REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188

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 this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. 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 ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) 16-04-2021	2. REPORT TYPE FINAL	3. DATES COVERED (From - To) DEC 2020 – APR 2021

4. TITLE AND SUBTITLE #WarLeveragingSocialMedia	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S) MAJ Christopher E. Stutzman Paper Advisor: Mr. John M. Sappenfield, Associate Professor	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES) Maritime Advanced Warfighting School Naval War College 686 Cushing Road Newport, RI 02841-1207	8. PERFORMING ORGANIZATION REPORT

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
Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES
A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT
#WarLeveragingSocialMedia
Incorporating social media into the intelligence cycles, JIPOE, and planning phases of operations will significantly increase theater commanders' ability to gain the initiative against both hostile state and non-state actors. Social media defines, describes, and informs a commander and their staff to fully understand and visualize the operating environment. Commanders and staff can leverage that understanding to enable higher quality decisions, which translate into more effective future operational plans, and enhanced mission command. Social media provides unique opportunities to exploit an enemy or insurgency's ad hoc command-and-control structure, allowing U.S. forces to disrupt future and potential plans. This document discusses two case studies from the Arab Spring and relates those case studies and the lessons learned from social media's impact and its applications as the United States transitions to great power competition.

15. SUBJECT TERMS
Intel, JIPOE, OPART, Social Media, decision making, operating environment, Fake News

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Director, MAWS
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED		26	19b. TELEPHONE NUMBER (include area code) 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

#WarLeveragingSocialMedia

by

Christopher E. Stutzman

Major, U.S. Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Maritime Advanced Warfighting School.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

18 APR 2021

Contents

List of Illustrations

Abstract

Incorporating social media into the intelligence cycles, JIPOE, and planning phases of operations will significantly increase theater commanders' ability to gain the initiative against both hostile state and non-state actors. Social media defines, describes, and informs a commander and their staff to understand and visualize the operating environment fully. Commanders and staff can leverage that understanding to enable higher quality decisions, translating into more effective future operational plans and enhanced mission command. Social media provides unique opportunities to exploit an enemy or insurgency's ad hoc command-and-control structure, allowing U.S. forces to disrupt future and potential plans. This document discusses two case studies from the Arab Spring. It relates those case studies and the lessons learned from social media's impact and its applications as the United States transitions to great power competition.

Introduction

Social media traces its beginnings to the 1990s with simple school-centric sites such as classmates.com and sixdegrees.com. Social media expanded its reach during the next decade, evolving into powerhouses such as MySpace, Facebook, Twitter, and Instagram.[1] Today, people across the globe use hundreds of social media platforms to communicate, share information, organize, and connect with each other, as they bond over their shared interest in increasingly atomized niches, such as sharing one's favorite beer with friends using Untapped or posting one's latest academic paper for review by fellow researchers on Academia.[2] Recently, social media played a role in the U.S. Capitol insurrection, enabling domestic terrorists to organize and storm the Capitol.

With hundreds of social media platforms available, state and non-state actors have weaponized their use. Incorporating social media in the joint intelligence preparation of the operational environment (JIPOE) and planning phases will enable theater commanders to gain the initiative and have higher quality decision-making against hostile state and non-state actors. First, social media defines, describes, and informs a commander and their staff to fully understand and visualize the operating environment. Second, commanders and staff can leverage that understanding to enable higher quality decisions, translating into more effective future operational plans and enhanced mission command. Lastly, social media can exploit ad hoc command-and-control structures, creating unique opportunities to exploit the enemy's operations and counter the enemy's ability to conduct command-and-control effectively.

---

[1] Chenda Ngak, "Then and Now: A History of Social Networking Sites." . Accessed Feb 27, 2021.
[2] "101+ Social Media Sites You Need to Know in 2021." . Accessed Mar 11, 2021. https://influencermarketinghub.com/social-media-sites/.

Social Media's Role in the Arab Spring

Social media, at its heart, is a communication platform that allows grandmothers to see pictures and videos of their grandchildren, politicians to update their constituents about a pressing issue, or hostile state or non-state actors to spread their propaganda and battle plans to their supporters. Social media influenced the events of the Arab Spring in Tunisia, Egypt, Iran, and Afghanistan.[3] Social media enabled the local populace to organize and raise awareness of government overreach and corruption against citizens. Protests within the region are not new, and before social media became prevalent, the events that occurred could have happened with little to no reaction from the local populace. What was new for the region was the ability of social media to reach the masses. Key to these case studies and key for commanders to understand is the reach that social media has. A single tweet by a 'Kim Kardashian' or any significant internet influencer within a region can exponentially spread that information within hours (see figure 1). Had these events occurred before social media's widespread use, it would be doubtful, if not improbable, that any change would have occurred within the region.

---

[3] Dennis Wille, *Every Soldier a Messenger: Using Social Media in the Contemporary Operating Environment* U.S. Army Command and General Staff College, 2012. P24

Figure 1: Graphical representation of how fast a tweet can spread across a population.[4]

Tunisia 2010 – 2011

Mohamed Bouazizi, a young street merchant, lit himself on fire in protest, having suffered years of abuse from the Tunisian government. Ever since Bouazizi was a young child selling fruit, he was continually extorted by the police, while the government refused to listen to his grievances.[5] His family began to protest the corrupt Tunisian government. These protests were recorded and uploaded to YouTube, gaining regional and international traction due to social media.[6] Local influencers, the 'Kim Kardashian's' of the region, posted his self-immolation video and his family's initial protest. Within days, it led to organized protests and outrage throughout the country and internationally. The timeline of events is what is most telling.

---

[4] *Who is spreading fake news on Twitter?* in Brian Resnick, "On Twitter, False News Travels Faster than True Stories." . https://www.vox.com/science-and-health/2018/3/8/17085928/fake-news-study-mit-science.
[5] Nathanael Burnore. *Social Media Applications for Unconventional Warfare*. U.S. Army Command and General Staff College, 2014. P24
[6] Wille, *Every Solider a Messenger: Using Social Media in the Contemporary Operating Environment* P34

Bouazizi lights himself on fire on 17 December 2010, and influencers post his story on social media. Protests begin on 18 December, intensifying through 13 January 2011, with police killing dozens of protesters. On 13 January, President Ben Ali states he will not seek reelection in 2014. On 14 January, Ali and his family flee to Saudi Arabia.[7] Tunisia's government changed in 26 days due to social media's capabilities, increasing protests' scale and intensity. Had Bouazizi's story only been broadcast on the nightly news or within local newspapers, it would have been one story drowned out by many. With social media, anyone who favored change within Tunisia had an international platform to speak, organize, and effect change within the region.

Egypt 2010 – 2011

Much like the Tunisian example, social media played a massive role in the Egyptian Arab Spring. In June 2010, Khaled Mohamed Saeed, a computer programmer, died while in Egyptian police custody after allegedly being beaten to death during his arrest.[8] Wael Ghonim, a fellow computer scientist, turned internet activist, created a Facebook page to commemorate Saeed's life and end police corruption and brutality within Egypt.[9] Due to Ghonim's social media influence in the region, organized protests, styled the "Day of Revolution," spread throughout the country, disrupting Cairo, Alexandria, Mansour, and Suez, peaking on 25 January 2011, six months after Saeed's death. The goal of the protests was to force the resignation of Egypt's longtime President, Hosni Mubarak.[10] On 1 February, Mubarak stated he would not resign until

[7] Elie Abouaoun. "Tunisia Timeline: Since the Jasmine Revolution." *United State Institute of Peace* (July 12, 2019). https://www.usip.org/tunisia-timeline-jasmine-revolution.
[8] Ashraf Khalil. "Anger in Alexandria: 'We're Afraid of our Own Government'." . Accessed Mar 15, 2021. https://web.archive.org/web/20110427172608/http://www.almasryalyoum.com/en/node/51909.
[9] Wille *Every Solider a Messenger: Using Social Media in the Contemporary Operating Environment* P34
[10] Darrett Nada, and Mattisan Rowan. "Egypt Timeline: Since the Arab Uprising." *United State Institute of Peace* (July 2, 2019). https://www.usip.org/egypt-timeline-arab-uprising.

his term expired in September; however, on 11 February, Mubarak abdicated his position. On 14 February, the provisional government announced a six-month plan to establish a new government.[11] The swift change in the Egyptian government was primarily due to the increasingly widespread use and power of social media. Before the protests, on average, Egyptians tweeted 23,000 times a day.   However, in the week before Mubarak's resignation, Egyptian tweets expanded to over 230,000 times a day.[12] The increase in social media usage correlated directly with the surge in violence and resistance toward the Egyptian government.

Defining the Operating Environment

Social media is a tool that allows commanders and staff to understand, visualize, and describe the operational environment at the strategic and operational levels of war. First, following the lead of several tech giants, the U.S. Military can describe the operating environment through local interests and shared intent. Second, commanders and staff can use trending information to understand the operating environment and depict political, military, economic, social, information, and infrastructure (PMESII). Third, by incorporating social media posts and consolidating the information on a combined operating picture (COP) overlay, that data will give commanders added visualization to operate more effectively within their theater of operations.

Much like marketing and tech giants such as Apple, Amazon, Google, and countless others, the U.S. Military can use social media to mine data and information that describes the local population's interests and intent. Amazon, Google, and Facebook advertise based upon

---

[11] Nada, Darrett, and Mattisan Rowan. "Egypt Timeline: Since the Arab Uprising." *United State Institute of Peace* (July 2, 2019). https://www.usip.org/egypt-timeline-arab-uprising.
[12] Philip Howard, Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad. *Opening Closed Regimes: What was the Role of Social Media during the Arab Spring?*, 2011.

what their users would like to buy. Using cookies to identify computers, computer networks, and users, these sites collect internet browsing history and develop personalized advertisements.[13] Similarly, anyone using an open-source social media site can gain location data from geotagged or locational metadata found in some photographs, text messages, websites, or videos. Using this data has been helpful at the tactical level. In 2015 the U.S. conducted an airstrike on the Islamic State of Iraq and the Levant (ISIL) headquarters building from a social media post containing a geotagged picture.[14] Building upon the tactical applications, intelligence collectors and analysts can combine multiple metadata postings. By filtering these posts and building data about an enemy force, analysts can begin answering the questions of who, where, what, or when.[15] The ability to filter this metadata can better describe the operating environment through time-space-force factors using operational art.

Suppose the United States goes to war with the Democratic Republic of North Korea (DPRK). As DPRK invades South Korea, South Koreans will likely post information and pictures on social media about the invasion. From these posts, we will gain valuable intelligence describing troop locations, disposition, and composition, potentially identifying movement times, and building a pattern of life, all because of social media data aggregation. This will enable current operations and impact future operations by predicting the enemy's next move. Conducting predictive analysis will lead planners to develop better plans. Commanders will make higher caliber informed decisions and accept prudent risk due to predictive analysis, allowing friendly forces to array themselves in more advantageous positions to defeat the enemy.

---

[13] Karen Weise, "Amazon Knows what You Buy. and It's Building a Big Ad Business from It." *NYTimes.Com Feed,* Jan 20, 2019. https://global.factiva.com/en/du/article.asp?accessionno=NYTFEED020190120ef1k002p9.
[14] William Marcellino, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, 2017 P11
[15] B Forrester, and K. den Hollander, "The Role of Social Media in the Intelligence Cycle." (Jan 1, 2016). P7

After describing our environment, commanders and staff must understand it. Using social media trends, whether for hostile, neutral or friendly intent, enables a better depiction of the PMESII environment, which gives commanders and staff a better understanding of their operating environment and the series of networks within a given theater. In Syria, for example, regional actors opposing ISIL use social media to identify, network, and employ key influencers within the region to steer supporters away from ISIL by conducting keyword searches such as 'Daesh,' a local term for ISIL used by those who oppose them.[16] By doing this, they were able to identify resistance within the local population and recruit others against ISIL. Social media enables private citizens to publish content, live stream, and post their version of the news.[17] Graphically depicting support or influence during phase 0 or I of military conflicts will enable theater commanders to understand the operating environment better. If conducted before the deployment of forces, it will enable critical support locations (see Figure 2). Understanding the operating environment through social media gives our forces the initiative, leading to greater success.

---

[16] Marcellino, *Monitoring Social Media* P12
[17] Forrester. and Hollander. "The Role of Social Media in the Intelligence Cycle." P7
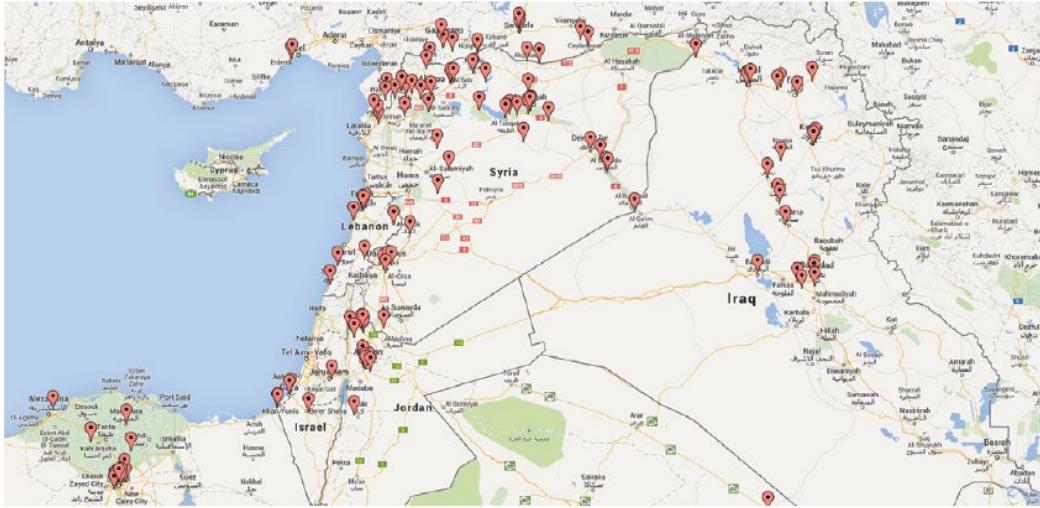
Figure 2: 2014 Brookings Institute Study of ISIL supported tweets in one out of their last two-hundred tweets. [18]

Once a commander and their staff understand the operating environment, they must visualize it. As described earlier when discussing geotagging, geotagged social media posts projected on a graphical COP allow commanders and their subordinates to visualize the battlefield accurately. With this geotagged data, analysts can predict adversary networks and their connections to the area.[19] In 2007, Iraqi insurgents did just that, targeting an airfield in Iraq from a soldier unknowingly posting a geotagged picture of his section in front of their Blackhawk.[20] Insurgents could pinpoint targets based on pictures posted online. Following those principles, as our analysts collect and consolidate data onto an operational overlay, our planners can then begin developing the plan based on their visualization of the environment. Consolidating the data enables refined objective development, operational fires, and the nesting of tactical and operational level objectives towards the strategic objective.

---

[18] *Figure 1* in J.M. Berger and Jonathon Morgan. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*: Brookings Institution, 2015. P10
[19] Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*. Latvia: NATO Strategic Communications Centre of Excellence, 2016. P13
[20] "Insurgents used Cell Phone Geotags to Destroy AH-64s in Iraq." . Accessed Feb 27, 2021. https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq#:~:text=Here's%20a%20battlefield%20safety%20issue,of%20troops%20on%20a%20battlefield.

Using social media to better describe, understand, and visualize the operational environment will enable commanders and their staff to refine JIPOE and better appreciate their current or future operating environment. Describing the environment using geotagged data, as marketing companies do, provides information on the region's interests and intent. Aggregating that data and depicting it within a PMESII matrix creates a better understanding of the environment. Lastly, presenting all that information graphically allows the commander to visualize the operating environment better, leading to greater effects when using operational functions as they proceed to conflict.

Planning with Social Media

After understanding the operational environment through social media, operational commanders can use this advanced knowledge of the environment to improve plans, enabling a higher quality of decisions and operational plans. First, as social media can identify thoughts, trends, or the local population's radicalization, commanders and their staff can use those trends to identify locations and population-dense areas to support or counter those trends. Second, planners can understand how changing governments and non-state actors attempt to influence public opinion within the region. Lastly, by understanding trends, radicalization, and how governments and non-state actors attempt to persuade their populations, operational level commanders can use that information to recruit support for both operations and influencers within their theater of operations.

Using social media trends that identify public sentiment or radicalization among the local population, commanders and their staff can plan future operations to counter those thoughts or trends. Personnel with significant influence, such as political leaders, military leaders, celebrities, or even internet influencers, can show the regional perspective from their official

social media accounts.[21] Filtering views opposing those of government officials can identify the likelihood of dissension or radicalization. Monitoring those trends within the region will incorporate safeguards against possible undesired effects in planned operations, decreasing the requirement to develop branch plans and utilize those plans in the future. This will enable commanders at all echelons to prevent or slow the spread of undesired effects due to social media, enhancing mission command. Had local government officials monitored social media trends in Egypt and Tunisia during the Arab Spring, they could have predicted the spread of protests and worked toward slowing radicalization and avoiding governmental change.

Additionally, tracking trends of government officials will enable a better understanding of public thought and resistance. President Hassan Rouhani of Iran tweeted from his official government account on 22 September 2020, "Future U.S. administrations need to understand that the resilient Iranian nation will not Surrender."[22] This tweet received over 2,100 comments, 356 re-tweets, and 1,200 shares. In a simple human review of the comments, one can already find dissension from Rouhani. Twitter handle '@IranDemocracy' replied with a tweeted video showing human rights violations; Twitter handle '@baronessedulac,' an Iranian influencer replied, "you are a criminal," with several other tweets from several other individuals with opposing remarks.[23] Based on a simple human review of open-source social media posts, we can gather information supporting or lacking support for the Iranian government through Rouhani's Twitter account. As previously discussed, conducting this on a grander scale and mapping out

---

[21] Svetoka, *Social Media as a Tool of Hybrid Warfare*. P17
[22] "Hassan Rouhani on Twitter." Accessed Mar 15, 2021
https://twitter.com/HassanRouhani/status/1308460495809196032.
[23] "Hassan Rouhani on Twitter." Accessed Mar 15, 2021
https://twitter.com/HassanRouhani/status/1308460495809196032

their locations will identify friendly and hostile areas within the region. Having this information will give insight into future operations within the region.

Suppose the United States goes to war with Iran. Using information drawn from social media, we can identify that @baronessedulac is fairly influential within the region, with 2,272 followers,[24] as is @IranDemocracy with 2,736.[25] Combine that with geotagged information, and planners can begin to identify locations of support for American operations. Doing so will give commanders the ability to establish regional influence amongst a generally supportive population. Additionally, looking at supporting comments of Rouhani combined with geotagged information likely paint a picture of heavily contested regional areas that operational commanders and their staff will need to plan against. Using these social influencers within the region could expand on pro-United States support, discrediting the Iranian government further.

Similarly, commanders within regions that are in phase 0 of conflict or regions with changing governments can use social media to see what these governments are doing to influence local public opinion. Within the 2018 National Defense Strategy, the secretary of defense outlines the four-state threats, Russia, China, DPRK, and Iran. [26] China and Russia have actively used social media to coordinate marketing campaigns to spread pro-government propaganda, promote messaging to sway their population based on supporting government agenda, and criticize political opponents and opinions.[27] In a 2018 study, the RAND Corporation concluded that Russia's social media propaganda focus is on former USSR and Russian-speaking countries, influencing the common idea believed by many that "the West in the

[24] "Baronessedulac." Accessed Mar 15, 2021. https://twitter.com/baronessedulac.
[25] "Iran Democracy." Accessed Mar 15, 2021. https://twitter.com/IranDemoracy.
[26] Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, 2018.P1
[27] Marcellino, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations* P15

late 1990s betrayed them by failing to deliver on promises of prosperity".[28] Essentially this makes Russia's job easier. They now can use marketing techniques to further fracture relationships between Eastern European countries and the rest of Europe and the United States.

With five NATO-allied countries bordering Russia, this can create a quagmire. Monitoring social media in countries such as Estonia and Latvia, which have significant Russian populations, can provide U.S. commanders more insight into military relationships during specific exercises. The United States European Command (EUCOM) conducts several annual training exercises in Europe, such as Swift Response and Rapid Trident, training Ukrainians alongside NATO allies, such as Estonians, to protect Ukraine's sovereignty.[29] Suppose members of the Estonian Parliament begin posting or reposting Russian social media propaganda during a training event. Such postings can predict dwindling U.S. support within the region, leading to an unfortunate turn of events. By monitoring this activity, commanders can position their forces more advantageously against threats from an enemy or an impending enemy.

Monitoring governmental changes within social media will also enable commanders to gain local populace support for U.S.-based objectives as we transition into phase I through phase V of operational conflicts, enabling a faster transition to local civil authority. Special operations forces in the late 2000s through mid-2010s used Village Stability Operations (VSO) on a small tactical scale to develop local police and recruit Afghans to join the military and fight against Taliban and Al-Qaeda to stabilize insurgent strong points. They focused "on the center of

---

[28] Todd C.Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. *Russian Social Media Influence*. Santa Monica, Calif: RAND Corporation, 2018.
[29] Davis Winkie. "Rapid Trident 20 Exercise Kicks Off in Ukraine with Fewer US Troops than Last Year." *Army Times,* Sep, 14, 2020. https://www.armytimes.com/2020/09/14/rapid-trident-20-exercise-kicks-off-in-ukraine-with-fewer-us-troops-than-last-year/.

gravity – the population."[30] This concept is not groundbreaking and is a principle of counter-

insurgency operations. Using the same principles, commanders can use this technique at the

operational level geared toward great power competition. In Russia, China, Iran, or the DPRK,

the United States can recruit influencers that sway the local population toward U.S.-backed

ideas. Using open-sourced social media information, such as those who follow

@IranDemocracy and @baronessedulac, operational level commanders can task their public

affairs officers and intel section to map social media networks for those supporting U.S. interests

(see Figure 3). Using the influencers will allow a faster transition to Phase V with more

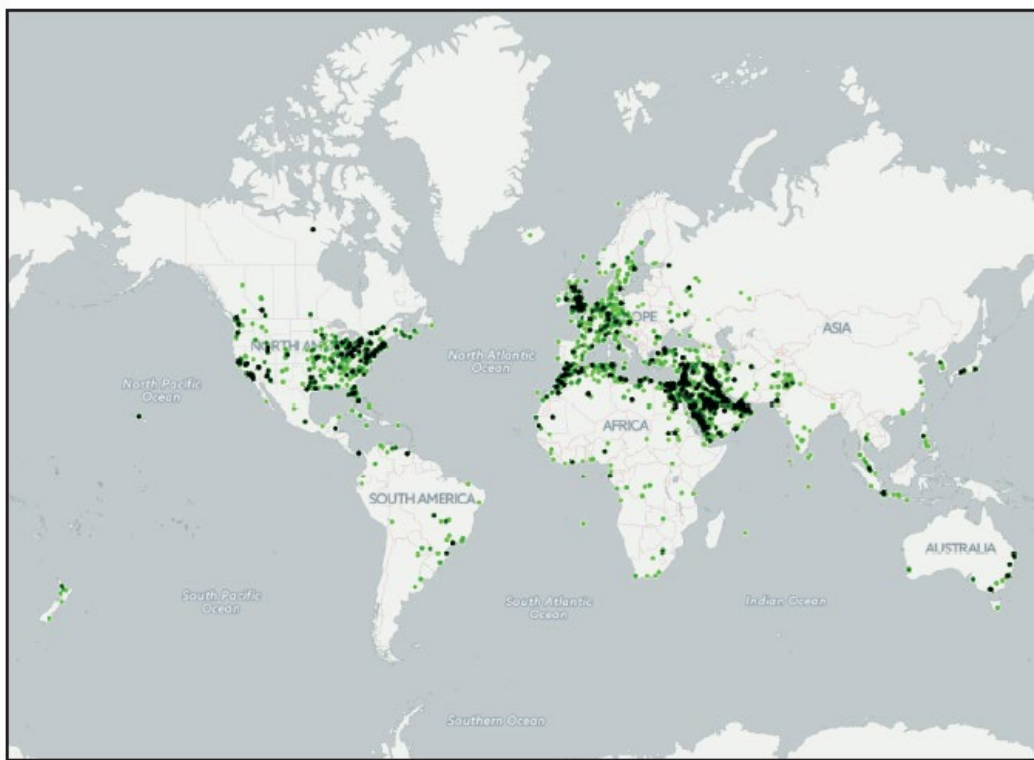extensive support for a U.S.-backed local civil authority.

Figure 3: July 2014- May 2015 Global tweets against ISIL, dark green represents a larger anti-ISIL Tweet volume.
[31]

---

[30] Ty Connett, and Bob Cassidy. "Village Stability Operations: More than Village Defense." *Special Warfare* 24, no. 3 (Sep, 2011). https://www.soc.mil/SWCS/SWmag/archive/SW2403/

[31] *Figure 2.3* in Elizabeth Bodine-Barron, Todd Helmus, Madeline Magnuson, and Zev Winkelman. *Examining ISIL Support and Opposition Networks on Twitter* RAND Corporation, 2016.

Incorporating social media into planning future operations enhances operational plans. Improved plans will aid mission command and support improved decision-making across all echelons of command. First, it will identify the local population's trends and popular support, whether aligned with U.S. objectives or not. Second, planners and commanders can begin identifying any changing governmental ideas and messaging, potentially identifying public opinion changes. Lastly, by compiling this information, operational commanders can recruit support through local influencers, improving the local population sentiment for U.S.-based objectives and ideals, leading to a faster transition toward supporting civil authority.

Counter-Command and Control

As noted above, social media is a communication platform. It gives people the ability to connect and communicate with many people quickly. Through prompt analysis and dissemination, social media's nature can help commanders affect current operations at the operational and tactical levels. First, social media can map the interweb of connections to determine a particular group's size and formation, whether it may be a foreign military or a non-state actor, and identify any ad hoc command-and-control structure. Second, it can provide real-time situational awareness on what these groups are currently doing, supporting operational commanders' allocation of resources to subordinate tactical commanders. Lastly, social media's open-source nature allows commanders and their staff to monitor an enemy's communication and capitalize on poor operational security practices.

Social media can help map out particular groups and network their connections to each other, ultimately providing the information to understand their command-and-control application. A 2018 RAND corporation study, based on a sample size of 20,000 Twitter users' ISIL-supported tweets with locational data-enabled, concluded that most tweets originated from

ISIL-contested territory.[32] Incorporating this kind of analysis, planners can begin identifying

command-and-control nodes. ISIL, for example, used social media as their primary means of

communication and coordination of operations, using an encrypted chat feature available on the

PlayStation network.[33] Having the disposition of enemy networks and the adversary's

communication means, gives operational and tactical commanders an advantage. While

knowing the enemy locations will greatly help tactical operations, knowing their command-and-

control platform is an operational game-changer. Planners can then focus on non-kinetic forms

of shaping, such as cyber and electronic warfare, to dismantle their command structure, thus

degrading or preventing an enemy operation from occurring. For both state and non-state actors,

dismantling a communication platform creates second and third-order effects that are challenging

to overcome. If subordinates cannot receive orders or coordinate effects, their mission will be

compromised, and the ability to reinforce their operations is limited.

Having the disposition of hostile networks and their command-and-control structure

provides real-world situational awareness in which commanders can use, process, and allocate

resources. This is comparable to the Navy's use of scouting by collecting information, reporting

it, and disseminating it to place effective fires on that target.[34] Planners both at the tactical and

operational levels can identify objectives from the information they collect on social media.

Most importantly, operational level commanders can use this information to prevent civil unrest,

especially as we move into phase IV operations. Using the case studies in Egypt, or Tunisia, or

any other Arab Spring event with significant civil unrest demonstrates how social media can

---

[32] Marcellino, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, P12
[33] Sanda. *Social Media as a Tool of Hybrid Warfare* P17
[34] Wayne P Hughes, and Robert Girrier, *Fleet Tactics and Naval Operations*. Third edition ed. Annapolis, Maryland: Naval Institute Press, 2018.P184-185

organize and disseminate information efficiently. What different actions could the Egyptian or

Tunisian governments take by monitoring social media? Having real-time situational awareness

of current or near-future civil unrest would enable a better allocation of resources to that area.

To prevent the result, the government could have established curfews and reinforced the police

to curb crowds and civil unrest developing in Cairo, Alexandria, Mansour, and Suez. Having

real-time or near-real-time situational awareness of occurring or predicted actions would provide

the level of detail commanders require to make informed decisions on the proper allocation of

forces to deal with the current problem.

Greater than real-time situational awareness is the ability to monitor a communications

platform, intercepting potential plans and operations from our enemy. When at war with a near-

peer adversary, we can likely expect that adversary will not use social media as part of their

communications. However, suppose we face another insurgency, similar to what happened in

Iraq after the dominate phase. With an insurgency, we can expect primitive communication

technology, requiring social media use to communicate. Doing so will give the United States the

ability to monitor these communications. Wilhelm Fickle said it best, "The endeavor to learn

what is in the opponent's mind and to draw advantage from it has always been very important

through the history of mankind…" [35] Knowing not only the location of an enemy's command-

and-control structure but what they are saying creates a marked advantage. If your opponent

knows your battle plans, your opponent can defeat you just by countering your actions. This can

create a unique opportunity for U.S. plans. Even if it is a small insurgency, understanding the

---

[35] Wilhelm Flicke, "The Beginnings of Radio Intercept in World War
I." https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-
spectrum/beginnings_radio_intercept.pdf.

enemy's plans can help us easily counter them by placing an adequate force to prevent and counter those actions.

Enemy forces, especially non-state actors, can and will use social media as a command-and-control communications platform that the United States can easily exploit. First, it can determine the hostile force's interweb of connections and determine their size and composition. Second, it can provide real-time situational awareness to commanders, helping inform their decisions on how and where to allocate resources. Finally, as social media is open-source, commanders and staff can capitalize off enemy battle plans or organizational plans. Although exploiting social media command-and-control structures limited to non-state insurgencies, it will provide valuable intelligence for future operations planning.

Validity, Credibility, and Accuracy of Social Media Data

As commanders begin to use social media intelligence to define the operating environment, plan operations, and identify and intercept critical communications, they can become susceptible to deception due to misinformation. Social media analysts can only assess the information provided to them, whether accurate or not. In 2014 during the Russian annexation of Crimea, the Russian government employed over 600 personnel, spending over 19 million dollars to post pro-Russian news, positive outlooks, and information for Russian operations using robotic (bots) and fake accounts.[36] Doing so created the illusion of local support within Crimea for the annexation. China employs the same tactics, with formal positions known as internet commentators. These commentators get paid for each positive tweet posted in

---

[36] Michael Holloway, "How Russia Weaponized Social Media in Crimea ." . Accessed Feb 27, 2021. https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html.

support of the Chinese Communist Party.[37] Weibo, China's version of Twitter, posted several

pictures of protesters rioting and protesting radically while portraying police heroically,

controlling the narrative of the actions occurring in Hong Kong in 2019.[38] In both cases, if

analyst information only came from state-run media, bots, or fake social media accounts, the

events' perspective would be dramatically different. Suppose China, Russia, or any other hostile

state or non-state actor knew that the United States used social media to visualize the operating

environment, plan operations, or counter command and control. If so, they could quickly

increase their number of fake reports and deceive the United States into an unfavorable location

or position, making social media a dangerous intelligence tool.

Combatting Fake News

While valid, these fake reports may enable the commanders to continue to gain an

advantage over their enemies by using artificial intelligence (AI) to verify and group relevant

posts and data mining information to distinguish the valid from the invalid. Currently available,

software-based analytical tools can sort and filter social media posts. These tools can

differentiate between a bot versus a human post. What is pro or anti-government. They can

network all aspects of the information provided.[39] By filtering these posts between real and fake,

intelligence analysts can continue to provide the operating environment's social aspect. This will

translate into more refined planning of operations within the theater. To counteract fake news,

commanders should incorporate social media into their commander's critical information

---

[37] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *The American Political Science Review* 111, no. 3 (Aug, 2017) P484

[38] Kuo Lily. "Beijing's New Weapon to Muffle Hong Kong Protests: Fake News." *The Observer (London),* Aug 12, 2019. https://search.proquest.com/docview/2272045311.

[39] Marcellino, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations* P13

requirements (CCIR), including the following questions: what is the public support of the local civil authority? Are there indications of a social media deception? With a clear CCIR, social media intelligence analysts at both the tactical and operational levels can maximize their data interpretation, better analyze the information, and provide answers to legitimate questions about the operating environment.

Conclusion

To gain the initiative against hostile state and non-state actors, theater commanders and their staff must incorporate social media into the intelligence cycles, JIPOE, and planning phases of operations. First, social media helps define the operating environment and refine the operational area's ground truth. Second, by understanding the operating environment better, planners can integrate that information into better plans, enabling mission command, quality command decisions, and preventing undesired effects. Last, social media will help define the command-and-control structure, creating unique opportunities to exploit the enemy's operations. Using social media as a military tool may open the door to deception operations organized by opposing governments such as Russia and China, creating the false visualization of government support in contested regions. However, by using AI and filtering, analysts can exploit fake information and capitalize on it. Social media helps define cultural and regional changes. The military must adapt and leverage social media to support future wars.

BIBLIOGRAPHY

"101+ Social Media Sites You Need to Know in 2021.". Accessed 11 March, 2021. https://influencermarketinghub.com/social-media-sites/.

"Baronessedulac.". Accessed 15 March, 2021. https://twitter.com/baronessedulac.

"Hassan Rouhani on Twitter." . https://twitter.com/HassanRouhani/status/1308460495809196032.

"Insurgents used Cell Phone Geotags to Destroy AH-64s in Iraq." . Accessed Feb 27, 2021. https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq#:~:text=Here's%20a%20battlefield%20safety%20issue,of%20troops%20on%20a%20battlefield.

"Iran Democracy.". Accessed 15 March, 2021. https://twitter.com/IranDemoracy.

Abouaoun, Elie. "Tunisia Timeline: Since the Jasmine Revolution." *United State Institute of Peace* (12 July, 2019). https://www.usip.org/tunisia-timeline-jasmine-revolution.

Bodine-Barron, Elizabeth, Todd Helmus, Madeline Magnuson, and Zev Winkelman. *Examining ISIL Support and Opposition Networks on Twitter* RAND Corporation, 2016.

Burnore, Nathanael. "Social Media Applications for Unconventional Warfare." U.S. Army Command and General Staff College, 2014.

Connett, Ty and Bob Cassidy. "Village Stability Operations: More than Village Defense." *Special Warfare* 24, no. 3 (Sep, 2011). https://www.soc.mil/SWCS/SWmag/archive/SW2403/SW2403VillageStabilityOperations_MoreThanVillageDefense.html#:~:text=VSO%20are%20one%20of%20several,campaign%20of%20counterinsurgency%2C%20or%20COIN.

Flicke, Wilhelm. "The Beginnings of Radio Intercept in World War I." (: 20. https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/beginnings_radio_intercept.pdf.

Forrester, B. and K. den Hollander. "The Role of Social Media in the Intelligence Cycle." (1 January, 2016). https://www.narcis.nl/publication/RecordID/oai:tudelft.nl:uuid:28f2c5f7-46e0-4602-8d27-fc62370460b9.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman. *Russian Social Media Influence*. Santa Monica, Calif: RAND Corporation, 2018.

Holloway, Michael. "How Russia Weaponized Social Media in Crimea .". Accessed 27 February, 2021. https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html.

Howard, Philip, Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad. *Opening Closed Regimes: What was the Role of Social Media during the Arab Spring?*, 2011.

Hughes, Wayne P. and Robert Girrier. *Fleet Tactics and Naval Operations*. Third edition ed. Annapolis, Maryland: Naval Institute Press, 2018.

J.M. Berger and Jonathon Morgan. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*: Brookings Institution, 2015.

Khalil, Ashraf. "Anger in Alexandria: 'We're Afraid of our Own Government'.". Accessed 15 March, 2021. https://web.archive.org/web/20110427172608/http://www.almasryalyoum.com/en/node/51909.

King, Gary, Pan, Jennifer, and Roberts, Margaret E. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *The American Political Science Review* 111, no. 3 (Aug, 2017): 484-501. doi:10.1017/S0003055417000144.

Lily Kuo. "Beijing's New Weapon to Muffle Hong Kong Protests: Fake News." *The Observer (London),* 12 August, 2019. https://search.proquest.com/docview/2272045311.

Marcellino, William. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, 2017.

Mattis, Jim. *Summary of the 2018 National Defense Strategy of the United States of America*, 2018.

Nada, Darrett and Rowan, Mattisan. "Egypt Timeline: Since the Arab Uprising." *United State Institute of Peace* (2 July, 2019). https://www.usip.org/egypt-timeline-arab-uprising.

Ngak, Chenda. "Then and Now: A History of Social Networking Sites.". Accessed 27 February, 2021.

Resnick, Brian. "On Twitter, False News Travels Faster than True Stories.". https://www.vox.com/science-and-health/2018/3/8/17085928/fake-news-study-mit-science.

Svetoka, Sanda. *Social Media as a Tool of Hybrid Warfare*. Latvia: NATO Strategic Communications Centre of Excellence, 2016a.

Weise, Karen. "Amazon Knows what You Buy. and It's Building a Big Ad Business from It." *NYTimes.Com Feed,* 20 January, 2019. https://global.factiva.com/en/du/article.asp?accessionno=NYTFEED020190120ef1k002p9.

Wille, Dennis. "Every Soldier a Messenger: Using Social Media in the Contemporary Operating Environment." U.S. Army Command and General Staff College, 2012.

Winkie, Davis. "Rapid Trident 20 Exercise Kicks Off in Ukraine with Fewer US Troops than Last Year." *Army Times,* Sep, 14, 2020. https://www.armytimes.com/2020/09/14/rapid-trident-20-exercise-kicks-off-in-ukraine-with-fewer-us-troops-than-last-year/.