use and integrate the social media environment with traditional media sources.

Chapter 3: Social Media Utilization by Al-Shabaab and Russia

Case Study #3: Al-Shabaab Wins and then Loses the Narrative

Al-Shabaab, a Somali terrorist group with links to al-Qaeda, provides an excellent example of how to both gain and lose influence and support through social media. From its beginnings in the mid 2000's, al-Shabaab relied upon social media to project its narrative, recruit, and solicit funding and support. The primary objective of al-Shabaab's media operations was to influence the information environment in order to facilitate their struggle for power on the ground.[1] Though over time, they lost control of the narrative and the support they once gained through social media.

Despite Somalia's high poverty rate and lack of infrastructure, businesses in Somalia have been able to take advantage of emerging communications technologies. Somalia's lack of strong central government over the past twenty years has allowed private businesses to operate unregulated, giving rise to numerous cellphone and communication companies.[2] After al-Shabaab organized in 2006, they quickly turned to the internet and social media to gain support for their movement to create an Islamic state in Somalia. Al-Shabaab used social media successfully in early efforts to gather support by targeting several audiences simultaneously, to include locally, regionally, and globally.[3] They skillfully tailored messaging for each group and used the most effective media outlets to gain support for their cause.

---

[1] Christopher Anzalone, "Continuity and Change: The Evolution and Resilience of al-Shabaab's Media Insurgency," Hate Speech International (November 9, 2016): 30, https://www.hate-speech.org/new-report-on-al-shabab-media (accessed December 20, 2017).
[2] Al Shabaab and Social Media, Ken Menhaus, 311
[3] Anzalone, 24.

In Somalia, al-Shabaab focused on a narrative that concentrated on nationalism and sought to build al-Shabaab into a viable governing organization.[4] Using the Somali language, al-Shabaab broadcasted messages not only over the internet, but radio and satellite television, as well.[5] The message that resonated with the people of Somalia was one that sought an end to the twenty years of civil war and lack of governance while expressing Islamo-nationalist motives.[6]

Islamo-nationalism also provided a narrative for al-Shabaab to reach out to the Somali diaspora. Al-Shabaab's goal was to recruit and gain financial support from the Somalis abroad. The terrorist organization met the group where they were located in the social media environment; on YouTube, Facebook, and various other websites. They also used the English language, which much of the diaspora, to include a generation born outside of Somalia, was familiar with.[7] The Western media's portrayal of the prolonged Somali conflict alienated Somalis around the globe. Feelings of humiliation set the conditions for al-Shabaab narratives to be highly successful by disseminating a storyline of oppression and Somali victimhood through blogs and websites.[8] By supporting al-Shabaab either financially or physically, the diaspora developed a connection with their homeland. As members of the diaspora joined al-Shabaab in Somalia they were then used to reach back to friends and family at home. They used their social media accounts to

---

[4] Anzalone, 7; CBS News, "Al-Shabab Showed Gruesome Social Media Savvy During Attack," CBS News, https://www.cbsnews.com/news/al-shabab-showed-gruesome-social-media-savvy-during-attack (accessed December 20, 2017).

[5] Ken Menkhaus, "Al-Shabaab And Social Media: A Double-Edged Sword," *Brown Journal of World Affairs* Vol. 20, No. 2 (Spring/Summer 2014): 311, https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=100570507&site=ehost-live&scope=site (accessed September 17, 2017).

[6] Ibid., 313.

[7] CBS News.

[8] Menkhaus, 311-312.

maintain communications with other diaspora members, posting YouTube videos that promoted life in al-Shabaab and engaging in dialogue and debate through Facebook and Twitter.[9]

A narrative that resounded with all audiences early on was one of an Islamic struggle against a hostile Christian West.[10] Publication of derogatory cartoons and depictions of the Prophet Muhammad in Western media during 2007 and 2008 inflamed Islamic sensibilities and roused jihadi sentiment.[11] The global jihad narrative resonated with Muslims both at home and abroad, to include non-Somali Muslims. To reach external sources of support they produced and posted videos in English, Arabic, Somali, and Swahili, a language commonly spoken in neighboring countries.[12] Al-Shabaab integrated other means of media into their messaging outside Somalia. Through their own websites they would post media content found in reputable news sites.[13] This gave a false sense of neutrality and legitimacy to their own content. Al-Shabaab was selective in the material it re-posted, choosing only those news articles that helped develop the narrative they were trying to develop. The group also took risks by granting access and interviews to news sources.[14] Once again, they were selective in the news agencies they dealt with, talking only with the agencies that generally reflected al-Shabaab's world view, such as Al-Jazeera.

In addition to selectively collaborating with legitimate news sources, al-Shabaab also sought to undermine opposition news while presenting itself as a source of truth. Al-

---

[9] Ibid., 316.
[10] Anzalone, 10; Menkhaus, 313.
[11] Anzalone, 10.
[12] Ibid., 12.
[13] Menkhaus 315.
[14] Ibid., 316.

Shabaab successfully did this during the 2013 attack on Westgate Mall in Nairobi, Kenya. Real-time postings on Twitter were used by popular news sources, such as CNN, giving credibility to al-Shabaab's reporting.[15] Furthermore, they were able to stay ahead of the Kenyan government reports and in some instances demonstrate the inaccuracy of those reports, thereby presenting themselves as a truthful and reliable news source while undermining the opposition's credibility.[16]

Despite early successes through social media, al-Shabaab has lost both internal and external support. Internally, support has eroded partially due to a shift in the focus of the narrative. By 2010, al-Shabaab had seemingly given up on aspirations to mobilize masses in Somalia, indifferent to winning the hearts and minds of the masses.[17] Instead, they became more focused on the messaging of global jihad through a call for "lone wolf" jihadists to conduct suicide bomb attacks.[18] The change in narrative, coupled with a growing negative reputation, lost Somali support while also creating a key strategical division within its own organization.[19]

The al-Shabaab case study provides lessons learned both on how to use social media effectively to gain support on the ground as well as the risks involved when using social media. Al-Shabaab demonstrated an understanding of the social media environment by effectively using various media sources to target local, regional, and global audiences. Once al-Shabaab understood where to find their target audience, they tailored the message both linguistically and narratively to gain support. The key to building a

---

[15] Anzalone, 32.
[16] Ibid.
[17] Menkhaus, 317.
[18] Anzalone, 33; Menkhaus, 317.
[19] Menkhaus, 317.

successful narrative through social media was using pieces of existing frames, or filters on how someone perceives the world.[20] Using the existing frames of an alienated diaspora population and an Islamic struggle against Western Christianity, al-Shabaab built narratives that resonated with several populations.

Al-Shabaab used social media to build relationships with its target audiences and shape the narrative. Early social media engagements utilized chat rooms and Facebook to allow followers to ask questions and interact with al-Shabaab military leaders.[21] As al-Shabaab gained recruits from various diaspora populations, they used recruits as influencers to continue building support abroad. By 2011, al-Shabaab had a well-established media agency known as Harakat al-Shabaab al-Mujahedeen Press (HSM Press), largely run by educated diaspora members who engaged with audiences in a personal and professional manner.[22]

Al-Shabaab also used popular news sources to build their own credibility. By reposting articles and granting selective interviews they aligned themselves with neutral news sources. Through social media, al-Shabaab provided real-time reporting that was then used by popular news sources, building al-Shabaab's credibility. Using these methods, al-Shabaab was successful in early efforts to gain support through social media.

In 2012, al-Shabaab began to lose some of the support they had gained through social media. While the HSM Press gave al-Shabaab an appearance of legitimacy and a means to focus on information operations, they failed to uphold two of Kaplan and Haenlein's

---

[20] Gupta and Brooks, 302.

[21] Menkhaus, 316.

[22] Will Oremus, "Twitter of Terror: Somalia's al-Shabaab Unveils a New Social Media Strategy for Militants," *Slate.com,* December 23, 2011, under "al-Shabaab social media," http://www.slate.com/articles/technology/technocracy/2011/12/al_shabaab_twitter_a_somali_militant_group_unveils_a_new_social_media_strategy_for_terrorists_.html (accessed December 20, 2017).

five points for corporations to be effective on social media: be humble and be

unprofessional. Engagements with HSM Press on Twitter devolved from polite

interaction that promoted the narrative, to what appeared as an arrogant display of their

mastery of the English language with tweets such as "what's beyond abhorrence is the

collective Western Crusade against Islam of which you seem quite blasé about if not

supportive."[23]

From 2011 to 2013, al-Shabaab lost control of the narrative. Use of social media by

individuals within the organization presented mixed messaging and provided a means for

internal tensions to be exposed openly.[24] Dissatisfaction with al-Shabaab leadership and

fear for his own life was posted by popular jihadist, Omar Hammami, who once was a

key spokesperson for the group. An open letter posted by co-founder of al-Shabaab to al-

Qaeda leadership further exposed loss of support from the Somali people and potential

failure due to abusive leadership.[25]

In addition to losing control over posts from individuals within the organization, their

own messaging resulted in a loss of capability. While the postings during the Westgate

Mall attack provided real-time coverage of the event, the administrators of Twitter

deemed it inappropriate content and shut-down the HSM Press Twitter account, negating

Twitter as a viable means of communication for the group.[26]   Westgate also revealed that

al-Shabaab had no control over bogus Twitter accounts purporting to be the official al-

---

[23] Menkhaus, 321.
[24] Ibid., 317.
[25] Ibid., 319.
[26] Ibid., 321.

Shabaab account. Once they lost their account, they no longer had a means to control the message.[27]

There are several key points the DoD should apply from the al-Shabaab case study. First, the case study reinforces the need to understand the social media environment locally, regionally, and globally, and be able to tailor the narrative accordingly. The DoD also needs to know what frames exist already and build narratives around them. Social media applications such as Twitter do not give enough space to build new narratives, but are ideal for putting out small bits of evidence that reinforce existing ones.[28] This case study also exemplifies the importance of maintaining humility and ensuring messaging is about the narrative and not the message itself.

Finally, the DoD must remember that there are risks involved in using social media. Social media was intended for individuals to interact with each other. Therefore, individuals within organizations typically have personal accounts. Due to an individual's association with an organization, their opinions posted on personal accounts may be misconstrued as the organization's message. Current DoD training on appropriate social media use is important not only for maintaining operational security, but to also ensure that individual messages are concurrent with organizational themes. Fake accounts, known as trolls, also pose a risk to falsely portraying an organization's message. The DoD needs to account for these risks and take appropriate measures to counter them.

---

[27] Ibid., 322.
[28] Ibid., 320.

Case Study #4: Russian Usage of Social Media in Information Warfare

To understand Russia's application of social media, one must first understand Russia's view of Information Warfare. Unlike Western states, Russia does not make a distinction between cyber and non-cyber information. All information is contained within "information space" and is sub-categorized into information-psychological warfare, which is aimed at personnel, and information-technological warfare, which is aimed at the systems.[29] According to Russian doctrine, information-psychological warfare is a continuous operation in both peacetime and wartime, whereas information-technological warfare is used only during wartime to debilitate an enemy's capability to broadcast/receive information.[30] The key point is Western nations limit psychological warfare in peacetime while Russia does not; Russia continuously engages in misinformation and deception efforts to foment discourse in other states.[31]

Russia is currently weaker militarily that most Western powers and therefore relies on Information Warfare to create asymmetrical force.[32] By creating confusion and psychological tension, Russian officials believes they will gain a psychological advantage that negates its physical disadvantage.[33] The range of goals for Russian Information Warfare includes regime change and "long-term weakening and undermining of societies overall" to increase their own relative power.[34] Following Sun Tzu's principle to seek

[29] Keir Gleis, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016), 9.
[30] Ibid.
[31] Ibid., 11.
[32] Ibid., 16.
[33] Ibid., 18.
[34] Ibid., 18, 24.

attainment of strategic goals without battle, Russian officials see Information Warfare as a means to attain their strategic goals while avoiding armed conflict.[35]

One of Russia's key techniques of Information Warfare is deception. The NATO Handbook of Russian Information Warfare cites the following principles of media campaigns:

- Direct lies for the purpose of disinformation both of the domestic population and foreign services;
- Concealing critically important information;
- Burying valuable information in a mass of information dross;
- Simplification, confirmation and repetition (inculcation);
- Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;
- Introducing taboos on specific forms of information or categories of news;
- Image recognition; known politicians or celebrities can take part in political actions to order, thus exerting influence on the world view of their followers;
- Providing negative information, which is more readily accepted by the audience than positive.[36]

A recent Rand study further explains the effect of some of these principles. Rand found that Russia uses multiple media sources; traditional television and radio media, internet news sources, social media, etc., to flood the public with its messages. By flooding the information environment, Moscow ensures more users receive their desired message. These broadcasts ensure the message is transmitted numerous times over several media sources, increasing the message's credibility while drowning out opposing messages or other world events which it does not want attention drawn to.[37] Additionally, because the message is often false with the goal of stirring public emotions, Moscow is not concerned

[35] Ibid., 16.
[36] Ibid., 47-48.
[37] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter it*, (Santa Monica, CA: RAND Corporation, 2016): 2-3, under "Russia social media," https://www.rand.org/pubs/perspectives/PE198.html (accessed September 16, 2017).

with taking time to check facts and can often put its message out quickly, making the first impression on users. By making the first impression, officials control the narrative, even when exposed as false, by spinning the story as it develops.[38]

Russia uses "Troll Farms" and "Bots" to flood the information environment with false information. A troll is an online personae run by humans that is specifically intended to stir up discourse by posting provocative and inflammatory information.[39] An internet bot is "an automated application used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform," to include scraping media content or manipulating comments/votes.[40] In the 2016 U.S. Presidential elections, Russian cyber-experts used troll farms to create online identities that influenced social media. Examples of Russian trolling include the creation of two supposed African-American bloggers, Williams and Kalvin, who posted false information about the Clintons on Facebook, Twitter, Instagram, and YouTube, and the creation of American Muslim identities in a group called United Muslims of America to spread false information on several politicians.[41] In order to build up the credibility of the fake profiles and generate followers for exploitation at a later date Russia employs trolls and bots on social media before hostilities exist. This method of establishing credibility helps

[38] Ibid., 4, 6.

[39] Gleis, 54; Elise Moreau, "Internet Trolling: How do You Spot a Real Troll?," *Lifewire.com*, June 13, 2017, under "internet troll," https://www.lifewire.com/what-is-internet-trolling-3485891 (accessed October 23, 2017).

[40] Technopedia, "Internet Bot: Definition," Technopedia.com, https://www.techopedia.com/definition/24063/internet-bot (accessed October 23, 2017).

[41] Max Boot, "The United States Has Already Lost a Major Battle in the Information War," *Business Insider*, October 14, 2017, under "information warfare," http://www.businessinsider.com/the-united-states-lost-a-major-battle-in-the-information-war-2017-10 (accessed October 16, 2017).

Russia "develop [sic] tactics for defeating analytical methods used to identify false personae."[42]

In addition to broadcasting false messages en masse over social media through false identities and click-bait advertising that points users to Russian-backed media, Russia also targets individuals. Using bots and trolls to build relationships with genuine users, Russia then exploits the personal information on the users. Personal information is gained both through the data which is posted online as well as through technology that collects the data from personal electronic devices. In this way, Russia has demonstrated an ability to gain access to individuals to their advantage, such as building a database of nearby adversarial military personnel. Recent examples show that Russia has been able to target specific populations, such as the "simultaneous telephoning of Polish military personnel from Russia, and precisely geographically targeted intimidating text messages in Ukraine."[43] More recently, Russia targeted Facebook ads towards voters in Michigan and Wisconsin, states in which Trump won by less than one percent and were critical to his Electoral College Victory.[44]

The Russian case study provides some unique lessons that the DoD needs to understand in order to both project its own influence via social media as well as counter those of adversaries. It should be noted that democratic states such as the United States have less latitude as to how they may use information warfare due to the liberal principles they espouse. While the DoD may not seek regime change or to cause mass confusion

---

[42] Gleis, 70.
[43] Gleis, 71 citing K. Giles, The Next Phase of Russian Information Warfare, op. cit.
[44] Boot.

that weakens a society, some of Russia's Information Warfare principles may be applicable to shaping the information environment.

The first lesson to understand is the idea of broadcasting messages en masse to shape the environment. Russia used all means of media, to include social media, to broadcast their message. Repetition of a message builds a heuristic, or a way that the mind simplifies problem solving by relying on quickly accessible information.[45] In social media, repeated messages become "trends" and can quickly build into a truth of their own.

Russian Information Warfare relies upon the use of bots and trolls to help build trends out of the message that they want to broadcast. Bots and trolls pose two basic questions that the DoD needs to answer: First, how can they be quickly detected and countered? Second, is this a technique that the DoD needs to investigate in more detail to determine legality of their use? In addition to the consideration of using bots, the DoD needs to establish relationships in peacetime. In the absence of bots and trolls, a network of followers could become influencers to rebroadcast desired messages.

The last lesson the Russian case study teaches is the importance of flexibility and agility on social media. One of the key benefits of social media as demonstrated in the al-Shabaab case study is that it allows rapid dissemination of a narrative, often times before conventional press is able to detect the story. While the DoD may not completely disregard the truth to maintain agility as Russian information warfare does, it must find ways to ensure the narrative is flexible enough to quickly adapt to changing situations.

---

[45] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* Vol. 11, No. 4 (Winter 2017): 56, https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=9&sid=a6610c41-b3ee-4edc-b647-1163e254596c%40sessionmgr4008 (accessed December 8, 2017).

An examination of these four case studies demonstrates some key principles for operating in the social media environment. The next step is to explore how these principles fit in with DoD operations.

Chapter 4: Social Media Applied to DoD Operations

By using some of the lessons learned from marketing and adversaries, DoD planners can better incorporate social media into their operations. Three ways that social media needs to be incorporated are in the development of the joint intelligence preparation of the operating environment (JIPOE), information operations (IO) during day-to-day operations, and in the specific targeting of information related capabilities (IRC) during contingency operations. These three areas build upon each other as the DoD moves from understanding the social media environment, to building relationships and identifying influencers within social networks, and finally using social media and influencers for specific desired effects on a target audience.

The first step in the joint planning process (JPP), Planning Initiation, includes understanding the strategic guidance and the operating environment (OE).[1] The JIPOE, developed by the intelligence community, helps planners understand the OE. Part of the OE includes understanding the social media environment. Analysis of the social media environment should begin with identification of what devices (computer, smart phone, tablet) and social media platforms are available. Just as the al-Shabaab case study illustrated, this must be done locally, regionally, and globally. Resources, such as Ravi Gupta and Hugh Brooks book *Using Social Media for Global Security,* can provide summaries of popular social media applications by region. It is important to understand

---

[1] U.S. Joint Chiefs of Staff, *Joint Planning,* Joint Publication 5-0 (Washington DC: Joint Chiefs of Staff, June 16, 2017), V-4.

the functionality, or purpose, of each of these platforms in order to determine what portion of the population might reside on them.

An example of appropriately choosing a social media platform by region was provided by the US Army in 2007. At that time, the Army used the social networking site, Univision, rather than Facebook to reach the Hispanic community, because Univision held a larger Latin-American audience.[2] Additionally, Univision provides a moderating service that Facebook does not while checking comments for appropriate content prior to posting them.[3] Knowing the functionality and who resided on the platform allowed the Army to reach their target audience. Analyzing the platforms and devices is only one part of understanding the social media environment, the intelligence community will also need to monitor the content of social media as they build the JIPOE to build awareness of the networks that reside in the OE.

Once social media platforms have been identified, the intelligence community will begin collecting information about the populations that reside on them. The first roles the DoD should play in a new social media environment are those of spectator and collector in order to gather information about existing networks of people. Social media provides a wealth of open source information from global, regional, and local trending topics down to personal information on individuals within networks. Intelligence and IO planners should also utilize location-based platforms and crowdsourcing platforms to gather more localized intelligence. In addition to social media, cookies from DoD websites may be analyzed to gain valuable information about individual behaviors and preferences, or associate specific devices with users. Using the information about existing networks in

---

[2] Kaplan and Haenlein, 65.
[3] Ibid.

the social media environment, the intelligence community can build a more complete

JIPOE for planners.

Using information gained from the JIPOE about the social media environment, and

specifically about the networks within the OE, IO cells may build long-term campaign

plans that help DoD entities establish relationships on social media through the roles of

critic and creator. The initial goal as a critic is to provide positive feedback, gaining

influence through the principle of reciprocity. This may be done in the form of retweeting

or reposting content, liking content, or leaving favorable comments. Remaining humble

and personal is critical to this phase of building relationships within the networks.

Messages should not only be transmitted on owned media, such as websites or

Facebook Fan Page, but they should also incorporate earned media through

crowdsourcing. By crowdsourcing and receiving feedback, DoD entities begin to build

influence through the principle of consistency. Crowdsourcing also allows a participatory

audience to take ownership of new ideas through leading questions and interactions.[4] The

We Are All Fans promotional spots that solicited and incorporated videos from users is

an excellent example of successful crowdsourcing to generate interest in a topic. By

filling the roles of critic and creator throughout a theater campaign, the IO cell establishes

the relationships necessary to influence the social media environment while gaining a

better understanding of where target audiences reside.

When contingencies such as a non-combatant evacuation operation (NEO) arise

within an area of responsibility, IO planners will use their understanding of the social

media environment and the developed relationships to influence target audiences in a way

---

[4] Gupta and Brooks, 306.

that supports DoD operations. Joint Publication (JP) 3-13, Information Operations, characterizes IO as "the integrated employment, during military operations, of information-related capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[5] Using the example of a NEO resulting from rebel forces threatening the government of country Orange, IO planners could use social media to target and influence various audiences to support a safe evacuation plan.

During the first step in the JPP, IO planners use their understanding of the OE and strategic guidance to determine the desired target audience.[6] For the NEO example, the IO cell might identify American citizens (AMCITS) in country Orange as one target audience, and rebel forces as a second. As the IO cell analyzes the social media environment, they will not only need to identify the platforms and social networks of each group, but also key influencers within the networks.

IO planners will need to understand how various social networks and social media platforms view influence differently. In some networks influencers may include true celebrities, but that will depend on the social media platform and its purpose. Users of professional platforms such as LinkedIn, and platforms intended to share ideas such as Twitter, may identify with experts and celebrities as the influencers. However, in social networks on platforms such as Facebook, individual members also hold considerable influence over other members of the network.[7] While a network or select population may be the target audience, the key influencers are the critical nodes to reaching the target

---

[5] U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington DC: Joint Chiefs of Staff, November 20, 2014), I-1.
[6] JP 3-13, IV-4.
[7] Brown.

audience. Whether broadcasting or blocking a message, success will lie in how the key influencers will be used. Using the NEO example, the rebel group may utilize Facebook to influence the population. Once identified, IO planners may target the primary influencers to disrupt their messages or deter further actions. Similarly, the U.S. embassy will likely be a key influencer with AMCITS in country Orange. IO planners will need to work with the embassy team to ensure AMCITS are reached and given direction for NEO procedures.

Another important aspect for DoD entities to consider is how to support messages on social media through other forms of media. A common element in the JPMorgan, al-Shabaab, and Russian case studies was the use of numerous forms of both traditional and social media to broadcast a message. It's critical that DoD messaging remain consistent, but that consistency must bridge across all governmental agencies involved in an action or operation. However, as demonstrated in the Russian case study, hearing a message repeatedly begins to build a bias towards the narrative. Additionally, messages that fit within an existing bias or a repressed bias will have greater success influencing the network.[8] The al-Shabaab case study demonstrated this when they built their initial narrative around the existing belief that Western Christianity was attacking Islam. As the message resonates with key influencers and begins to spread, the principles of authority and consensus allow the message to gain influence over other members of the network and shape the environment for the desired purpose. For example, it may be determined that a message over social media to deter further aggressive action by the rebels in country Orange might be best supported by radio announcements or billboards.

---

[8] Gupta and Brooks, 302.

Last, as JP 3-13 states, the IO plan must be assessed and adjusted as necessary.[9] There are many risks involved in using social media, to include mixed messages from inside the organization, a lack of control over the narratives others might be trying to achieve, or false personas that may include DoD impersonators. Constant monitoring of the social networks and adjustment of the message is imperative to ensuring the desired narrative is communicated. This is true not only in the case of contingencies, such as the NEO example, but is a continuing action throughout the theater campaign.

The above discussion on actions in Country Orange exemplifies how social media may be integrated into the JIPOE, campaign plan, and contingency plans. As CYBERCOM continues to develop, consideration should be given to more complex ways to use social media to shape the broader information environment. The development of social media experts may be beneficial. Capabilities that these experts might have would include development of social media platforms, exploiting information from social media, developing countermeasures to bots and trolls, as well as consideration on how the DoD might use bots and trolls to rapidly build a trend or conduct military deception. Risk assessment must be conducted throughout the development of these capabilities though; as demonstrated in the JPMorgan case study, it is important to understand the rules of etiquette before using a social media platform. If the DoD intends to break the rules through the use of deception, it must weigh the risks involved, to include loss of credibility on the network. But if CYBERCOM develops capabilities correctly, social media will be a force multiplier in shaping the information environment.

---

[9] JP 3-13, IV-8.

Conclusion:

Social media has become a critical element of the information environment. While the Department of Defense has taken some steps to establish a presence on and monitor main stream social media, it lacks a comprehensive plan that fully integrates social media into the information operations plan. A study of non-state and state actors, such as al-Shabaab and Russia, demonstrates that the DoD is losing the battle of the narrative in the social media environment. By studying non-state actors, state actors, and business models, the DoD will be able to better incorporate social media into their information operation plans.

The further development of CYBERCOM as a combatant command and the designation of *Information* as a joint function presents a unique opportunity to explore DoD capabilities in social media. As CYBERCOM develops and gains additional resources, consideration should be given to investing some of those resources into social media. Furthermore, CYBERCOM, with legal guidance, needs to explore all opportunities that social media may provide, to include the use of bots and trolls as well as development of new technologies or platforms that may be able to counter them. Nearly three-quarters of the world's internet population resides on social media. The DoD must invest wisely in developing its social media capabilities.

Bibliography

Anzalone, Christopher. "Continuity and Change: The Evolution and Resilience of al-Shabaab's Media Insurgency." Hate Speech International (November 9, 2016). https://www.hate-speech.org/new-report-on-al-shabab-media (accessed December 20, 2017).

Birkhahn, Ted. "Here's What You Should Learn from JPMorgan's #disaster." CNBC. https://www.cnbc.com/2013/11/18/six-things-to-learn-from-jpmorgans-mistakes.html (accessed December 20, 2017).

Boot, Max. "The United States Has Already Lost a Major Battle in the Information War." *Business Insider*, October 14, 2017. http://www.businessinsider.com/the-united-states-lost-a-major-battle-in-the-information-war-2017-10 (accessed October 16, 2017).

Brown, Danny. "Breaking from Tradition: The Four-Ms of Influence Marketing." Convince and Convert. http://www.convinceandconvert.com/social-media-case-studies/breaking-from-tradition-the-four-ms-of-influence-marketing (accessed December 27, 2017).

CBS News. "Al-Shabaab Showed Gruesome Social Media Savvy During Attack." CBS News. https://www.cbsnews.com/news/al-shabab-showed-gruesome-social-media-savvy-during-attack (accessed December 20, 2017).

Chief Information Officer. "Social Media Education and Training." U.S. Department of Defense. http://dodcio.defense.gov/Social-Media/SMEandT (accessed January 2, 2018).

Cialdini, Robert. "Science of Persuasion (Video Transcript)." Influence at Work. https://www.influenceatwork.com/principles-of-persuasion (accessed December 27, 2017).

Federal Trade Commission. Consumer Information. "Online Tracking." Federal Trade Commission. https://www.consumer.ftc.gov/articles/0042-online-tracking (accessed December 20, 2017).

Flintoff, Corey. "Viral Images, the Military's Recurring Nightmare." National Public Radio. http://www.npr.org/2012/01/12/145117940/viral-images-the-militarys-recurring-nightmare?ps=cprs (accessed October 30, 2017).

Garamone, Jim and Lisa Ferdinando. "DoD Initiates Process To Elevate U.S. Cyber Command To Unified Combatant Command." Department of Defense News. https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ (accessed 10/16, 2017).

Gleis, Keir. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016.

Greenhouse, Emily. "JPMorgan's Twitter Mistake." *The New Yorker*. November 16, 2013. https://www.newyorker.com/business/currency/jpmorgans-twitter-mistake (accessed December 20, 2017).

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

Hannah, Richard, Andrew Rohm, and Victoria L. Crittenden. "We're All Connected: The Power of the Social Media Ecosystem." *Business Horizons* Vol. 54, No. 3 (May-June 2011): 265-273. http://www.sciencedirect.com/science/article/pii/S0007681311000243?via%3Dihub (accessed September 10, 2017).

Harvard Business School Digital Initiative. "Waze – Crowdsourcing Maps and Traffic Information." Harvard Business School. https://digit.hbs.org/submission/waze-crowdsourcing-maps-and-traffic-information/ (accessed March 30, 2018).

Jaeggi, Manuel. "Use These 6 Principles Behind the Science of Persuasion (or Science of Influence) and Start Getting More Customers Before Your Competition Does, Or You May Lose Your Business!" Postcron. https://postcron.com/en/blog/use-6-principles-science-of-persuasion-get-customers (accessed December 27, 2017).

Kaplan, Andreas M. and Michael Haenlein. "Users of the World, Unite! The Challenges and Opportunities of Social Media". *Business Horizons* Vol. 53, No. 1 (January-February 2010): 59-68. http://www.sciencedirect.com/journal/business-horizons/vol/53/issue/1 (accessed October 31, 2017).

Krulak, Charles. "The Strategic Corporal: Leadership in the Three Block War." *Marine Corps Gazette* Vol. 83, No. 1 (January 1999): 18-22. https://www.mca-marines.org/leatherneck/1999/01/strategic-corporal-leadership-three-block-war (accessed October 30, 2017)

Marcellino, William, Meagan L. Smith, Christopher Paul, and Lauren Skrabala. "Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations." Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1742.html (accessed December 20, 2017).

Menkhaus, Ken. "Al-Shabaab and Social Media: A Double-Edged Sword." *Brown Journal of World Affairs* Vol. 20, No. 2 (Spring/Summer 2014): 309-327. https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=100570507&site=ehost-live&scope=site (accessed September 17, 2017).

Mligo, Elia Shabani. *Introduction to Research Methods and Report Writing: A Practical Guide for Students and Researchers in Social Sciences and the Humanities*. Eugene, OR: Resource Publications, 2016. https://ebookcentral.proquest.com/lib/nationaldefense-ebooks/detail.action?docID=4835551 (accessed October 31, 2017).

Moreau, Elise. "Internet Trolling: How do You Spot a Real Troll?" *Lifewire.com*, June 13, 2017. https://www.lifewire.com/what-is-internet-trolling-3485891 (accessed October 23, 2017).

Oremus, Will. "Twitter of Terror: Somalia's al-Shabaab Unveils a New Social Media Strategy for Militants." *Slate.com,* December 23, 2011. http://www.slate.com/articles/technology/technocracy/2011/12/al_shabaab_twitter_a_somali_militant_group_unveils_a_new_social_media_strategy_for_terrorists_.html (accessed December 20, 2017).

Paul, Christopher and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter it*. Santa Monica, CA: RAND Corporation, July 11, 2016. https://www.rand.org/pubs/perspectives/PE198.html (accessed September 16, 2017).

Prier, Jarred. "Commanding the Trend: Social Media as Information Warfare." *Strategic Studies Quarterly* Vol. 11, No. 4 (Winter 2017): 50-85. https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=9&sid=a6610c41-b3ee-4edc-b647-1163e254596c%40sessionmgr4008 (accessed December 8, 2017).

Saigol, Lina, Camilla Hall, and Hannah Kuchler. "#AskJPM Underscores Risks of Twitter Engagement." *Financial Times*, November 14, 2013. https://www.ft.com/content/def2fd4c-4d2a-11e3-9f40-00144feabdc0 (accessed December 20, 2017).

Sexton, Jeff. "6 Powerful Social Media Persuasion Techniques." Social Media Examiner. https://www.socialmediaexaminer.com/6-powerful-social-media-persuasion-techniques (accessed December 27, 2017).

Taibbi, Matt. "Chase's Twitter Gambit Devolves into All-Time PR Fiasco." *Rolling Stone*. November 15, 2013. https://www.rollingstone.com/politics/news/chases-twitter-gambit-devolves-into-all-time-pr-fiasco-20131115 (accessed December 20, 2017).

Taube, Aaron. "What Banks Can Learn from JPMorgan Twitter Fail." *Business Insider.* November 15, 2013. http://www.businessinsider.com/what-banks-can-learn-from-jpmorgan-twitter-fail-2013-11 (accessed December 20, 2017).

Technopedia. "Internet Bot: Definition." Technopedia.com. https://www.techopedia.com/definition/24063/internet-bot (accessed October 23, 2017).

U.S. Department of Defense. *DoD Strategy for Operations in the Information Environment.* Washington DC: Department of Defense, June 13, 2016.

U.S. Joint Chiefs of Staff. *Information Operations.* Joint Publication 3-13. Washington DC: Joint Chiefs of Staff, November 20, 2014.

U.S. Joint Chiefs of Staff. *Joint Planning.* Joint Publication 5-0. Washington DC: Joint Chiefs of Staff, November 20, 2014

U.S. Secretary of Defense. *Information as a Joint Function.* Memorandum. Washington DC: Department of Defense, 15 September 2018.

Vukovic, Edward. "The Six Principle of Influence and How to Make them Work for You." Digital Actuaries. https://www.actuaries.digital/2015/09/19/the-six-principles-of-influence-and-how-to-make-them-work-for-you (accessed December 27, 2017).

Warren, Christina. "How Social Media is Changing the 2010 Grammys." *Mashable.* January 25, 2010. http://mashable.com/2010/01/25/grammys-2010/#snBycBRCDqqN (accessed December 20, 2017).

Xie, Karen and Young-Jin Lee. "Social Media and Brand Purchase: Quantifying the Effects of Exposures to Earned and Owned Social Media Activities in a Two-Stage Decision Making Model." *Journal of Management Information Systems* Vol. 32, No. 2 (Fall 2015): 204-238. https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=2ca64ecc-c3a9-4dea-9b22-851610dafb6e%40sessionmgr4010 (accessed December 27, 2017).

Zhao, Wayne Xin, Jing Liu, Yulan He, Chin-Yew Lin, and Ji-Rong Wen. "A Computational Approach to Measuring the Correlation Between Expertise and Social Media Influence for Celebrities on Microblogs." *World Wide Web; New York* Vol. 19, No. 5 (September 2016): 865-886. https://search.proquest.com/docview/1799427794?accountid=12686 (accessed September 10, 2017).

Vita

Lieutenant Colonel Brett A. Allison (USMC) was commissioned in 1998 after graduating from the US Naval Academy. LtCol Allison was designated as a CH-46E pilot and served in Marine Medium Helicopter squadrons (HMM) on the east and west coasts as well as a tour as an instructor pilot at Marine Aviation Weapons and Tactics Squadron 1(MAWTS-1). Deployments include Mediterranean and Western Pacific Marine Expeditionary Unit deployments and a deployment to Iraq. LtCol Allison served as the Site Commander with HMM-774 and transitioned to the MV-22 aircraft with the squadron. LtCol Allison has completed Marine Corps Command and Staff College, Weapons and Tactics Instructor Course, and Aviation Safety Officer Course.