REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15042016	Army Science Board	Jan-Jul 2015

4. TITLE AND SUBTITLE
Human Interaction and Behavioral Enhancement

5a. CONTRACT NUMBER
NA

5b. GRANT NUMBER
NA

5c. PROGRAM ELEMENT NUMBER
NA

6. AUTHOR(S)

Michael Macedonia, PhD.

5d. PROJECT NUMBER
NA

5e. TASK NUMBER
NA

5f. WORK UNIT NUMBER
NA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Army Science Board
2530 Crystal Dr. Suite 7098
Arlington, VA 22202-3911

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Department of the Army
Office of the Deputy Undersecretary of the Army
Washington, DC 20310-0103

10. SPONSOR/MONITOR'S ACRONYM(S)
HQDA/DUSA

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The Army Science Board is the senior scientific advisory body for the Department of the Army and is chartered as a Federal Advisory Committee organized under the Federal Advisory Committee Act.

14. ABSTRACT
The purpose of the study was to identify and assess methods and techniques to understand, interact, and influence human behavior. Because he Army increasingly conducts operations in urban areas in which the perception and behavior of non-combatants significantly affects the probability of Army mission success, adversaries are taking advantage of social networking and other information technology means to influence local populations in countering or hindering Army operations. The study team recommended the Army assign an executive agency and develop proponency for social media operations, to include monitoring and leveraging social media research and development. Additional recommendations are classified.

15. SUBJECT TERMS
social media, behavior, human interaction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mark S. Swiatek
U	U	U	UU/SAR	22	19b. TELEPHONE NUMBER *(Include area code)* 7035458657

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18
Adobe Professional 7.0

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Army Science Board
Fiscal Year 2015 Study

Human Interaction and Behavioral Enhancement

Final Report
April 2016

Department of the Army
Office of the Deputy Under Secretary of the Army
Washington, D.C. 20310-0103

Distribution Statement A: Approved for public release; distribution is unlimited.

DISCLAIMER

This report is the product of the Army Science Board (ASB). The ASB is a Federal Advisory Committee established to provide independent advice to the Secretary of the Army (SA) and the Chief of Staff, Army (CSA). Statements, opinions, conclusions, and recommendations contained in this report are those of the Army Science Board and do not necessarily reflect any official position of the United States Army or the Department of Defense.

This document will be available from the Defense Technical Information Center (DTIC). For this limited distribution item, please visit the secure site: https://www.dtic.mil. Non-registered Government/contractor DTIC users can register at http://www.dtic.mil/dtic/registration/.

DEPARTMENT OF THE ARMY
ARMY SCIENCE BOARD
2530 CRYSTAL DRIVE. SUITE 7098
ARLINGTON, VA 22202

DUSA-ASB May 15, 2016

MEMORANDUM FOR SECRETARY OF THE ARMY

SUBJECT: Final Report of the Army Science Board, "Human Interaction and Behavioral Enhancement."

1. I am pleased to forward the final report of the Army Science Board study titled "Human Interaction and Behavioral Enhancement." The study identified and assessed methods and techniques the Army could use to understand, interact with and influence human behavior among populations located within the Army's areas of operation. Specifically, the study team investigated methods the Army could adopt to establish a human interaction overmatch capability. While the team focused primarily on social media, the scope of their investigation included other non-kinetic means to influence attitudes and behavior.

2. For this effort, the study team brought subject matter experts in Computer Science, Neuroscience, Chemistry, Resource Strategy, Physics, Psychology, Medicine, Engineering (Electrical and Mechanical), Network Architecture, and a variety of military operations and technologies, as well as former Army leaders. During it's seven months together, the study team conducted over thirty-five visits and interviews among Army and DoD agencies, FFRDCs, Academe, and commercial industry.

3. As a result of these efforts, the study team made a number of findings and recommendations aimed at identifying concepts, technologies, and procedures the Army might adopt to challenge our adversaries' exploitation of social media. The study team's findings and recommendations, as well as the ASB approved briefing, are included in a separate, classified appendix to this study report. The unclassified sections of the report contained herein provide background on the study team's approach to responding to each of the tasks listed in the Terms of Reference. The findings and recommendations in this study were adopted by the Army Science Board by unanimous vote on October 6, 2015.

4. I hereby endorse the findings and recommendations in this report.

James A. Tegnelia
Chairman

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

1.0 Executive Summary 1

2.0 Introduction 2
2.1 Terms of Reference (TOR) 4
2.2 Methodology 5

3.0 Leading Edge Methods 7

4.0 Emerging Concepts 10

5.0 Army Social Media Overmatch Capability 12
5.1 Techniques 13
5.2 Operations Concept 13
5.3 Enablers 15

6.0 Summary 17

APPENDICIES

A. Terms of Reference 18
B. Study Team Members 20
C. Glossary of Key Terms 21

LIST OF FIGURES

2.1 Global Digital Snapshot 3
2.2 Examples of “Internet Time” 3
2.3 Summary of the HI-BE Study Team Data Collection 5
2.4 Systems Analysis Approach 6
2.5 Measures of Effectiveness 6
3.1 SM Impacting Military Operations 7
5.1 The U.S. Army on Twitter and Facebook 12
5.2 Elements of an Army SM Operational Capability 14

1.0 EXECUTIVE SUMMARY

Rapid, technological changes are universally transforming the way humans interact with each other. Consequently, a new test of wills has arisen among nation states and non-state actors. Previous studies within DoD[1] noted that the commercial, digital revolution is having a wide-ranging impact on warfare. In particular, the introduction of smartphones over the last decade has allowed many state and non-state actors to employ the mobile devices for worldwide, interactive communication. In terms of their military application, these devices provide commercial software platforms (i.e., Facebook, Twitter, etc.) that enable command and control, intelligence gathering, and recruitment, all on a global scale.

These developments have already had a major impact on warfare, and the Army recognizes the need for a time critical, operational, social media (SM) overmatch capability.[2] The Secretary of the Army (SECARMY) commissioned the Army Science Board (ASB) to address these issues, and the Deputy Undersecretary of the Army (DUSA) sponsored this study to begin assessing the Army's operational needs in the realm of SM.

During the course of its investigation, the study team observed several conditions in the Army that prevent it from using SM communities and real-time feeds as effectively as our adversaries. As a result, our adversaries are able to exploit what amounts to a new battlefield in cyberspace, whereas the Army's use of SM is fragmented, ad hoc, and unable to keep pace. For example, if it needed to, how would the Army counter the SM operations that contributed to the Arab Spring? The simple answer: it couldn't. That's an important consideration in the 21st century, because an effective SM program might mitigate or even curtail the need for some level of conventional kinetic operations. At this point, the Army simply isn't fully engaged to leverage emerging, real-time SM.

The study team's findings and recommendations are classified, and may be accessed via coordination with the ASB office.[3] The following report provides the unclassified background and observations made by the study team that contributed to the findings and recommendations.

---

[1] For example, the Defense Science Board's *Understanding Human Dynamics* (2009); http://www.acq.osd.mil/dsb/reports/ADA495025.pdf

[2] Army Operating Concept (TRADOC PAM 525-3-1)

[3] Contact the Executive Director, Army Science Board, 2530 Crystal Drive, Suite 7098, Arlington, VA 22202-3911

2.0 INTRODUCTION

The Army recognizes the importance of information technology (IT) in mediating human interaction (HI). IT may be used to inform non-combatants, or to influence the behavior of foreign adversaries. Army FM 3-13, "Inform and Influence Activities," provides specific direction for operations in these areas, but it also delineates the Army's doctrine:

> Operating in today's complex environment requires commanders and their staffs to enable and support joint, interagency, intergovernmental, and multinational partners to protect and reassure populations and isolate and defeat enemies.[4]

Traditional methods of influencing and informing populations through one-way broadcast television, radio, newspapers and leaflets used by Military Information Support Operations (MISO) organizations are quickly being subsumed by the Internet and the digitization of all media.[5] For context, according to Gallup, between 2012 and 2014, use of the internet in Iraq increased from 18% to 40 %. At this rate, almost all Iraqis (and the rest of the world) will have access to cyberspace by 2017.

Social Media (SM) is the latest technology to provide a platform for influencing and informing. It's a twenty-first century "game-changer," because it's become pervasive since the introduction of smartphones in 2007, other networked devices, and the rapid spread of Facebook to over one billion users.

Like any technology, SM has both positive and negative applications. The scale of its adoption makes it a dynamic and uncertain force, which includes the creation of a new, intimate relationship between humans and computing technology that will shape the perception and understanding of 7 billion people in the world (Fig. 2.1). Anyone with a smartphone now has the ability to broadcast and receive messages and images worldwide, instantly. Thus, countering and proactively managing this capability is essential to strategic messaging.

---

[4] FM 3-13 Inform and Influence Activities

[5] http://www.nytimes.com/2014/10/27/business/media/how-facebook-is-changing-the-way-its-users-consume-journalism.html?_r=1

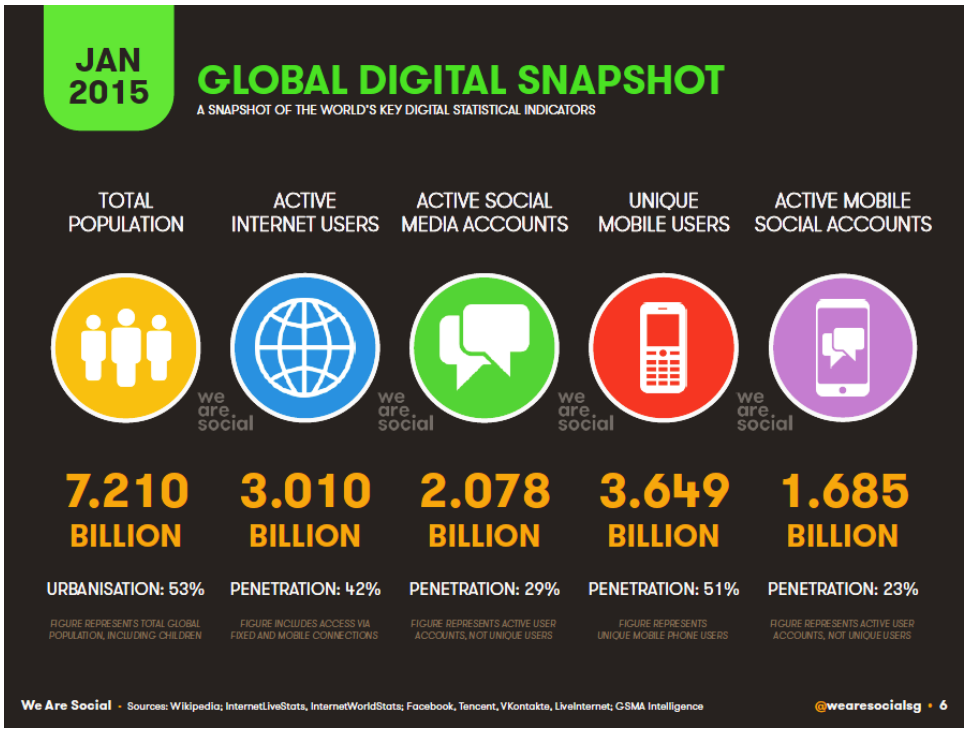

Figure 2.1 Global Digital Snapshot[6]

Human Interaction via SM will increase in magnitude as more people across the globe use smart technologies. So too, the speed at which the exchange of information occurs has rapidly fallen as technology has improved (Fig. 2.2). Events now unfold in "Internet time."

Figure 2.2 Examples of "Internet Time"

The vast majority of people use SM to improve the human condition. The ability to rapidly connect with someone else, at anytime and anywhere, has been a positive development. There

[6] http://wearesocial.com/sg/special-reports/digital-social-mobile-in-apac-in-2015

are many examples, such as families and friends who inform one another about their lives (Facebook, Instant Messenger, Skype, Twitter, etc.), professionals who inform one another of their work (LinkedIn, Research Gate, etc.), businesses that inform customers about their products (Groupon, Yelp, LivingSocial, etc.), and journalists who report on world events in real-time.

That same intimacy of SM that drives relationships, commerce, and information sharing can also be used to cause harm, and just as efficiently, by producing effects to enhance violence, aggression, and radicalization. Enemies of the United States use SM to recruit warriors willing to launch assaults against this country and our allies, from anywhere in the world. The most obvious example of late, the Islamic State (ISIS or ISIL), has prominently used SM to recruit new members, coordinate operations, and incite fear in others through real-time displays of their violence. In recruitment alone, it's estimated that over twenty thousand foreign fighters have been enlisted to wage war against the US and her allies.[7]

The technology around SM can also be used against U.S. forces by serving as a new kind of command and control system, as evidenced during the Egyptian uprising in 2013.[8] A similar operation, used against the U.S., could take away the advantage of surprise by providing our adversaries with a ubiquitous, organic means to continuously surveil U.S. military activities. Today's cellphones not only provide a platform for SM reporting such a text messaging and Twitter, they also carry powerful sensors, including night vision,[9] real-time video, GPS, and high-quality audio, all of which may be used for propaganda and intelligence collection.[10]

The Army recognizes the power of SM and is associated technology. The Army Operating Concept (TRADOC PAM 525-3-1), explicitly states a need for a time critical operational SM overmatch capability. Specifically, the document states, "the compression of events in time requires forces capable of responding rapidly in sufficient scale to seize the initiative, control the narrative, and consolidate order."

2.1 TERMS OF REFERENCE (TOR)

The Secretary of the Army requested the ASB identify and assess methods and techniques to understand, interact and influence human behavior in support of Army missions. As established in the study Terms of Reference (TOR) (see Appendix A), the intention was to counter adversaries' efforts to interact with and influence local populations where the Army conducts operations.

---

[7] http://www.telegraph.co.uk/news/worldnews/islamic-state/11770816/Iraq-and-Syria-How-many-foreign-fighters-are-fighting-for-Isil.html
[8] How an Egyptian Revolution Began on Facebook http://nyti.ms/15v7Gym
[9] http://gizmodo.com/a-tiny-night-vision-camera-that-lets-your-smartphone-se-1485632462
[10] The pressures of a potentially hostile population with ubiquitous access to SM is currently being felt by domestic law enforcement agencies, giving rise to the issuing of body cams to provide a counter narrative. (http://money.cnn.com/2015/08/07/investing/ferguson-body-cameras-taser-digital-ally/)

The TOR tasked the ASB to develop findings and recommendations using a systems analysis approach. Specific tasks included:

- Identifying and assessing the most effective current and leading edge methods and techniques from commercial businesses, academia and other military services that could establish a "human interaction overmatch capability" for the Army.

- Identifying emerging concepts, technologies and procedures that have the potential to disrupt enemy activities by significantly enabling the Army's interaction with people in foreign countries and influencing their attitudes and behavior.

- Determining specific elements of the force capable of taking lead on influencing human behavior through social media or other non-kinetic means, and identify their responsibilities in this area. In addition, examine the potential roles and capabilities that all ground forces may adopt to influence human behavior.

- Describing how the Army should prepare specific functional units and ground forces as whole for human interaction and recommend how to sustain those capabilities.

The study team made findings and recommendations in areas related to leading edge methods, emerging concepts, and development of an Army social media overmatch capability. These are provided in the classified Appendix to this report.

2.2 METHODOLOGY

The study team's investigation and data collection included over 35 visits, interviews, and teleconferences with various Army and Department of Defense (DoD) officials, Federally Funded Research and Development Centers (FFRDC), and over a dozen companies in commercial industry (Fig. 2.3).

DoD / Government Organizations:

- Federal Government: **Dept. of State**, Center for Strategic Counterterrorism Communications (CSCC)
- OSD/Joint: J8, DARPA, **CENTCOM**, SOCOM, J3, JSOC, Strategic Capabilities Office
- **Army:** INSCOM, XVIII ABN, PAO, TRADOC IO Proponent, USASOC, JFK School, Army General Counsel, **ARCYBER**

FFRDCs/Academe/Non-Federal:

- RAND, NYPD, UN, PARC

Industry:

- Marketing Firms: Gallup, Burson-Marsteller, Hightower, NBC Universal
- Social Media: Microsoft, **Twitter, Facebook**, IMGUR, SnapChat, Ori Branfman/Silicon Guild

Figure 2.3 Summary of the HI-BE Study Team Data Collection

From the four tasks outlined in the TOR, the study team distilled three broad lines of inquiry that guided discussion during the data gathering process:

1. Assess the current and leading edge methods to establish an HI overmatch capability,

2. Identify disruptive, emerging concepts, technologies and procedures that have the potential to improve the Army's interaction with people in foreign countries,

3. Determine elements of the force capable of taking lead on HI and identify their responsibilities.

To analyze the data collected, the study team developed a systems analysis approach to identify important issues related to the TOR tasks (Fig. 2.4).

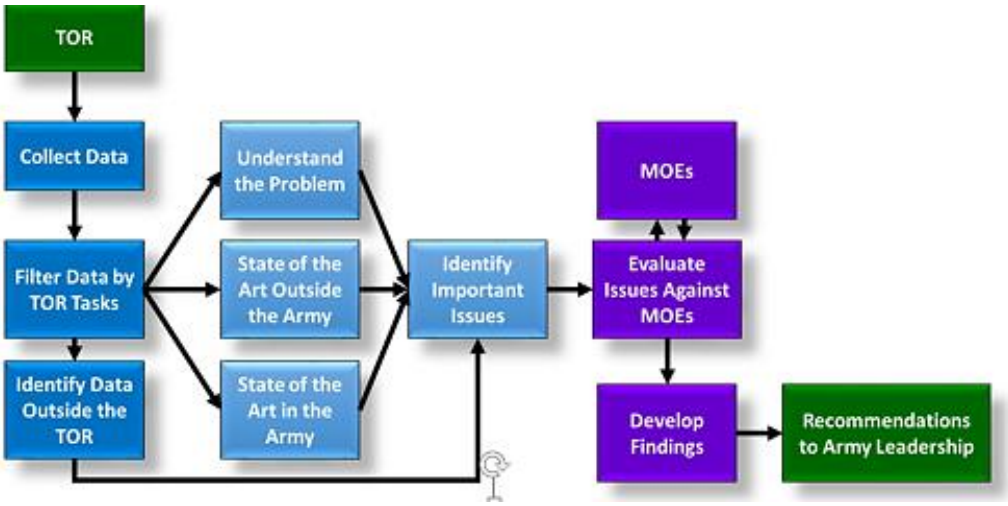

Figure 2.4 Systems Analysis Approach

Issues were then evaluated against a set of measures of effectiveness (MOE) the study team established that were tied to the development of an overmatch capability for the Army (Fig. 2.5). Based upon the evaluation against MOEs, findings and recommendations were made.

MEASURES OF EFFECTIVENESS (MOEs) for an Army Social Media Overmatch Capability:

- **The Scale of Human Interaction:**
  - Changes in the number of followers / breadth and depth of influence
- **The Timeliness of the Response**
- **The Degree of Behavioral Influence:**
  - Changes in the number or redirection of interactions and information sources
  - Changes in sentiment in target segment
  - Changes in social network topologies
  - Collective action (online and real world)

Figure 2.5 Measures of Effectiveness

3.0 LEADING EDGE METHODS

The study team interviewed numerous experts to understand which organizations were best at using SM to further their goals and why. Foreign states and advisories stood out, largely because of lax (compared to the U.S.) or non-existent legal constraints (Fig. 3.1).[11]

Figure 3.1 SM Impacting Military Operations

We hear and see examples of the Islamic State's effective use of social media frequently in the U.S. ISIS has polished marketing materials (Fig. 3.1 A) and it uses graphic images of beheadings and other atrocities to serve as a show of strength and to recruit additional believers to the Caliphate.[12] In March 2015, the Islamic State Hacking Division posted names and addresses of 100 U.S. military personnel on a website linked to ISIS and called for them to be killed.[13] ISIS also uses SM such as Facebook as a platform to reach out to those who may be vulnerable to influence, i.e., those who feel isolation, have a desire to belong to a group, and/or the need to feel special. ISIS has also used SM for more direct, operational activities, such as using Twitter as a command and control network.[14]

Other insurgent organizations such as Al Qaeda and the Mahdi Army have used SM to spread disinformation about U.S. military operations. One example is Operation Valhalla (Fig. 3.1 B), where a successful U.S. Special Forces strike was reframed over SM as a massacre of innocents

[11] A second set of success stories came from the world of political elections where advertising firms have teamed with candidates to provide individually targeted messaging with SM. A third group was in the US national security establishment, to include State Department and CENTCOM, who actively are using SM to counter ISIS.
[12] https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html
[13] Pentagon investigates 'IS online threat' to US military, http://www.bbc.com/news/world-us-canada-32006068
[14] The web is a terrorist's command-and-control network of choice http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3ubuezNHG

praying at a mosque.[15] Even though the U.S. had video of the operation that proved that it was against combatants, the Army's response to the SM attack took three days, by which time the damage from the adversary's SM attack had occurred.

Another recent example of SM attacks on U.S. credibility occurred when the Syrian Electronic Army's combined cyber and social media attack of the U.S. Army's website (Fig. 3.1 D) replaced the official Army content with pro-Syrian propaganda.

The ubiquitous nature of SM and its associated technology enables adversaries to collect real-time reconnaissance of Army operations from non-combatant observers. The attack on Osama bin Laden was tweeted live as the operation occurred (Fig. 3.1 C). With the increased saturation of social media globally, the implication is that it will be increasing difficult for Army operations to be conducted covertly.

In each of these cases, the Army may develop counters to adversary SM attacks and disinformation, but it only has minutes to employ them. The centralized, hierarchical decision-making process that defines a military institution simply cannot respond adequately. To do so, the Army would have to match the speed–Internet speed–of a global, distributed, real-time phenomenon. In addition, it needs to recognize the requirement for continuous SM operations and engagement to counter the SM threat.

Beyond ISIS and other terrorist groups, nation states like Russia and China are exploiting social media as a weapon to influence the behavior of both their own populations and their opponents.'[16] Russia's use of social media in the Ukraine and Crimea demonstrated a successful execution of its doctrine on information warfare—combined with kinetic operations and subversive efforts—by using social media to dissuade world reaction until their occupation of territory was nearly complete. The Russian government's use of bots (software that runs automated tasks over the Internet to imitate humans) and trolls (people who purposely sows discord and/or confusion in an online community such as Twitter) on social media to make its actions appear more acceptable also proved effective in controlling dissent within Russia.[17]

Russia also demonstrates an example of something like combined arms in the media; integrating SM and newer media into conventional platforms. For example, the Russia Today (RT) international television broadcast uses SM extensively and has become a platform to challenge Western media messaging with a glitzy mix of genuine investigation, bizarre conspiracy theory, and cynical disingenuousness.[18] RT's 2015 budget increased by almost 30%, suggesting the Kremlin values its role and has determined that the platform is effective in advancing its ideology.[19]

---

[15] http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art005.pdf
[16] http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/
[17] http://www.nytimes.com/2015/06/07/magazine/the-agency.html
[18] Loffe, 2010; O'Sullivan, 2014
[19] 'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't Mark Galeotti, Apr 16 2015

China's use of propaganda and SM appear to be more nuanced and largely inwardly focused. Their version of trolls is known as "50-centers," who are citizens paid to break up social media discussion deemed hostile to the Communist Party. Their external operations have been more covert and traditional, such as the employment of China Radio International to operate stations in the United States.[20]

Other countries, including Israel, are developing SM platforms to advance their agendas and to control strategic messaging.[21] The Israeli Defense Force (IDF) has established an organization that uses SM to document their fight with Hamas and the Palestinians. The unit uses YouTube, Twitter and Facebook to provide video and explanations of IDF operations in real-time. For example, The IDF provided updates via Twitter on rocket fire from Gaza and the activity of Israel's Iron Dome missile defense system, with tweets such as: "BREAKING: Iron Dome just intercepted 7 rockets above Ashkelon." Their efforts were established in part to counter a similarly sophisticated SM campaign by Hamas and the Palestinians during the 2014 Gaza conflict.[22]

In sum, the study team observed states, non-state actors, and other organizations using SM to further their military or quasi-military goals, and doing so successfully, in some cases gaining the same effects that would traditionally take conventional or kinetic operations. The recent expansion of SM communities and real-time feeds is being as a weapon to open a new battlefield in cyberspace.

[20] http://www.reuters.com/investigates/special-report/china-radio/
[21] Pillar of Tweets http://files.cargocollective.com/27931/The-Ongoing-Online-Israeli-Palestinian-Conflict.pdf
[22] http://www.bbc.com/news/world-middle-east-28292908

4.0 EMERGING CONCEPTS

In examining the future of SM and the impact it will have on Army operations, one dynamic was clear to the study team: the velocity and volume of SM information will continue to shorten the decision cycle for operational commanders, and if unaddressed by the Army, will put Soldiers at increased risk. Some of the trends that illustrate this new dynamic include:

1. Everyone will be connected via SM. With the rapid expansion in the percentage of the world's population that uses the internet and social media (Fig. 2.1), the trend is for future Army engagements to occur in a context of near global social media saturation. Social media use on smart phones occurs in 23% of the world's population, and over half the world's population uses a smart phone. In the future, most people will be connected using mobile phones and SM, more people will be influenced using SM, and they will be able to influence others using SM as well. Mobile devices will be connected with the internet of things, providing real-time device status, as well as personal health and biometric data. Mobile SM platforms will be universal and will be the preferred method of communication. As the pace of SM communications continues to increase, real-time information updates, communication and interactions will be the norm.

2. Increased SM capabilities. Social media will have an increasing ability to change attitudes and behavior, delivering more tailored and sophisticated messages to a larger number of targeted people. Currently, the audience for a SM message can be segmented to a target group. In the future, the profiles of all connected people will be enriched and unified, providing extremely detailed information on preferences, social connections, buying patterns, beliefs, and the ability to be influenced. Social media campaigns will directly impact how people find and process information, respond to crisis situations, and act in the real world. For example, Facebook conducted a controversial study in 2014 where SM was used to influence people's emotions by modifying their news feeds.[23] These new techniques will bring with them the necessary improvements in the ability to measure the influence, effectiveness and scope of SM campaigns, in real-time, and at much higher levels of detail.

3. Increased use of automated bots. As automated bots become more sophisticated, it will become impossible to distinguish a bot from a person online. Bots will be used to shape SM narratives, as well as to prepare the SM battlespace by collecting intelligence for situational awareness and/or cyber battle damage assessments. Bots are currently being used to direct people online to specific content, to direct interactions, and to change social groups. Social media messages can be amplified or suppressed automatically using automated bots. In the future, there will be an escalation in automated systems that attempt to determine whether an online user is a real person or a bot. There will also be a

[23] http://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html?_r=0

rise in bot versus bot SM campaigns, or bot wars. Bots will be integrated with cyber-attacks to suppress SM messages and shape the SM campaign.

The study team also identified the potential impact SM will have directly on Army operations:

1. Diminished tactical surprise and covert operations. Future Army combat engagements will be reported via live SM feeds and recorded and broadcast using SM video capabilities. All conflicts will provide real time content in SM and SM will generate time-critical targets during conflicts. Because of the ubiquitous nature of SM coverage of armed conflicts, tactical surprise on the battlefield will become increasingly difficult to create, both for U.S. forces and for adversaries.

2. Universal use of SM. Allies, adversaries, and non-combatants will use SM for operations, including nation states and non-state actors. Because of the easy access to SM tools and SM's global reach, this shift will move beyond asymmetric warfare, where individuals and distributed cells of adversaries will have disproportionate impact on conflicts. Indications of this trend towards universal use of SM for conflicts include the UK's 77th "Facebook Brigade," with two thousand members, the IDF's use of SM in Gaza, the recent opening of the Sawab Center in the UAE to combat ISIS, and various SM campaigns by Russia, China, Syria and ISIS.

3. Use of SM as a part of Army combined arms. In the future, the Army's real-time SM will be combined with Army cyber-attacks and EW, as well as SM-directed kinetic attacks. The recent USAF JDAM attack on an ISIL leader who was located using SM data is an example of the coupling of SM, intelligence exploitation, and kinematic response. In the future, SM battles will be an integrated part of the Cyber warfare domain, including defensive cyber operations, EW, and MISO. In turn, the integrated cyber suite of tools will coordinate in real-time with intelligence and kinetic operations for overall mission effectiveness.

4. Changes in the role of Army Public Affairs Officer (PAO) due to SM. The digitization and personalization of media is having a profound effect in all aspects of public affairs (PA). The Army PAO provides truthful information to our Soldiers and citizens. Deliberate efforts to influence fall outside the purview of the PAO, causing the US to lag in SM influence operations. In the future, Army PAO activities will be exclusively digital, including real-time SM interactions with U.S. citizens, coalition partners, and adversaries. Adversaries will increase use of SM to attack U.S. Soldiers and families, and to recruit U.S. citizens vulnerable to influence. This trend will require the PAO to engage our adversaries by providing dynamic, truthful information to counter their SM operations.

5.0 ARMY SOCIAL MEDIA OVERMATCH CAPABILITY

Figure 5.1 The U.S. Army on Twitter and Facebook

The Army will have to fight on two fronts in the new SM battlespace.

Army PA units, whose mission is to disperse information, employ some SM platforms such as Facebook and Twitter (Fig. 5.1), but PA personnel have limited or no formal training in their use. The PA forces have also been substantially reduced in strength since the end of Operating Enduring Freedom. Thus, while the Army faces growing challenges from adversaries' use of SM, it isn't postured to match or counter those efforts.

The Army also supports MISO for the COCOMs, primarily through USSOCOM. The Army's MISO operators mostly come from the reserves and focus on traditional media. As a result, the Army's SM operations used for influence and intelligence OCONUS is fragmented, ad hoc, and unable to keep pace with modern military operations. So, again, while the Army faces growing challenges from adversaries' use of SM, it isn't postured to field an overmatch to those efforts.

Even once the Army establishes a SM capability and can effectively counter adversary SM operations, it will face a pernicious challenge: the enemy's ability to contrive stories and shape reality through false messages. According to the head of IDF's social media operations:

> One of the big challenges for me dealing with digital media is the rumors and falsehoods, we have to be constantly aware, monitor the Web sites and the different platforms and make sure any such rumor would be immediately discovered. We have to do it within a couple of minutes because otherwise it can virally spread and it will be a totally different situation.[24]

[24] http://www.cnet.com/news/how-israel-and-hamas-weaponized-social-media

The Army's hierarchical structure, coupled with its dense bureaucracy, challenges the agility and speed necessary to managing strategic communications.

One final, less obvious challenge the Army will face comes from within its own ranks. The ability of any Soldier to post video or photos instantaneously through social media can compromise security, and potentially incite local populations to support or directly join the enemy. Perhaps the starkest example of this phenomena occurred around the release of photos from Abu Ghraib during Operation Iraqi Freedom.

5.1 TECHNIQUES

Leveraging SM as a platform to shape the narrative and/or to initiate counter efforts against enemy messaging will require coordinated and skilled approaches by Army personnel. The Army's SM operatives will need to understand the target culture and will need to become adept at crafting messages to advance a particular mission as well as the larger, strategic goals of the Army.

Beyond the skill sets required of future Arm SM operators, there are three leading techniques that will help the Army develop a SM overmatch capability:

1. Social Media Influence Operations. One of the key findings from a DARPA simulation was that "Influence campaigns involving bots continue to be both impactful and cost-effective." The DARPA team was able to demonstrate the bots' ability to engage with a large number of Twitter users on a political issue. However, confirming bot participation in influence operations remains a challenge at this point.[25]

2. Fact checking tools. Identifying false photos on social media is now possible with tools like Google image search and TinEye, which can quickly fact-check where a picture came from. Likewise, the use of Snopes and Storyful are helpful in verifying content.[26]

3. Cognitive ISR. Monitoring social media within an area of operational interest allows US forces to maintain a sense of what is happening on the ground, even if they do not have human or technological intelligence assets in the area.

5.2 OPERATIONS CONCEPT

Controlling human behavior, whether it's that of our Soldiers, non-combatants, and/or adversaries, is core to the mission of the Army, and SM can be a powerful tool to execute that mission. As outlined above, adversaries have demonstrated the use of SM tools to influence behaviors, and the speed and volume of SM information has been observed to disrupt the decision cycle of Army commanders in the field. Since adversaries are not limited by the same

[25] SMISC Detection Final Report, April 30, 2015
[26] http://www.cnet.com/news/how-israel-and-hamas-weaponized-social-media/

command and control structure as the Army's, an agile, operational SM capability with clear authority will be required as to win back this new battlespace.

To attain these objectives, the Army's SM operations will have to have specific elements and enablers (Fig, 5.2). It will be crucial for the SM function to operate continuously, before Phase 0, in order to know the audience and environment in the AO. This means developing SM relationships within the AO, understanding the SM influencers and social context, and preparing media (video, text, images) for use when conflict arises. The development of allies and the identification of potential adversaries is critical as a part of the SM intelligence preparation of the battlefield (IPB), as is the continuous collection of SM intelligence, including the adversary's messaging and SM channels, threats, HVTs and influencers, and counter-messaging to U.S. SM messages. This SM IPB requires continuous, real-time monitoring, so responses can occur in internet time (within minutes).

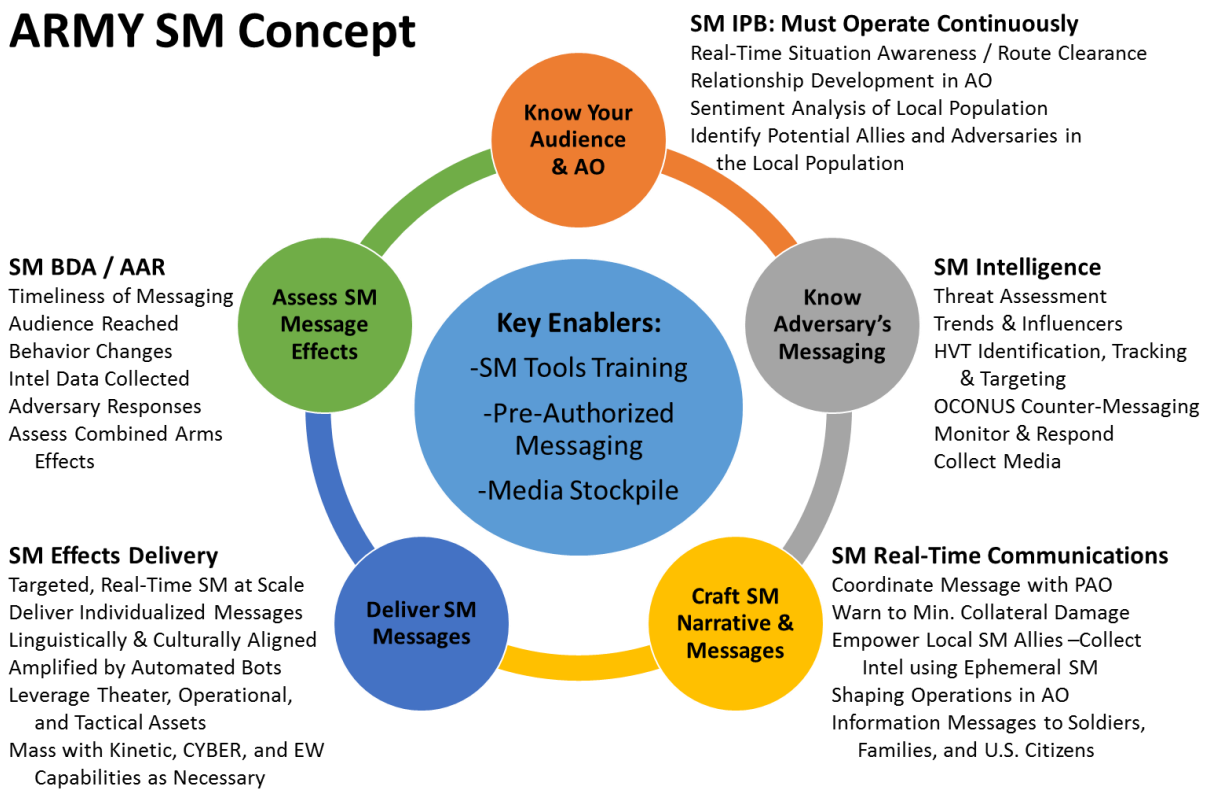

Figure 5.2 Elements of an Army SM Operational Capability

Once SM targets are identified within the context of the AO, SM messages can be created. These messages should align with the overall SM narrative specified by the Department of State and Coalition partners. Coordination of SM messaging to eliminate SM fratricide, or the countering friendly messages. Messages can be crafted for adversaries, potential recruits for adversaries, U.S. Soldiers and families, and Coalition troops. SM messaging can be used for shaping operations within the AO, as well as identifying friendly local allies that can use ephemeral SM (SM that deletes itself from

devices to avoid producing evidence) to report on troop movements, equipment, and plans of the adversary.

Once the narrative and SM messaging have been created and aligned, the SM message is delivered in real-time to targeted audience. Because of the nature of SM, individualized messaging can be tailored to each individual linguistically and culturally, while still sending SM at massive scale. The effect of the SM messaging can be amplified using automated bots, which can also support measurement of the effects of the SM campaign. The SM messaging can also be combined with cyber, kinetic, and EW capabilities to increase the total effect. SM battle damage assessment can be measured in terms of the timeliness of the response, the percent of the target audience reached, specific online behavior changes, the amount of intelligence data captured, the subsequent response of the adversary, and the overall combined arms effects, including actions on the ground.

5.3 ENABLERS

To establish and sustain an Army SM overmatch capability, the study team focused on these enablers:

1. Policy and legal considerations. There should be a comprehensive SM policy or a legal framework for employing SM in an operational environment so that commanders understand their constraints and capabilities. Legal issues exist with respect to informing versus influencing, and policy issues exist with respect to authorization of specific messaging.

> Information-related capabilities—such as military deception … provide support to the influence line of effort. The influence line of effort is most closely associated with the information operations of joint operations and is adversary focused.[27]

MISO is charged with information operations (IO),[28] and the effective use of SM to create an overmatch capability could extend the MISO mission onto the battlefield, creating mass with kinetic, cyber, and EW capabilities. Thus, gaps in legal and policy frameworks need to be addressed to enable the operationalization of SM.

2. Army real-time SM operations and training. The ability to effectively deploy real-time SM on the battlefield will be hampered by a bureaucratic approval structure with limited ability to respond to time urgent situations. Currently, the difference between what the Army can do compared to what adversaries can do is on the order of days versus minutes. Effective operations require SM content creation, in the stockpiling or queuing of pre-approved messages, and in its access to tools that ensure socially, culturally, and linguistically appropriate messages. An effective SM strategy must start with a presence in country prior to Phase 0 (i.e., prior to any named operation), and continue through all

[27] FM 3-13, 2-2 Information Operations and Strategic Communication
[28] As delineated in DOD Directive 3600.01, Information Operations

phases of the operation. SM measures of effectiveness and after-action procedures must be established to gauge the effectiveness of tools, tactics, and procedures. Formal training on how to employ SM for operators and commanders must also be established. Such training exists in other military organizations, for example, NATO's training program could provide a framework for the Army.

3. Technical infrastructure and research. IT and organizational Infrastructure is required for large-scale, real-time, operational and tactical SM missions. Furthermore, the Army does not have a simulation integration laboratory (SIL) for identifying, testing, integrating and deploying SM tools, or a program for leveraging advances in artificial intelligence and SM bots. Finally, creating a process for identifying adversaries, identifying misinformation, and finding fake profiles within SM to allow for effective operations in the AO is a major challenge. Current research funding is insignificant and will be unable to address these shortfalls. DARPA has conducted relevant research in the past, but current research is mainly in the commercial sector and therefore does not include Army mission relevant research on the psychology of SM influence, tools and analytics, or refining measures of effectiveness for SM tools.

4. Public Affairs Officer (PAO). SM is employed by the PAO in a limited manner and may be generally categorized as the sharing of positive image vignettes, including photography and video. The Army Facebook page has almost 4.1 million followers; the Army on Twitter has a lesser reach of approximately 900 thousand followers. The Army PAO should be staffed for the enormous audience it serves.

The study team did observe SM being used by the Army, but in each case, the effectiveness of the application was limited by the ad hoc nature of the efforts and the lack of synchronization between State Department, COCOMS and/or other Service SM operations. Organizational expertise was lost each time an individual changed assignments because the SM procedures were not captured as part of the individual's essential duties.

6.0 SUMMARY

The study team's findings and recommendations are classified and published separately as an annex to this report. The classified annex provides findings on the weaponization of SM, the global saturation of SM, SM challenges to the Army, leading edge methodologies, emerging trends in SM, and the Army's HI overmatch capability. The study team's recommendations cover the authority and resourcing for an Army SM operation, the roles and responsibilities associated with the Army SM mission, and the execution of that mission.

Access to the classified annex will be made available for individuals with appropriate security clearance and need to know. For access, contact the Executive Director, Army Science Board, 2530 Crystal Drive, Suite 7098, Arlington, VA 22202-3911.

APPENDIX A. TERMS OF REFERENCE

SECRETARY OF THE ARMY
WASHINGTON
JAN 06 2015

Dr. James A. Tegnelia
Chairman, Army Science Board
101 Army Pentagon
Washington, DC 20310

Dear Dr. Tegnelia:

I request that the Army Science Board (ASB) conduct a study entitled "Human Interaction and Behavioral Enhancement."

The Army is increasingly required to conduct operations in large population areas where the perceptions held by non-combatants, and their associated behaviors, significantly affect the probability of mission success. Potential opponents recognize the impact of influencing populations and are taking advantage of social networking and other forms of information technology to shape opinions and behavior, to the detriment of U.S. achievements. To counter our adversaries' efforts, deliberate techniques, and procedures for interacting with local populations will be critical to achieving success in future military operations. Failure to take advantage of advanced human interaction capabilities will reduce the Army's range of tactical options and will leave this space open for exploitation by enemy forces.

The purpose of the study is to identify and assess methods and techniques to understand, interact and influence human behavior in support of Army missions. Recommendations and findings must be supported by sound systems analysis.

The study tasks should include, but not necessarily be limited by, the following terms of reference (TOR):

a. Identify and assess the most effective current and leading edge methods and techniques from commercial businesses, academia and other military services that could establish a "human interaction overmatch capability" to the Army.

b. Identify emerging concepts, technologies and procedures that have the potential to disrupt enemy activities by significantly enabling the Army's interaction with people in foreign countries and influencing their attitudes and behavior.

c. Determine specific elements of the force capable of taking lead on influencing human behavior through social media or other non-kinetic means, and identify their responsibilities in this area. In addition, examine the potential roles and capabilities that all ground forces may adopt to influence human behavior.

d. Describe how the Army should prepare specific functional units and ground forces as a whole for human interaction, and recommend how to sustain those capabilities.

The Deputy Under Secretary of the Army (DUSA) is the sponsor of this study. The ASB must present a comprehensive briefing to the DUSA and me by September 30, 2015. The final written report must be provided by October 31, 2015. The supporting data for findings and recommendations need to be available to Army senior leaders upon request.

The study will operate in accordance with the Federal Advisory Committee Act and Department of Defense (DoD) Directive 5104.4, "DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of Title 18 United States Code Section 208, nor will it cause any member to be placed in the position of acting as a procurement official.

Sincerely,

John M. McHugh

APPENDIX B. STUDY TEAM MEMBERS

Dr. Mike Macedonia, Chair

Dr. Bruce Swett, Vice Chair

Dr. Jill Keith

Margaret Kulungowski

Dr. Lester Martinez-Lopez (MG-Ret)

Dr. Maria Mouratidis

Evelyn Mullen

Dr. Olugbemiga Olatidoye

Dr. Grant Warner

Dr. Sung Lee

William Guyton

Scott Gilman

LTC J.J. Dalle Lucca, Study Manager

LTC Grant Morris, Study Manager

Mark Swiatek, Tech Writer/Editor

APPENDIX C. GLOSSARY OF KEY TERMS

Bots – Simple computer program used to perform highly repetitive operations

Cognitive Security – Protection against adversarial SM influence

Cognitive Intelligence, Surveillance, and Reconnaissance (ISR) – Using SM as a sensor platform

Filter Bubble – Customized results from search engines that are geared to the individual based on that person's past search preferences

Inform – To give (someone) facts or information; Influence: The capacity to have an effect on the character, development, or behavior of someone or something, or the effect itself

Open-source intelligence (OSINT) – DOD Information of potential intelligence value that is available to the general public

Social Media (SM) – Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (e.g., video)

Social Media Communities – Online forums for social interaction; Feeds: Real-time streams of SM content; Ephemerals: SM channels that delete automatically