CHOOSING THE RIGHT SOCIAL MEDIA STRATEGY FOR AN ASYMMETRIC CONFLICT

Mr. J. Price

JCSP 39

Master of Defence Studies

PCEMI 39

Maîtrise en études de la défense

Canada

**CHOOSING THE RIGHT SOCIAL MEDIA STRATEGY FOR AN
ASYMMETRIC CONFLICT**

By Mr. J. Price
Par M. J. Price

Abstract

From its role in the "Twitter Revolution" in the Arab world, to its effectiveness as a tool of terror for Al Qaeda, social media has had a substantial impact on asymmetric warfare. This paper demonstrates that outside forces seeking to influence insurgencies should choose their online strategy based upon which quadrant of the appropriate Social Media Matrix for Insurgencies that the conflict they are engaged in lies. These matrixes incorporate the motivation of the population to revolt, the level of popular support for the outside force, the strength of the insurgency and the degree of control over the network that the counterinsurgents possess. In addition, commanders must choose appropriate messages, media, and messengers for the operating environment they face. Commanders who do not appropriately tailor their social media strategy for the conflict they are fighting will lose considerable ground in the battle for the hearts and minds of the local population.

Contents

There is now a menace which is called Twitter. The best examples of lies can be found there. To me, social media is the worst menace to society.

— Recep Tayyip Erdogan
Turkish Prime Minister

Introduction

Technology changes warfare. The use of the atom bomb on Hiroshima forever altered the nature of how nations would interact. It immediately brought an end to one war and has since had huge implications for all nations' militaries. However, the influence of technology is not always so straightforward and its impact on warfare can take much longer to be realized. Sending messages across airwaves allowed popular music to reach the masses, but it also allowed for more effective coordination of military units over vast differences, a key enabling factor for manoeuvre warfare. Likewise, social media, a tool that exploded in growth based on its ability for pictures of cats to be shared between former classmates, is now a component of armed conflict. The same technology used to popularize the hit song "Gangnam Style" is used to seek recruits for global conflicts and encourage and coordinate acts of terrorism.

Social media will follow the path of radio and serve as a catalyst that shapes the nature of global conflict. Commanders must develop and implement strategies that reflect that this technology will change how hearts and minds are won, especially when engaged in asymmetric warfare.[1] The voice of insurgents can be disproportionately magnified beyond their kinetic abilities through effective application of social media, and a victory on the battlefield can be turned into a defeat by public opinion if a few key images "go viral" and are shared with millions of users.[2]

Social media's collaborative nature means that a commander cannot treat this tool as an extension of traditional media. Television, print and radio can be simply analysed by

---

[1] Mayfield III, Thomas D., "A Commander's Strategy for Social Media," *JFQ: Joint Force Quarterly* no. 60: 79.
[2] One of social media's features is its ability to rapidly disseminate content that users want to share, reaching various populations through different vectors (individuals or websites). This rapid spreading of information is colloquially compared to unchecked disease transmittal and is referred to by using variations of the expression "to go viral."

intelligence gatherers, leveraged through news conferences, private conversations and site visits, and shut down as appropriate with targeted kinetic strikes. Military leaders that treat social media the same way are akin to Wing Commanders using next generation fighters as simply flying howitzers.

The majority of current literature prepared for commanders focuses on social media strategy from a Public Affairs or operational security perspective: share good news and information, ensure troops do not leak secrets, and monitor what the enemy is doing. Guidance for using social media as a key tool in conflict suggests commanders support insurgencies by ensuring the population has access to social media and combat insurgencies by getting the message out before the insurgents, while countering the enemy's messaging as appropriate.

Although this advice may be sufficient for some situations, modern commanders need to implement a social media strategy that is more complex if they are to be successful across a broad range of engagements. This paper will demonstrate that commanders competing in a battle for hearts in minds during an insurgency must adapt their approach depending on which quadrant of the appropriate Social Media Matrix for Insurgency they are operating in. The matrix for commanders supporting the insurgency measures the level of popular support for both the revolution and the outside force. The matrix for combating the insurgency measures the degree of control over the network and the intensity of the insurgency. Regardless of quadrant, choosing the correct message, medium and messenger are essential for swaying the public to either support or ignore the insurgency. Failing to adapt the social media strategy to these factors will either effectively cede the social media front to the adversaries, or result in an online loss to an opponent, who, through more effective engagement tactics, has brought a gun to a knife fight.

Context

For the purposes of this paper, a "commander" refers to an individual leading an "outside force" either in support of an established government facing an insurgency or working hand-in-hand with opposition forces to overthrow an established government. The outside force is considered to be physically present as part of a supporting or occupying force in the case of combating the insurgency and having limited (covert operatives and Special Forces) or no physical presence when supporting an insurgency. A commander who commits significant combat assets to a theatre in an attempt to support an insurgency is essentially invading a hostile nation. Although some principles from this paper may apply to this style of engagement, a war of this nature is beyond the scope of this document. Such a conflict could, however, evolve into an area covered by this paper, if, after the government is overthrown, the outside force either supports or runs the new regime and faces an insurgency from those who oppose it.

The frame of reference for the outsiders used in this paper is a NATO force, such as those used to combat an insurgency in Afghanistan and support one in Libya. However, examples of successful strategies are also drawn from other sources. Al-Qaeda has demonstrated deftness in employing social media in an insurgency and nations like China and Iran have had success in combating internal insurgents. The application of effective techniques in this new field is not limited to established democracies. Western nations on foreign soil seeking to win the support of the local population have often stumbled as their messaging has been disconnected from their actions. In Iraq, although the United States had operational reasons for attacking Fallujah, the

fallout of that initiative impacted the hearts and minds of the local population leading many Iraqis to believe that the Americans valued killing belligerents more than civilian safety.[3]

In contrast, an organisation that combines messaging and action well is Al-Qaeda. Their planners consider how target audiences will perceive their actions as they deftly use kinetic operations to impact public opinion. They focus on winning engagements that have a story, rather than trying to win tactical military engagements in which they are outclassed.[4] Some key metrics they employ to assess their success are how quickly they get an attack video to spread through social media channels and the news coverage the video receives.[5] Al-Qaeda leverages their kinetic attacks with social media engagement to tap into emotions beyond terror, leveraging their existing level of support as they seek recruits, funds, publicity and to raise morale.[6]

Like Al-Qaeda's mix of kinetic attacks with informational warfare, the approaches to social media recommended in this paper are meant to complement and be influenced by other activities that a commander is engaged in, including military operations, diplomacy, and humanitarian and logistical support. Much like "holding the high ground" and recognizing the importance of "an army marches on its stomach" the recommended approach for each situation is a best practice. The nature of conflict is such that there are exceptions where the rule does not hold, and this paper will not explore all factors that may influence choice of appropriate strategy. Finally, this paper was written in 2013 and the evolving nature of the technology discussed in this document is such that it can soon become dated.

---

[3] James P. Farwell, "Jihadi Video in the 'War of Ideas'," *Survival (00396338)* 52, no. 6 (Dec2010, 2010), 144.
[4] *Ibid.*, 131.
[5] *Ibid.*, 143.
[6] *Ibid.*, 131.

History

Social media arguably began when the first "Bulletin Board System" between connected computers was launched in 1978 and grew as the Usenet became popular, sites like Geocities appeared, and the weblog gained proponents. It refers to users interacting directly with their peers; a feature of "Web 2.0" which makes it distinct from the early web sites of the 1990's which were essentially broadcasting information, not facilitating conversations. In contrast Web 2.0 empowers users to create and share. Social media can encompass everything from commenting on news article or web postings to leading alternate online lives in places such as the World of Warcraft and Second Life. What is generally referred to when discussing social media with respect to conflict and warfare are sites like YouTube and Vimeo (where users post videos), Flickr and Instagram (where users post still photos) and Facebook and Twitter (where users chronicle their lives through a variety of means). [7] This paper will also use the same definition of social media, recognizing that specific sites and technology will either lose or gain favour in the coming years as new online entities seek to dominate global digital engagement.[8]

Throughout history, insurgencies have been aided by technology that changed how participants interact with one other. During the Atlantic Revolutions of the 18th century, revolutionaries and their ideas could only cross the ocean by using sailing ships subject to fickle winds. By the time of the Constitutional Revolutions of 1905 in Asia, propaganda was shared by

[7] Twitter users post 140 character messages which may include hyperlinks to imagery called "tweets", and users may "retweet" (repost) others' tweets. Facebook allows users to create a network of "friends" who follow the user and who can indicate support for a post by clicking on a "like" button.
[8] Anthony Curtis, "The Brief History of Social Media," http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html; Internet; accessed 17 January, 2013.

telegraph and revolutionaries used steamships and trains.[9]   In 2011 the Arab revolution spread

quickly through the use of satellite television, mobile phones and the Internet, which permitted

powerful imagery and calls to arms to be shared instantly with revolutionaries separated by

thousands of kilometres.[10]

Social media has irrevocably changed the battlespace as online social networks connect

geographically dispersed netizens.[11] It helps like-minded revolutionaries find each other and

interact both publicly and privately.   The movement that overthrew the Egyptian government in

2011 was helped by social media connecting a few key people with revolutionary views and

allowing them to plan the protests that would eventually topple their government.[12]

If an insurgent has 500 Facebook friends and each of them has 500 different Facebook

friends they can reach a population of up to 250,000 people all within two degrees of

separation.[13]   Although not everyone has this many unique friends, the third degree of

separation, even with plenty of overlap, could reach millions. This nimbleness can be used when

coordinating attacks or demonstrations, allowing insurgents to launch a call to action that

reverberates through the Internet instead of organizing days in advance and giving authorities

time to anticipate and react.[14] With the ubiquity of smartphones, even poor regions have

hundreds of "citizen reporters" uploading sounds and imagery from global hotspots.[15] The

---

[9] David Motadel, "Waves of Revolution," *History Today* 61, no. 4 (04, 2011), 3-4.
[10] *Ibid*.
[11] A netizen is a "citizen of the Internet," or "digital native" who relies on and is adept in using the Internet on a frequent basis.
[12] Daniel Keeney and Ed Schipul, "War of Words: Social Media's Role in Provoking Revolutionary Change," *Public Relations Tactics* 18, no. 4 (04, 2011), 10-11.
[13] Keeney and Schipul, *War of Words...*
[14] Marko Papic and Sean Noonan, "*Social Media as a Tool of Protest*," http://www.stratfor.com/weekly/20110202-social-media-tool-protest, Internet; accessed 17 January, 2013.
[15] Keeney and Schipul, *War of Words...*

editors and publishers of these individuals are not people wearing suits in corner offices. They are the friends and acquaintances of the users who promote their content, allowing for well-connected citizen journalists to share a compelling narrative faster than an Associated Press feed.

New technology introduces new rules and ways of playing the game. Those who effectively adopt it first have an advantage. The image of the British redcoats standing in a line while Minutemen outmaneuvered them and behaved in an "ungentlemanly fashion" is a frequent trope used in films and television programs set during the American Revolution. The first submariners were seen to have so violated the rules of war by striking from below the surface in silence that some officers consider them pirates who should be hanged. In both cases this new approach to conflict greatly benefited those who adopted it.

Today's commanders would obviously prefer to be on the winning side when interacting with new technology, but many have other considerations that have impacted their willingness to embrace social media. For some commanders the technology is foreign, and they would prefer to stick with the methods they learned over the past few decades. Others have ethical concerns. When the Geneva Conventions were crafted its authors were not thinking about camera equipped mobile phones. On the Internet a 48-year-old Colonel with a doctorate could be involved in a propaganda exchange with a 14-year-old orphan with no formal schooling, and neither may realize with whom they are sparring. New styles of engagement are developing for interaction over social media, and no Henri Dunant[16] has yet emerged to advocate for getting all parties to agree to the rules of warfare.

---

[16] Dunant won the first Nobel Peace Prize for helping create the Red Cross and the Geneva Convention.

Whether or not commanders avoid embracing this technology, their opponents will certainly be employing it. Social media users can be very creative in leveraging the Internet to their cause. For instance, members of Al-Qaeda use YouTube and other social media to obtain footage that can be edited into propaganda pieces which fit their narrative. [17] In one notable example, al-Qaeda in Mesopotamia created a montage based on the HBO documentary *Baghdad ER*, which dealt with emergency medical care for wounded coalition forces. The group substituted its own soundtrack and a new beginning and ending to communicate the message that US forces are crying, hurting and being defeated day after day.[18]

George W. Bush gained some notoriety for verbal blunders during his presidency, and one that provided a huge boost to jihadists was his use of the word "crusade" to describe U.S. activities in the Middle East. As America has gained power, its presidents' remarks have gained more and more global significance. In an age where those without the constraints of a journalistic code can produce material as widely viewed as broadcast media, leaders need to be extremely culturally sensitive. Through effective use of social media and providing their own context radicals were able to turn this casual remark into a declaration of anti-Islamic philosophy conveying the message "that the American presence represents a modern Crusade against Muslims." [19]

Correcting these impressions is difficult. Large organisations, such as most western militaries, have approval processes and release of information policies that limit what can be shared on social media. This increases the gap between the time of the event and the time of the

---

[17] Farwell, *Jihadi Video in the 'War of Ideas,"*131.
[18] *Ibid., 132.*
[19] *Ibid.*, 135.

publication of corresponding material. The social media victory for the Jaish al-Mahdi (JAM) over the U.S. in Iraq during Operation Valhalla demonstrates the power of operating without these constraints. U.S. Special Forces working alongside their Iraqi allies killed JAM fighters, rescued a hostage, and destroyed a weapons cache during a successful operation. After the Americans left, someone repositioned the bodies of the dead insurgents. Their weapons were removed and the scene was set up to make it look like they were murdered while praying.[20] The images were then published on the web with an accompanying news release which indicated that the American soldiers had butchered peaceful men who were taking part in religious activity at a mosque.[21] In spite of having helmet cameras and a combat camera team which documented that this was not the case, the Americans were unable to get their imagery approved for release until three days later. Their enemy's messaging went viral in less than an hour, spreading from one user to many in mere seconds. Today's news cycle necessitates that stories are quickly replaced with fresh material leaving their powerful initial impressions echo through social media; the American response was far too late and therefore their reputation was severely damaged.[22]

Whether commanders are trying to beat the insurgents or support an insurgency, clear strategic direction that incorporates social media into the campaign plan is necessary. Operation Valhalla demonstrates that relying exclusively on advanced technology and truth are not enough to win hearts and minds during an insurgency.

---

[20] Mayfield , "*A Commander's Strategy for Social Media*," 82.
[21] *Ibid.,* 82.
[22] *Ibid.,* 82.

Supporting an Insurgency

When looking to support an insurgency, such as the Libyans overthrowing Gaddafi in 2011 or the failed Iranian Green revolution, planners from outside forces need to identify how best to employ social media. One key factor in determining the appropriate approach is how dissatisfied the population is with the current regime and whether that motivation can be turned into concrete actions. A nation recently overtaken by a dictator has a very different character than one which has suffered for years under an oppressive regime. [23] In the first case, an active resistance movement, with a ready-made organisational structure, may lay just below the surface. In the second, years of oppression may have eliminated those who could have led an insurgency.

A Facebook Post does not a Revolution Make

Sometimes western forces want the "little guys" to unshackle themselves from their torment, and exploit the rush of freedom that comes through the power of democracy. A myth promoted by both media and academics is that the citizens of oppressed nations are eager to risk their lives and those of their families in order to overthrow their oppressors, but need a web connection to take action. [24] These writers imply authoritarian nations are governed by buffoons such as Kim Jong Un, "leaders who come across as stereotypically incompetent Bond villains: uniformly dressed, tasteless but expensive cliché obsessions, physically unintimidating, with every major attack blowing up in their face like Wile E. Coyote." [25]

---

[23] Headquarters, Department of the Army, "*Army Special Operations Forces Unconventional Warfare,*" https://www.fas.org/irp/doddir/army/fm3-05-130.pdf, 1-4, Internet; accessed 17 January, 2013.

[24] Evgeny Morozov and Inc Books24x7, *The Net Delusion*, 1st ed. (New York: Public Affairs, 2011), 85.

[25] Julian Hattem, "Why do We Laugh at North Korea but Fear Iran?," *The Atlantic,* http://www.theatlantic.com/international/archive/2013/04/why-do-we-laugh-at-north-korea-but-fear-iran/274680/; Internet; accessed 17 January, 2013.

The argument put forward is that all aspiring insurgents need is access to open Internet and they will tweet their way to democracy; a simple exchange of 140-character messages being enough to topple an established government. However, even if social media gains traction and a robust dialogue emerges about regime change there is not necessarily a causal link between tweets and other forms of online engagement and protests or insurgency. Assessing the motivation of a population to revolt requires a full assessment by intelligence analysts, not simply checking how many "likes" a Facebook page has.[26] The Internet can support and facilitate but never completely replace direct human contact. The loyalty to the "guy in the foxhole with you" comes through shared experience that is difficult to capture with a virtual presence. [27] The Arab Spring of 2011, sometimes called the Twitter Revolution was arguable aided by the presence of social media, but the real impact was likely overplayed, as illustrated in the examples below:

> If the Arab revolution taught us something, it's that the power of the people is greater than the people in power. In Egypt, if you asked Egyptians before Mubarak stepped down, "Do you want Mubarak in this country?" they would say, "No, but we don't know what to do about it." Any country that has reached this status, their dictator has to understand that it's coming. It's coming mainly because people now communicate with each other much easier, collaborate with each other much easier.[28]

Some advocates for the expanded role of media took this argument even further by insinuating that a successful insurgency was inevitable not because of the people but simply because of the technology:

---

[26] *Ibid.,*16.
[27] The Centre for the Study of Radicalisation and Political Violence, "*Countering Online Radicalisation: A Strategy for Action*," http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf; 73, Internet; accessed 17 January, 2013.
[28] Charlie Rose, "Charlie Rose Talks to Wael Ghonim," *Bloomberg Businessweek*, no. 4267 (02/20, 2012), 20-20.

Social-media collaboration generated accidental revolutionaries. The connected masses forged rapid, digital alliances too dynamic to be ignored and too unpredictable to be countered. In a remarkably short time span, social-media communities viewed their collective action in historical terms, generating the key ingredient required for revolutionary momentum: inevitability.[29]

Although some academics and many in the media promoted the idea that regime change has become easy with the advent of social media, it seems excessive to say that all that is necessary to overthrow a tyrant is to "ensure that young people have enough mobile phones, punch holes in any restrictive firewalls that may be in place to censor the Internet, and guarantee enough broadband capabilities." [30] Throughout history, engaging in risky violence for a group objective tends to be preceded by a prolonged process of socialisation which builds loyalty to a cause and strong personal ties between members.[31] The Internet's inability to provide in-person interaction means that it is difficult for it to be used exclusively to forge this kind of community.

In addition, although social media can have benefits for an insurgency it can have serious drawbacks. [32] Expecting the immediacy of results that followed the tearing down of the Berlin Wall during the Cold War is not realistic for those seeking to influence the world by tearing down the Great Firewall of China that restricts its citizens Internet access.[33] Attacking a nation's censorship apparatus may leave a commander disappointed. The content intended for insurgents

---

[29] LCol Brian Petit, U.S. Army John F. Kennedy Special Warfare Center and School, "*Social Media and UW*," http://www.soc.mil/swcs/swmag/archive/SW2502/SW2502SocialMediaAndUW.html; Internet; accessed 17 January, 2013.

[30] Nikolas Gvosdev, "Politics Vs. Social Media in the Arab Uprising," *World Politics Review* (03/04, 2011), 1-1.

[31] The Centre for the Study of Radicalisation and Political Violence, *Countering Online Radicalisation...*, 73.

[32] Evgeny Morozov and Inc Books24x7, *The Net Delusion*, 1st ed. (New York: PublicAffairs, 2011)xiv.

[33] *Ibid.,* 41.

might be deleted by a cyber-attack or perhaps worse, it will be ignored by users employing their new freedom and relations to learn about non-revolutionary topics like pirating movies and pornography.[34]

The argument that no regime can stand for long when faced with the power of social media falls flat when examined in the context of real conflicts. Social media was in place for some time prior to the mass unrest in the nations affected by Arab Spring. The 2010 Facebook penetration in Egypt was just over five percent, while Bahrain, which had a less successful uprising, was at 34 percent.[35] A commander's strategy needs to be adapted to the environment as even a large online movement does not equate to an active revolution ripe for outside support.

The recent Egyptian unrest emphasises the point. Although media reported extensively on how the successful 2011 revolution was aided by social media, an earlier revolution was less effective. In 2008 textile workers in the city of Mahala went on strike and attracted 70,000 supporters for their Facebook page.[36] Although members of the group had interesting conversations in virtual spaces, the loosely formed organisation was unable to bridge the gap between real-world impact and meaningful discussions between individuals sitting alone in the relative comfort of basements and cafes.[37]

When Ed Schipul and Daniel Keeney examined the Facebook sites, Twitter feeds and blogs that were credited for the resignation of Egyptian President Hosni Mubarak, they found the volume of activity prior to the event relatively insignificant. Given 45 million of Egypt's 84

---

[34] *Ibid.,* 110.
[35] Schipul, *War of Words: Social Media's Role in Provoking Revolutionary Change*, 10.
[36] Nikolas Gvosdev, "Politics Vs. Social Media in the Arab Uprising," *World Politics Review* (03/04, 2011), 1-1.
[37] *Ibid.*, 1-1.

million citizens are younger than 30 they were surprised that the Facebook page "We Are All Khalid Said," widely given credit for its role in galvanizing the uprising had less than 70,000 fans and many were from outside Egypt. [38] The Google executive, Wael Ghonim, widely viewed as the de facto leader of the uprising, had only 46,000 Twitter followers.[39]

Schipul and Keeney argue that it is insulting to the revolutionaries who risk their lives to give so much credit for their success to a popular Twitter account or Facebook page. They state that it is prolonged periods of discontent that disenfranchise a society and sow the seeds of rebellion and that "evolution is borne of desperation, not of smartphone apps."[40]

Although the Internet provides a convenient platform for insurgents to renew their commitment and reach out to their like-minded counterparts throughout the world, it is largely ineffective at recruiting combatants. [41] The disconnect between traditional frontline insurgent and the casual web warrior who will "like" a page still exists and was summed up nicely by Peter Certo, who, when referring to how surreal it was to follow a war on Twitter, wrote "imagine, fiddling with your phone on your lunch break, perusing actual hashtagged death threats from representatives of Hamas and the IDF in between all-caps proclamations from Kanye West and "Shit My Dad Says." [42]

Therefore, although effective insurgents and revolutionaries use social media to communicate and collaborate with each other, this is likely a correlation to their success and not the cause. The tools alone are not enough to trigger change. Social media was not necessary for

---

[38] Schipul, *War of Words: Social Media's Role in Provoking Revolutionary Change*, 10.
[39] *Ibid.*, 10.
[40] *Ibid.*, 10.
[41] The Centre for the Study of Radicalisation and Political Violence, *Countering Online Radicalisation...,* 73
[42] Peter Certo, "Israel's Real-World Flame War," *Foreign Policy in Focus* (11/16, 2012), 2-2.

the American Revolution, Castro's overthrow of Batista or the People Power Revolution in the

Philippines. [43] Although a valuable tool for a geographically dispersed insurgency, social media

may in some ways be overhyped. "Radicalisation comes from schools, from family, mosques

and the community; places where there is real-world and emotional contact. Deals aren't closed

in cyberspace."[44]

In a situation where an outside force seeks regime change, but a critical mass of

participants are not fully engaged (the populace is essentially passive towards the idea of

rebellion), the outside force needs to assess how they are perceived by the population. If not

supported fully, (for instance the lingering anti-American sentiment in Iran) than the best social

media strategy is to simply monitor the situation and wait for conditions to change (see Figure 1:

Social Media Matrix for an Outside Force Assisting an Insurgency).

However, if the outside force is perceived favourably (more akin to how Palestinians in

Israel view Saudi Arabia) social media can be used to effectively deliver messages that

encourage dissent that will lead to the population developing the willingness to overthrow their

government. If the nascent insurgency grew in strength, an outside force viewed more

favourably by the population could have a more direct role in the command and control of the

ensuing conflict, while one less favourably perceived would need to use a proxy to influence the

insurgency.

---

[43] Schipul, *War of Words: Social Media's Role in Provoking Revolutionary Change*, 10.
[44] PC Pro, "*Web terrorism: fact or fiction,*" http://www.pcpro.co.uk/features/262084/web-terrorism-fact-or-fiction;
Internet; accessed 17 January, 2013.

Figure 1: Social Media Matrix for an Outside Force Assisting an Insurgency
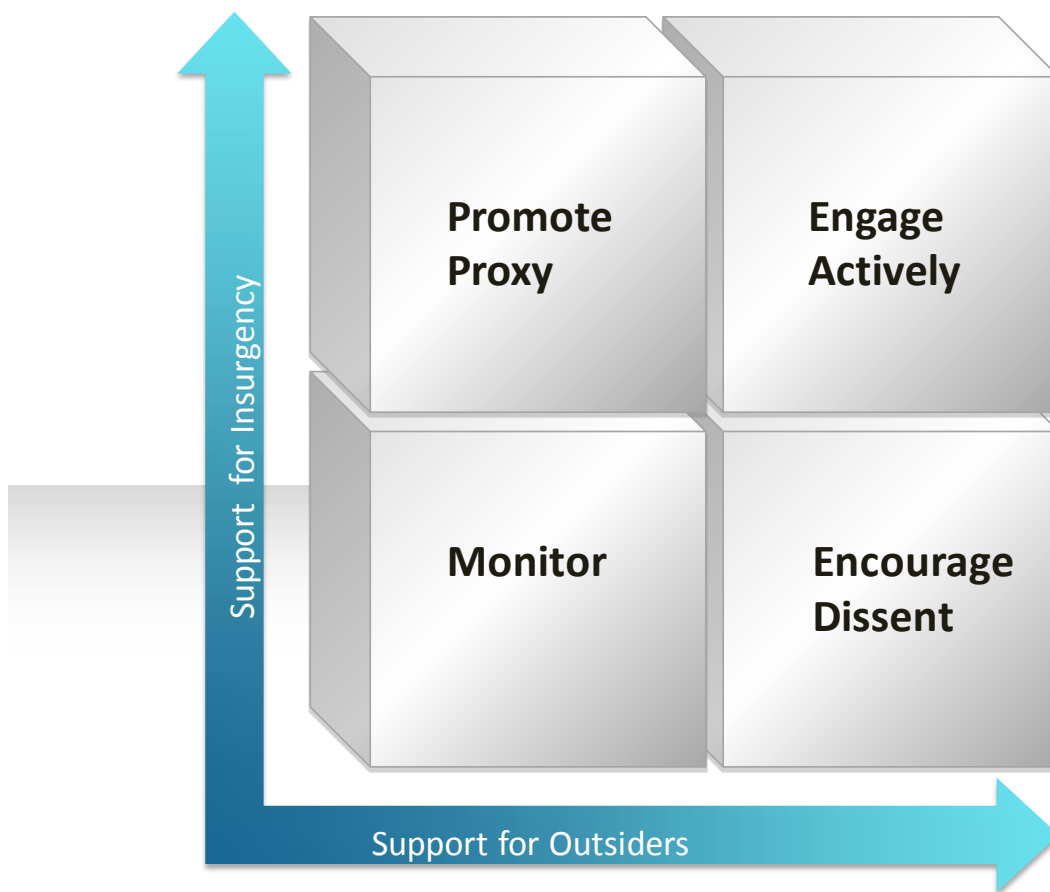
Monitoring

Although the Iranian Green Revolution had considerable momentum, the critical mass necessary for a winning the insurgency was not present. The view that the U.S. State Department seemed to have had was that with some outside support this could have been change, and therefore their representative asked Twitter to not undertake scheduled maintenance for the duration of the revolution.[45] The U.S. considered this social media tool as instrumental in both getting the message out to mainstream global media and in helping expand the revolutionary connections amongst the technologically connected leaders of the Iranian movement.[46] Had the perception of Iranians towards the U.S. been favourable this may have been an appropriate strategy. However, as this was not the case, things played out differently.

Although 98% of the most popular tweets on Twitter during the 2010 Green revolution in Iran were related to that uprising, most were not posted or retweeted by people in Iran.[47] The Iranian government capitalized on this by exploiting the impression that the Internet was a tool of the west for regime change by focussing on the disproportionate numbers of western media and expatriates following and tweeting about resistance activities in Iran. In addition, they were able to reverse-engineer the real-life social network of the revolution through Facebook, identifying active expatriates and threatening both them and their families back in Iran.[48] Clearly if the medium is to be used effectively by commanders seeking to assist the insurgents it must be

---

[45] Morozov, *The Net Delusion*, 9.
[46] Schipul, *War of Words: Social Media's Role in Provoking Revolutionary Change*, 10-11
[47] Morozov, *The Net Delusion*, 15.
[48] *Ibid.*, 10.

employed carefully. The consequences of "outing" the core of an insurgency before it gains ground, or of tainting an insurgency with "outside influence" before it is accepted by the populace is too great.

A more effective approach would have been to permit the movement to grow more organically and for the revolution to gain ground and be viewed as a local movement independent of the influence of outside forces. If this growth occurred, the outside force could support the insurgency through a proxy.

A more successful influence activity occurred around the same time period and was not directed by Americans but rather at Americans. During their revolution in 2011, Egyptian insurgents provided an effective outside influence on the United States. President Hosni Mubarak was once a trusted ally of the west. As Egypt began to revolt, enough convincing information reached the U.S., particularly via Twitter and Facebook, that a critical mass of Americans believed a genuine uprising was taking place. [49] As the social media from the land of the Sphinx reached eager netizens in the land of Lady Liberty the insurgency's message resonated with both average Americans and their media. This put both subtle and direct pressure on the U.S. government to "defriend" the dictator. In this case, the message from Egypt was not for American citizens to revolt, just to pressure their government to support the insurgency. However, its impact can be contrasted with the lack of American success in Iran based on how the average Iranian viewed America (skeptically) versus how the average American viewed the average Egyptian (sympathetically).

---

[49] Sushil Pradhan, "Social Media as a Catalyst in the Egyptian Unrest," *USI Journal* 141, no. 583 (Jan, 2011), 42.

Encouraging Dissent

A population which is not engaged in an active insurgency but which sympathetically views the outside force can be manipulated or encouraged towards beginning an insurgency. Proactively engaging with key audiences is the first step in conveying the message of rebellion to a critical mass of the population. Social media involves two-way communication and can be fully leveraged to promote an insurgency by creating opportunities for ongoing conversation with audiences that matter, allowing for trust and credibility to be established. With this accomplished, key messaging is likely to be listened to and adversarial propaganda will be less effective.[50]

However, in order for the conversation to take place a commander's forces need to be able to be where the audience is and a passive population is not actively seeking engagement with an outside force. Using appropriate media is essential, especially when devising the social media campaign that aims to turn the seeds of discontent into the fruits of a rebellion. Various insurgent groups seeking to mobilize young disaffected males with advanced education and relatively substantial financial resources have turned to using social media to promote video games that deliver their message. Al-Qaeda created a game where the player tries to kill the American president and British prime minister and Hezbollah has produced sophisticated first-person shooters under the *Special Force* brand where players fight Israelis. China has just recently launched the "Glorious Mission Online" game series which is developed in partnership

---

[50] Rafal Rohozinski and Dierdre Collings, *Bullets and Blogs: The New Media and the Warfighter* (Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, 2008) 3.

with the People's Liberation Army.[51] The first mission involves taking part in a modern battle

with Japan to reclaim contested islands. These games aim to create the mindset in these youth

that their actions can make a difference in the campaign against the enemy.[52] This mood can be

built on through social media engagement on the games forums about both strategy and the

underlying issues raised in the game. By effectively planting the seeds of rebellion the outside

force can help establish an active insurgency.

Some of these young video-gaming potential insurgents have day jobs in their countries

security apparatus. Powerful nations with large quantities of secret data are particularly

vulnerable to social media attacks from insurgents within their protected networks. Bradley

Manning allegedly used his position in the American military to download a massive quantity of

sensitive data which he then shared with WikiLeaks, a social media construct created to allow

whistleblowers to remain anonymous while preserving their data. Edward Snowden allegedly

exploited his role as a security consultant to leak similar information, relying on journalist Glenn

Greenwald to disseminate the material through both the traditional media of the Guardian

newspaper and on social media channels such as Twitter.

By revealing carefully guarded secrets and allowing the information to be collaboratively

pored over and dissected by internal and external audiences, social media can permit attacks such

as these to simultaneously isolate a government from its allies, identify weaknesses in its defence

structure, and enrage its population. Commanders need to make sure that when these well-

placed early-stage insurgents can be identified that they have the tools needed to ensure their

---

[51] Michael Lipin, Voice of America, "*Chinese Video Game Lets Players Seize Japan-Controlled Island*"; http://www.voanews.com/content/chinese-video-game-lets-players-seize-japancontrolled-islands/1715532.html; Internet; accessed 3 August, 2013.
[52] Farwell, *Jihadi Video in the 'War of Ideas'*,140.

actions have maximum effect. The kind of impact that would typically require hundreds of operatives could instead be achieved with one well-connected insider.

Mistakes in this area, however, can be costly. Fifth columnists may have agendas that do not match those of the outside force. The outside force may find their plans stymied when the well-placed insider provides information that leads to an invasion by an unfriendly nation, a revolution led by a faction unaligned with outside interests, or unrest in a neighboring nation. Assuring alignment of objectives or being able to throttle the information flow at the source can limit these unintended consequences. If the conditions on the ground are favourable, forging relationships with the right individual and providing them mechanisms such as WikiLeaks and credible social media accounts can turn the work of a few key individuals into a full-blown revolution.

Active Insurgencies

Although some populations unhappy with their governing regimes are not motivated to action, others already have a burgeoning insurgency. The mental disconnect between clicking a mouse and taking actions in the real world may not necessarily be so vast once such an insurgency starts, and the commander should alter the social media strategy appropriately.

Understanding what social media can be expected to accomplish and what it is unlikely to achieve will prepare the commander to make the right choices. Recognizing social media as a catalyst that enables a movement and not a cause of a revolution is critical when assessing what kind of support increased social media activity can be expected to generate. Having assessed that a population is highly motivated (typically demonstrated through massive rallies, acts of

civil disobedience, or an active campaign of violence tacitly supported by non-participants) the commander must use available intelligence assets to assess how the outside force is perceived (favourably as a trusted ally or unfavourably as a potential conqueror).

When looking to promote an ally in such a manner the conventional warfare perspective is no longer appropriate. A better approach is to use the lens of Unconventional Warfare (UW), which is "conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[53]

When preparing these efforts commanders must be aware that established dictators in oppressive regimes maintain power through demonstrated success in suppressing or foiling insurgencies.[54] This is why the motivation of the population for change must already be established before an UW social media approach is used. If not present, the methods described above might allow for an insurgency to develop as could a natural disaster or a faltering economy. These conditions must sufficiently weaken the government in order for a resistance to mobilize, as it "is extremely difficult to organize successful resistance under a fully consolidated government or occupying power with a strong internal security apparatus." [55]

However, as the technology driving social media evolves and becomes more prevalent, it may be a game-changer in this type of campaign. The next generation of social media tools may allow for a much lower threshold of popular engagement before an active strategy can be successfully employed by a commander. For the insurgency to be successful with such a small

---

[53] Department of the Army, *Army Special Operations Forces...*, 1-1.1
[54] *Ibid.*, 1-3.
[55] *Ibid,.* 1-3.

critical mass it needs the tacit support of the large percentage of the population located between the extremes of insurgents and rabid pro-government supporters. This passive demographic must see the fledgling organisation as legitimate and dealing with a passive population is a speciality of social media. The ability to support causes through pressing buttons and sharing information with friends as opposed to engaging in dangerous night-time antics with masked colleagues will not win a revolution by itself. However, with a core of fully engaged supporters, converting a passive population from bystanders into passive supporters is often the final step in allowing a well supported insurgency to seize power. [56]

Typically, as the insurgency gathers momentum the passive majority will decrease.[57] Overcoming the initial inertia is traditionally accomplished by convincing the populace that victory is inevitable or that they have nothing to lose by revolting. Although the latter might be fairly complex to accomplish using social media, the former seems quite possible. Simply witnessing the amount of support a popular posting receive through "likes," "retweets" and page views can generate a sense of inevitably through the enormity of the participation. In addition, when a catalyzing event occurs, social media can allow news of it to quickly spread. [58]

Social media can also be adapted to UW doctrine by using online communication to provide an "artificial safe haven" that replicates the isolation and restrictive terrain that allow traditional insurgents to meet without fear of persecution. [59] However, where this can prove problematic is where governments are technological advanced enough to manoeuvre freely and monitor these spaces. This was the case in the U.S. during the "Occupy Movement," an event

---

[56] *Ibid.,* 1-18.
[57] *Ibid.,*1-18.
[58] *Ibid.,* 2-1.
[59] *Ibid.,* 1- 4.

which shared similar characteristics to an insurgency. During this period, as a result of government monitoring, protestors evolved their tools and bypassed Facebook and Twitter (U.S. entities which could easily be monitored by government) creating their own social media in order to hide their intentions from government watchers and maintain the element of surprise against law enforcement.[60]

This arms race in social media will at times allow it to progresses to the point that a government's traditional online defence mechanisms can be bypassed. This will especially be the case if the insurgency is supported by a commander from a technologically advanced organisation that shares best practices, software and hardware with the insurgency. This support to a blossoming insurgency can permit covert association without relying on participants sneaking past police patrols. It can permit momentum to build in online discussion forums instead of relying on communications broadcasted from poorly defended radio or TV towers. Leveraged effectively, outside support can allow the movement to percolate and begin to build the infrastructure it needs, including command and control, funding, and awareness—all acquired at relatively low risk. Providing education, technology (cameras laptops), marketing expertise, funding and network access are some of the ways an established force can support the insurgency. These tools can certainly set up winning conditions, but it is highly unlikely with today's technology a commander can win a war exclusively through exceptional social media use.

---

[60] Rajash Rawal and Paul Nixon, "Re-Tweet to Democracy? the Social Media #Revolution in Perspective," *Proceedings of the European Conference on E-Government* (01, 2012), 604.

Promoting Proxies

Although the use of UW principles applies across the board when supporting an active insurgency, the visibility of the commander's organisation will depend on how the population views the outside force. Frequently, through longstanding regime's branding of the "West" as evil, a commander will find that outside forces are not held in high regard by the local populace. Outside assistance can be critical in supporting an asynchronous conflict against a superior foe, but care must be taken so that the revolution is not tainted by the involvement of unsympathetic forces. In this situation, support for an insurgency can best be achieved through promoting a proxy, an entity that is a conduit between the outside force and the insurgency. Money, technology and expertise can flow through this select group and keep the outside force at arm's length. As the twisting of the American involvement with Twitter from a logistics boon to a PR nightmare during the Iranian Green Revolution demonstrates, this is a very difficult task and one that requires a subtle touch.

The use of a proxy and a low-key social media presence (including monitoring) can improve perception such that an outside force could be involved in a later stage of rebellion or in the aftermath of a victory. Social media can be used to introduce and prepare a population for the presence of an occupying force and to gather information normally achieved through human intelligence. Social media can allow an outside force to live "among the people" monitoring and assessing their behaviour in preparation for in-person contact.[61] By simultaneously promoting a proxy and independently observing and participating in the online community in their area of responsibility commanders can improve their understanding of the society, its concerns and

---

[61] Mayfield , *A Commander's Strategy for Social Media*, 80.

interests, and identify patterns that can be exploited.[62] The significance of the community must be kept in perspective, however, as social media operators may only be engaging with an aspect of the population with access to wealth or the Internet. In spite of this limitation, this may still provide immense value as these individual may be the primary influencers who control the society. [63]

Historically, the Special Forces soldiers and spies who would penetrate into these societies have had to improvise and make do without full access to the nuances of language and cultural training that cannot be taught in time for short notice assignments. Living online through social media allows for the contribution of individuals who possess these key competencies, but who, as a result of their age, risk aversion, or other hindering factors could never contribute to a traditional "living among" mission. [64]

Actively Engaging

Although effective in instituting regime change, proxies are difficult to directly control.   If an outside force is viewed favourably, social media can instead be harnessed to have a more direct impact on the insurgency, allowing for a greater influence on events. Using a proxy when the outside force is viewed favourably adds unnecessary layers, complications that may give opponents the edge they need to maintain power. Therefore, when the population is ready to embrace an insurgency, a positively viewed outside force needs to take a much more aggressive social media posture.

---

[62] *Ibid.,* 80.
[63] Rohozinski and Collings, *Bullets and Blogs...,* III-11.
[64] Mayfield , *A Commander's Strategy for Social Media*, 82.

Well designed Improvised Explosive Device and experienced assassination squads can be effective tools in an insurgency. However, in isolation both are relatively limited in the breadth of what they can accomplish. Social media, in contrast, can assist an insurgency across a number of dimensions, in particular, if supported by a well resourced outside force that the population favours.

Publicity and Recruiting

Whereas the Nazis supporting Lord Haw Haw[65] had to be content to let radio waves carry his discouraging messages to British citizens during World War II, modern propagandists have a more robust medium in social media. Insurgents can share globally, in real-time, photos of "collateral damage" from NATO air strikes or digital videos of beheading of a journalist such as Daniel Pearl.[66] Those supporting an insurgency can use the Internet to spread disinformation, deliver threats intended to distill fear and helplessness, and captivate the attention of sympathizers.

In addition to providing a "digital recruiting office" for individuals seeking to join an insurgency, social media can capture information about the more passive users who browse an organisation's websites or with whom they interact on social media. This information can be used to gain momentum in influencing a passive population towards becoming more active participants in the conflict. Targeting for direct contact those who are well suited to the work that

---

[65] Lord Haw Haw was the moniker given to various German radio announcers broadcasting Nazi propaganda aimed at discouraging the British during World War II.
[66] Gabriel Weimann, United States Institute for Peace, *"How Modern Terrorism Uses the Internet,"* http://www.usip.org/files/resources/sr116.pdf; 5, Internet; accessed 17 January, 2013.

needs to be accomplished (by geographic location, ethnicity, or skill set) and who have indicated that they are favourably disposed to the insurgency allows an organisation to make targeted requests for action to those who have the means to contribute.[67] Similar techniques can be used to attract those who could back the organisation financially by using discreet commercial services like PayPal and Bitcoin.

Al-Qaeda uses social media effectively for publicity by sending out regular "news bulletins" directed at audiences throughout the world in which a masked man in a studio recounts events from the many fronts of jihad, while ticker-tape feeds provide running updates on the number of Americans allegedly killed.[68] The Economist found online instructions to future terrorists that instructed them to "film everything; this is good advice for all mujahideen [holy warriors]. Brothers, don't disdain photography. You should be aware that every frame you take is as good as a missile fired at the Crusader enemy and his puppets." [69]

With the ability of social media to bypass traditional media when delivering video to viewers, a citizen-journalist with a mobile phone that shoots and upload imagery is becoming arguably more important than, or at a minimum, a necessary partner for, a combatant with an AK-47 or rocket-launcher. [70] Prior to widespread adoption of the Internet, the Afghani Mujahedeen and Chechen rebels pioneered videos that told the story of their insurgency. They recognized, like good film directors, a compelling story should be told with a tight focus, and even if an attack against the Russian soldiers was relatively small, filming the operation would

---

[67] Weimann, *How Modern Terrorism Uses the Internet*, 8.
[68] "A World Wide Web of Terror." *Economist* 384, no. 8537 (07/14, 2007), 28-30.
[69] *Ibid.*
[70] *Ibid*.

allow for a huge statement that would resonate with viewers. [71] Now with access to sites like YouTube, similar organisations can broadcast nearly instantaneously to their followers without a large logistics challenge. Outside nations can support this effort with their specialized professionals. Providing access to Hollywood producers who build careers on moving people to tears or laughter can help insurgents produce videos and messaging that can knit combat footage or scenes of desperation into a compelling narrative that drives a revolution forward. Giving an insurgency access to a platoon of MBAs with market segmentation strategies can be a force multiplier that focuses supporters on the critical path to success.

Training

Social media is a safe and cost effective way for a struggling insurgency to provide basic instruction to members.[72] Effectively the medium can serve as an online revolutionary academy where training manuals and videos can be posted and geographically disperse and ideologically different terrorists groups can share best practises on topics from dealing with shady bankers to avoiding border patrols.[73] Using the right connections, from the privacy of a basement or an Internet cafe, a well-connected radical can find "The Terrorist's Handbook, The Anarchist Cookbook, The Mujahadeen Poisons Handbook, The Encyclopedia of Jihad (prepared by Al Qaeda) and How to Make Bombs that offer detailed instructions on how to unleash terror attacks." [74]

---

[71] Arab Salem, Edna Reid and Hsinchun Chen, "Multimedia Content Coding and Analysis: Unraveling the Content of Jihadi Extremist Groups' Videos," *Studies in Conflict & Terrorism* 31, no. 7 (07, 2008), 607.

[72] Papic and Noonan, *Social Media as a Tool of Protest*.

[73] Sushil Pradhan, "Internet, Social Media and Terrorism," *USI Journal* 141, no. 585 (Jul, 2011), 366-374.

[74] Ibid.

Once the Taliban was removed NATO deemed its mentorship program for Afghan forces necessary to ensure a solid transition. A similar goal may have been in desirable in Libya, but without willingness for soldiers to be on the ground in large numbers, that did not occur. Social media can augment training, and although not a complete replacement for skilled units of operational mentors, it can help fill the gap. Leveraging the expertise in this field held by western online learning academies that promote interaction between participants who share best practices with each other can allow the insurgency to use this tool to its full extent.

Intelligence Gathering

A nation's military secrets can be hacked, the connectedness of its agents exploited, and its weaknesses identified through social media engineering. Lax information security protocols allow for information about troop deployments to be posted online to families back home, and a soldier's Facebook profile is a map of who to taunt when a unit is involved in an important operation or who to seek funds from during a hostage taking. Unrestricted access to what soldiers do in Internet cafés as they engage with their families would be extremely useful for unscrupulous enemies, but on social media you often do not need to look over the person's shoulder as their videos, pictures and thoughts are posted publically and reposted widely by their loved ones.[75]

Western governments supporting overseas insurgencies can make use of data mining technology employed by companies like Facebook. That site employs user data to determine whether an individual should be shown an advertisement of, for example, a Lexus or a discount

---

[75] Rohozinski and Collings, *Bullets and Blogs...,* 57.

brand of olive oil. However, getting the occasional olive oil loving cyclist to click on a luxury car site is a small error, and a price companies are willing to pay in the context of increased overall profits. In contrast, identifying thousands of false positives as accounts belonging to potential insurgent allies (or enemies) is a more complicated matter. Using data mining to spot potential terror networks, or identify key government agents that could be turned via the web has an underlying problem that the more people that are monitored the more false-positives there are that need to be addressed. Attempting to filter out these inaccuracies requires extensive, intrusive and costly surveillance, resources insurgents could better utilise elsewhere. However an outside force, with more financial clout and access to technology might be in a position to provide this support. Recent revelations in the U.S. and Canada indicate both nations are developing this kind of competence and are quite prepared to employ it in support of their objectives.

Command and Control

Virtual private networks which allow for the real location of a web user to be hidden and various other privacy enhancing technologies can permit communication with minimal risk of the user's real identity being found out. Outside forces may equip an insurgency with these tools in much the same manner as Stinger missiles were given to the Afghan resistance in the 1980's. However, rather than a direct kinetic effect, like shooting down a helicopter, sharing technology that allows social media to be accessed behind a veil of secrecy allows insurgents to freely use

online collaboration tools such as wikis, research tools such as Google Earth, and messaging services like Gmail to plan and execute their attacks.[76]

Insurgent groups are frequently organised as affiliations of semi-independent cells with no structured hierarchy. Through the use of the social media these loosely aligned groups are able to maintain contact with allies, supporters and each other.[77] Wael Ghonim, a leader of the uprising in Egypt began his efforts in Dubai and was imprisoned for 12 days, during which time social media allowed his horizontal virtual command and control structure to remain functional. Removing the leaders of a hierarchical movement has historically been an efficient way to make an organisation ineffective. The imprisonment of Nelson Mandela, for instance, is believed by some to have set back the apartheid movement by a generation. [78] Social media addresses this by giving persistence to ideas and networks that can allow them to survive after the creators are no longer actively involved in the movement.

These social tools can also be used by an outside force to provide guidance and target identification, allowing them to have greater control in guiding the conflict. A commander's intelligence assets can providing a list of key objectives and present them through social media allowing individual cells to coordinate their efforts. Kickstarter is a social media tool that promotes "crowdsourcing" of projects where many individuals commit to contributing funds and money is collected from donors only if a certain objective is raised within a limited time. This

---

[76] Sushil Pradhan, "Internet, Social Media and Terrorism," *USI Journal* 141, no. 585 (Jul, 2011), 368.
[77] *Ibid.,* 368.
[78] Schipul, "*War of Words: Social Media's Role in Inciting Revolutionary Change*,"; http://schipul.com/articles/inciting-revolutionary-change/ Internet; accessed 17 January, 2013.

concept could be adapted to an insurgency, quantifying goals and objectives that need to be achieved before the rebellion moves to the next phase, allowing it to receive additional support from the outside force.

Combating an Insurgency

Providing support for an insurgency is not always the role an outside force will be tasked with. As has been the case in Afghanistan and Iraq, western nation often find themselves either as the governing force or in support of a government that is combating an insurgency. In many ways the social media challenges associated with combating an insurgency are much more difficult to overcome than those involved in supporting one. The assumption for a commander supporting an insurgency is that the government is bad and needs to be brought down; the limiting factors are the resources required to achieve this task. The more complicated view of the commander fighting an insurgency is one of propping up, stabilizing and supporting a government. This is combined with being on the defensive and not being able to pick and choose when and how to engage your opponent.

The horizontal structure of successful insurgencies is epitomized in the work of Al-Qaeda, which has a disperse network unconstrained by both geography and the elements of the vertical hierarchy it employs. Rather than locking itself into secret compartments or relying entirely on coded communications Al-Qaeda shares vast parts of its agenda and policies publically through social media. This medium provides all members to have access to strategies and tactics that have been successful. As new members join the organisation they can adopt the elements they

want, form new groups, and undertake violent acts without a difficult approval process.[79] This

global insurgency, perceived by some as uneducated barbarians, has adopted the innovative,

open-source and participatory nature that has been employed successful in high-tech start-ups.[80]

Brafman and Beckstrom describe Al-Qaeda as a decentralised organisation that functions

like a starfish that can still survive if it loses a leg, but which "can really take off" when all the

legs working together. [81] The decentralisation allows Al-Qaeda to survive the loss of leader

Osama Bin Laden in part by using social media to promotes communication and interaction

between the different parts of the organisation.

A similar hierarchy was used successfully by the Apaches, who fought the Spanish as

they laid claim to North America. Whereas under Hernando Cortés the Spanish military was

able to successfully seize control of the Aztec and Inca centralized civilizations, they failed in

their attempts to use a similar approach with the Apaches in the north. Their opponent's

distributed political power and lack of centralization stymied the Spanish strategy of crippling

their opponents' capitals.[82] The Apache behaviour parallels effective social media use for

insurgents. The Apache's had Nant'an – spiritual leaders, who were followed not by obligation,

but for their ability to convince others, a mechanism comparable to gaining a following on a

---

[79] Farwell, *Jihadi Video in the 'War of Ideas,"*128.
[80] *Ibid*., 128.
[81] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Portfolio, 2006), 230.
[82]*Ibid*., 19.

YouTube channel or getting "likes" on Facebook. Much as social media has inputs that are unrestricted by geography, the Apache's had no capital or central command post where decisions were made. [83]

This contributed to the Apache's being a tough opponent. Their flexibility, shared power, and ambiguity made their command and control apparatus immune to attacks that would have destroyed a more centralised society.[84] The Apache's were never really defeated using traditional means; even once the Americans had taken over the territory they occupied, Apache nimbleness and decentralisation kept them independent. However during the First World War the Apaches were effectively broken from within when Nant'ans were issued cattle by the U.S. government, giving them material goods that complemented their spiritual power. This altered the dynamic from a nation where Nant'ans led by example, to one in which they could reward and punish tribe members by leveraging their wealth.[85] This shift in structure led to a more centralised organisation that could be manipulated using traditional means. When combating social media perhaps the most apt comparison was the unintentional path to irrelevancy of the user-generated social news aggregator, Digg. The company essentially self-destructed because of an unpopular site redesign which, echoing the cattle to Nant'an example, gave "publishers an extraordinary amount of power on the site and revoked the ability of users to actually create the news."[86]

---

[83] *Ibid*., 21.
[84] *Ibid*.,, 21.
[85] *Ibid*.,, 151.
[86] Greg Finn, Search Engine Land, "*Diggv4: How to Successfully Kill a Community*," http://searchengineland.com/digg-v4-how-to-successfully-kill-a-community-50450; Internet; accessed 17 January, 2013.

Denying the Insurgents the benefits of Social Media

Providing preferential power to certain members is not the only way to take on horizontal organisations. Good social media strategy supports winning the insurgency but does not rely on a rigid approach. For instance, sometimes denying the enemy access to the field is sufficient for a social media victory.

Censorship, often considered an enemy of the core values of liberal democracy can be an important element of the social media strategy used to combat an insurgency. In addition to limiting their ability to win hearts and mind, effective censorship blocks the insurgent's ability to use the medium for command and control.

The Social Media Matrix for an Outside Force Fighting an Insurgency (Figure 2) demonstrates the factors a commander should consider when determining how to best counter insurgents' access to this medium. The key elements to consider are the strength of the insurgency and the amount of control the government has over the network. When the insurgency is not strong its use of social media can largely be ignored, and simply monitored as another means of assessing public opinion. If the government has a strong degree of network control (the insurgency is confined to a geographic region where the government can influence network carriers and the government has advanced censoring technologies) the government can allow for mostly free access to the technology but selectively censor troublesome areas likes the Anarchist's Cookbook. Conversely, if the insurgency is very active, a government with sufficient network control can enforce heavy and wide-ranging censorship, while a government without that degree of control must instead resort to attacking the network itself.

Figure 2: Social Media Matrix for an Outside Force Fighting an Insurgency
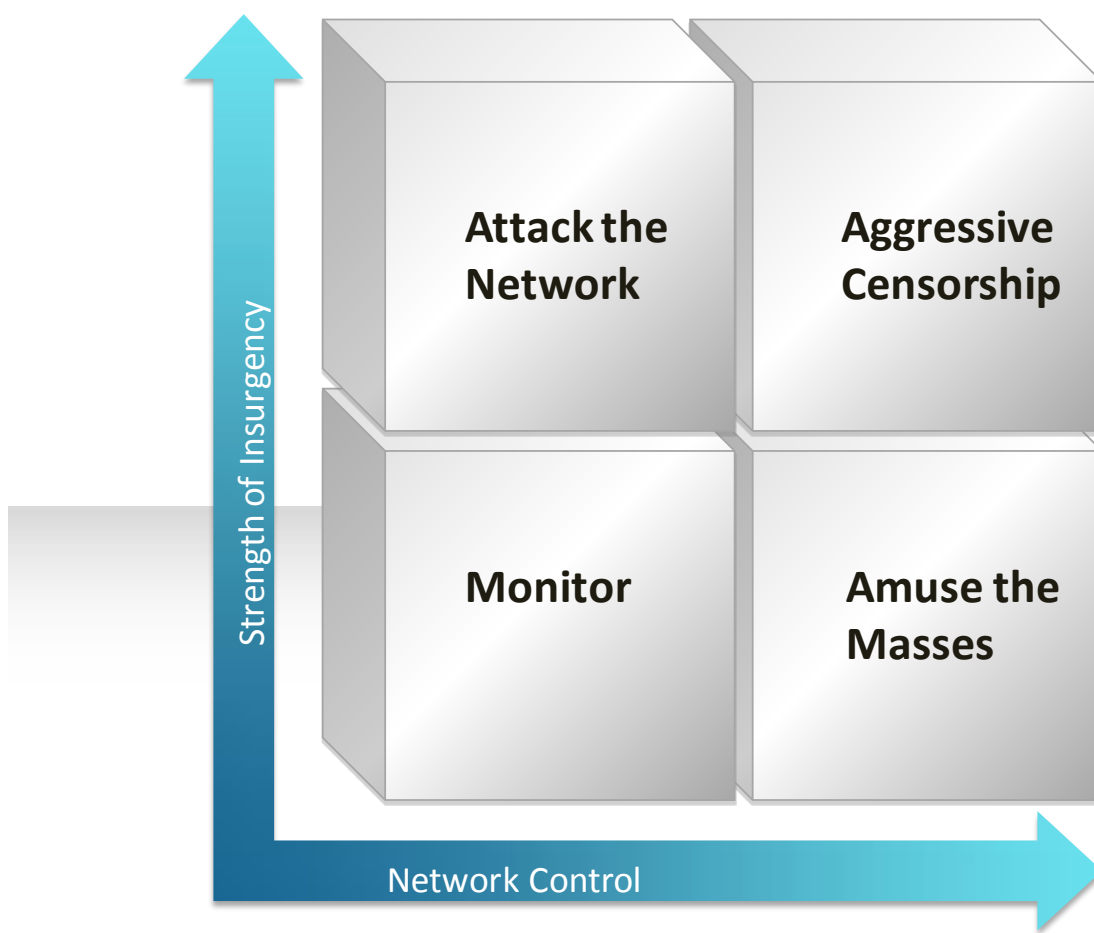
Attacking the Network

In the past when insurgents controlled a method of mass communication a government or occupying power could simply target a printing press, broadcast tower, or television station. Physically countering the message delivery system by taking down websites or cellular towers reflects established military traditions of "if it causes a problem – shut it down," a tried and tested formula that is both simple and effective. [87] Applying the kind of targeting that worked against insurgencies in the twentieth century is much more difficult in the twenty-first, given social media's "multiple nodes and self-healing properties" and the viral nature of the global information environment.[88]

Blunt network attacks by the government should be used sparingly. Rendering a nation's Internet unusable impacts national prosperity because access to this technology is so closely linked to a modern economy. Given the difficulty of attacking the network selectively, and the consequences of such an attack for the economy, it should only be done if the insurgency is very active and those combating it have limited control over the network (typically because of dated technology or lack of control over telecommunication entities). Physical attacks work best in a conflict with a limited geographic scope; halting mobile data in Afghanistan might be justified as a way to fight Al Qaeda, but few would allow the entire Internet to be shutdown to fight the global jihad.

Attacking the network is most effective if authorities have alternative ways to maintain communication and exercise command and control, as they can outmanoeuvre their adversaries and have their opponents become simply a collection of individuals. Essentially, if insurgents

---

[87] Rohozinski and Collings, *Bullets and Blogs...,* 58.
[88] *Ibid.,* 58.

are relying almost exclusively on social media, this can be exploited by a regime that has

effective communication options that are less useful to its opponents.[89] During the Egyptian

revolution the shutdown of the Internet forced the tech-savvy protesters to rely on pamphlets,

faxes and landlines for communications, reducing their efficiency. [90]

   North Korea takes the matter to an extreme, essentially keeping the country in a perpetual

state of government-directed communication and actively suppressing dissent. This has cost it

economically; a comparison of living standards with its southern neighbour is shocking.

However the durability of its regime and lack of substantial insurgency is a testament to the

strategy's effectiveness. However, once a significant insurgency has deeply taken root, "pulling

the plug" on social media is an immediate and temporary solution not a permanent cure.

Radicalisation is largely a real-world phenomenon that will persist even if the insurgent's access

to social media is blocked; revolutions occurred throughout history without the aid of social

media and will continue even if Twitter and Facebook crash.[91]

   The North Korean model is also likely effective because of other factors including its

physical and economic proximity to China. This example aside, blunt destruction of the network

tends to best be used only as a stop-gap. Through its actions a nation or occupying force must

gain credibility with those it seeks to govern, or seek a finer degree of network control moving it

towards another quadrant in Figure 2.   Although network attacks have their place in social

media warfare, if the population is denied access to this communication for long periods, such as

---

[89] Papic and Noonan, *Social Media as a Tool of Protest*.
[90] *Ibid.*
[91] The Centre for the Study of Radicalisation and Political Violence, *Countering Online Radicalisation..., 17.*

in the face of a persistent threat of insurgency, there are economic consequences that will be felt in the bellies and wallets of the people that will lead to widespread dissatisfaction, which in turn can give momentum to a rebellion.

Crackdown Censorship

To avoid this situation a nation with a stronger degree of network control can use hard-line censorship. This allows for the web to still function for financial purposes allowing the state to maintain a stable economic position, but attempts to block the insurgents' social media capability

However, unlike in the early part of the twentieth century, where limited publishers could be relatively easily corralled by oppressive government forces, the use of censorship in social media has second order consequences. Online censorship draws attention to information, identifying it as controversial, and even if you try to eliminate content, it can reappear somewhere else, like the mythical Hydra regaining its heads. Without a truly Herculean effort to eliminate the content from the web it will grow back. One digital file is all that is needed for content to be replicated and reappear. This power of social media is aptly demonstrated in a positive way by Wikipedia, the collaborative online encyclopedia. Its volunteer moderators' ability to keep the site functional in the face of coordinated interference by special interest groups demonstrates the robustness of social media as a means to promote useful information. The site shows how over time a well-run social media network can build a collective institutional memory that can withstand fierce assaults.[92]

Site creators or online forum moderators could be targeted, but may become martyrs as their connectedness means they have a perpetual spotlight on them; their absence is news. An

---

[92] *Ibid.,*73.

alternative to using force and compulsion to take down content in developed countries is the legal system–if the insurgent's identities can be proven. However this strategy can backfire; failed cases can create a body of case law that makes future prosecutions more difficult, especially in nations with a free speech tradition.[93]

Therefore, with current technology any strategy that relies on eliminating content will be crude, expensive and potentially counterproductive. [94] In spite of this, effective censorship is still taking place on the Internet. In a bizarre twist for a medium where geography is essentially irrelevant, content suppression is most effective when the efforts are confined within national borders, as this is where the most effective application of network control can occur. Facing long-term internal opposition, China and Saudi Arabia, leaders in the field of information suppression, have focused on removing or blocking radicalising material on the parts of the Internet that they permit their citizens to access. Both nations have developed sufficient control over their networks to allow partial access to online media but still maintaining strict control. Essentially they have adapted an approach with similar goals to North Korea (eliminate avenues for dissent to fester); however, the wealthier nations' technological edge allows them to strike with finesse in their efforts to control the web, preserving its financial benefit.

China and Saudi Arabia leverage the current state of technology which requires that Internet access requires consumers to pay for the bandwidth that is transmitted over fibre optic lines and airwaves. Services that host blogs and websites need to negotiate to have access to this infrastructure, and in spite of their "don't be evil" motto, even online advertising giant Google can be influenced to personalise search results for a country. As much as talk of social media

---

[93] *Ibid.,* 73.
[94] *Ibid.*, 73.

refers to the "cloud" humans are located in the physical spaces of the geographical world and

currently gaining access to this digital space requires infrastructure that is controlled or which

can be influenced by the state.   Entities that rely on support of other organisations expose

themselves to the type of personalised pressure that cannot be effectively applied to 25,000

relatively anonymous members of a pro-insurgent group. Recognizing this, China has chosen to

work together with enterprises to jointly enforce a highly customised censorship, effectively

blunting the impact of nascent insurgent groups while seemingly having no impact on its

economic growth.[95] Even Scotland Yard, a legendary institution considered a bastion of good

governance in one of the world's most venerable democratic and open nations considered pulling

the plug on Twitter during a period of civil unrest in 2011 in an effort to shut down the rioters

command and control apparatus.[96]

Recognizing the difficulties inherent in censoring a decentralised collective like the

Internet, key actors have decentralised their censoring system. Harnessing the technology's

strength, they use social media to combat social media. Saudi Arabia uses its loosely grouped

network of advocates to point out pages in need of censoring, a task that in some cases earns

cash for the participants. In other cases, actors not formally affiliated with governments, such as

the Jewish Internet Defence Force, take matters into their own hands. The latter was able to

---

[95] Morozov, *The Net Delusion* , 103.
[96] Mark Hughes, The Telegraph, "*Scotland Yard Considered Shutting Down Twitter,*"
http://www.telegraph.co.uk/news/uknews/crime/8705281/Scotland-Yard-considered-shutting-down-Twitter.html;
Internet; accessed 17 January, 2013.

infiltrate and assume the role of moderator of an "118,000 strong Arabic language group sympathetic to Hezbollah" and effectively destroy the group by deleting nearly 110,000 members' accounts.[97]

In addition, online groups can effectively censor a site or channel through repeatedly accessing its resources on a coordinated massive scale in what is known as Distributed Denial of Service (DDOS) attacks. These attacks have famously brought down everything from banks and credit card sites to online gaming platforms. The members coordinate attacks through social media and the hardware and software necessary to participate can cost less than a thousand dollars. The fact that activists can participate in these activities without extensive programming background or complicated hardware democratizes censorship.[98]

Keeping the Masses Amused

Although the kindling of an insurgency may be present, if it has not yet caught fire the outside force should not take the kind of measures it would take during an active insurgency. Given the economic impact of the cost of a destroyed network or the expense of active censorship an alternative approach should be found that allows the nation to remain economically viable.

Many authoritarian governments are displaying a more deft touch in keeping their citizens from becoming involved in an insurgency. Censoring an Amnesty International report but permitting online gaming and pornography keeps citizens occupied, amused and distracted from politics. Focusing on blocking key documents when feasible but largely allowing free access

---

[97] Morozov, *The Net Delusion*, 105.
[98] *Ibid.*,110.

limits the economic burden and as the insurgency is at a relatively innocuous early stage it presents limited risks that would justify the cost to directly oppose it online. In an experiment using a tool called Psiphon, western activists who lent unfettered bandwidth to those behind firewalls found the "revolutionaries" they were supporting frequently searched for naked pictures of famous entertainers.[99] This should not come as a surprise as even in an established democracy with access to all sorts of academic studies, most Americans are not looking to change problems with their government, such as how imprisoned citizens are treated, as much as they are seeking news of the latest Hollywood gossip.[100] Furthermore, the battle cry of "the truth shall set you free" rings hollow when even in an "educated and civilized nation" the birthing controversy surrounding President Obama showed that "the easy availability of evidence to the contrary is not enough to dispel such myths, for they are not always based on the rationale examination of evidence."[101]

Freedom on the Internet has to some degree become akin to the "elections" dictators regularly run to present an aura of legitimacy.   These exercises cost substantial money and resources, and their use throughout the world clearly demonstrated that although laughable in some quarters, these staged performances are a valued part of the regime's image. When not directly combating an active insurgency, those seeking to repress a nascent movement may find it more effective to foster an environment where social media activists can serve as token representatives of freedom which can help the state build foreign and domestic legitimacy.[102]

---

[99] *Ibid.*, 85.
[100] *Ibid.*, 96.
[101] *Ibid.*, 110.
[102] *Ibid.*, 89.

Monitoring the Insurgency

Not all organisations will have the control of the network needed to manage social media activism with the deft touch required when there is not an active insurgency. Preventing insurgents from accessing social media without shutting down the network and making the overall situation worse through economic unrest is not possible for most governments. This does not, however, mean nothing should be done to prevent the situation from worsening.

When an insurgency is limited in scope, actively monitoring the situation can give the government the edge it needs to remain ahead of the insurgents. The fall of an authoritarian regime is frequently unexpected. Providing those in power the ability to harvest data from social media permits investigation and analysis that might limit an insurgency's element of surprise and give those in power time to prepare.[103]

In addition, it is not just the insurgents with captured laptops that can use social media for electronic eavesdropping. Google uses links as part of their algorithm for determining the popularity of a page. Regimes supported by a technologically advanced outside force can reverse engineer this process and assume all pages linked from a useful insurgency page are also potential threats. This effort can be aided by using the weighted (through likes/retweets) links social media sites like Twitter and Facebook provide.[104] Companies like Google and Facebook want to be viewed neutrally for fear that some countries would restrict access to their citizens or that their company would be targeted by insurgents. However human rights advocates argue that

---

[103] *Ibid.*, 165.
[104] *Ibid.*, 100.

Facebook's company's fraud-prevention policy requiring users to sign up with their real identities, "could put people at risk from governments looking to silence dissent."[105]

In order to operate freely in a country, social networking websites need to make deals with the governments and organisations that control the infrastructure. These deals may require the network to share user data, sites visited and GPS locations. Google's arrangements to modify its product inside China in order to have access to enter that nation's citizens, and the company's subsequent withdrawal from the market, demonstrates that national borders can easily block even Internet giants. Recent revelations about the U.S. National Security Agency monitoring Internet traffic demonstrate these concerns are not only relevant in authoritarian regimes. [106]

Even without behind the scenes monitoring and manipulation by the government something as seemingly innocuous as a Facebook profile can be a treasure trove of information for government intelligence collectors. Status updates, "friends" lists, imagery, geographic "check-ins" and sites that are liked can be used to harness one individual's online history to build an organisational profile of an entire insurgent group.[107]

Delivering a Counternarrative

When examining the current online jihad that is occurring over social media, it is apparent that censorship and network denial alone will not have the desired impact. This is because the insurgency is spread over a vast geographic area, and network control or destruction

---

[105] Greg Beaubien, "Facebook Playing a Vital but Reticent Role in Middle East Revolts," *Public Relations Tactics* 18, no. 3 (03, 2011), 4-4.

[106] Papic and Noonan, *Social Media as a Tool of Protest*.

[107] *Ibid.*

is not feasible on a global basis. When insurgents are not restricted to a land mass where the government can exert targeted pressure on broadband providers the limited network control available to the counterinsurgents restricts their ability to deny the enemy access to this strategic resource.

At one time, information superiority meant getting your message out over the airwaves while the opponent had no ability to broadcast.   With social media and the diversity of channels for information, this may be possible to achieve through a kinetic network attack, difficult but feasible in some cases to achieve with rigorous censorship, but in many cases will be simply impossible. This requires a change in tactics and an acceptance by the commander that the enemy's messages will often be seen and heard. The social media strategy needs to be adjusted to deal with the message, not the originator.[108] A commander's goals need to reach beyond information dissemination and message control, objectives which were traditionally associated with winning hearts and minds. Instead the main effort in the social media push is effective communication and "message stickiness" with target audiences. [109]

An example from history that shows a brilliant use of message, medium and messenger to build an effective counternarrative involves none other than the Man of Steel himself. In the 1940s the Superman radio show was used to counter the Ku Klux Klan through an episode arc called "Clan of the Fiery Cross" which revealed secret Klan code words and rituals that

---

[108] Rohozinski and Collings, *Bullets and Blogs...*, 47.
[109] *Ibid.*, 2.

schoolchildren began to use while playing superheroes, effectively making a mockery of an organisation once shrouded in mystique. This broke the spirit of the Klan and crippled its recruiting.[110]

The message was clear, the Klan was a joke. Insurgents are by their nature passionate about their cause and treat it very seriously; social media allows them to shine in the spotlight, but can also allow them to be the subject of mockery and derision from those whose approval they seek.[111] In addition to discrediting the Klan, the Superman show was entertaining, the story included superpowers and heroics, not extensive debates. The medium was simple and direct: an action packed children's radio show that was widely listened to by families across the nation. The messenger was also appropriate for the environment, the National Association for the Advancement of Coloured People, although likely supportive of the program, were not perceived as being involved in the broadcast. Their involvement may have soured the view of the target audience of 1940's white Americans who lived in a world of casual racism.

Building the Counternarrative – Developing Messaging

The narratives of violent extremists tend to combine political, historical, sociological and religious narratives to legitimate their violent actions.[112] This allows them to broadcast "a broad worldview that provides ready-made, swift and easy answers to many complex, real, and valid

---

[110] Mark Juddery, mental_floss, "*How Superman Defeated the Ku Klux Klan,*" Lkanhttp://mentalfloss.com/article/23157/how-superman-defeated-ku-klux-klan; Internet; accessed 17 January, 2013.

[111] Jim Michaels and USA TODAY, "Pentagon Fighting Taliban on Social Media Front," http://usatoday30.usatoday.com/news/washington/story/2012-08-29/pentagon-taliban-twitter-social-media-fight/57418034/1; Internet; accessed 17 January, 2013.

[112] Omar Ashour, "Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy," *Perspectives on Terrorism* 4, no. 6 (12, 2010), 16.

questions." [113] Countering these messages ("it is our homeland," "it is God's will," "they are racially inferior," "their privilege comes at our expense") requires addressing every dimension of their narrative and tailoring the approach based on the audience. A counter-narrative such as the one developed to be used in the Superman gambit against the Ku Klux Klan would look quite different from one built to counter Al-Qaeda. [114]

Despite Twitter limiting messages to 140 characters, social media allows for multiple quick exchanges for debate and discussion. Counter narratives cannot be generic and shallow as this can easily be turned by the opposition (ex: #Canadians say they will blend in with the community create a better life for everyone? Tell that to my brother killed this morning by their tank while driving his taxi!). The tailored narrative needs to be compelling. This means admitting where appropriate the the validity of grievances and offering alternatives to insurgency as a way to address those grievances by highlighting the legitimacy and effectiveness of non-violent strategies. [115]

Insurgencies fester upon a foundation of concerns, and the roots of the problem cannot be addressed by platitudes or by simply ignoring the underlying issues if a counternarrative is going to work. The history of the insurgency needs to be understood and worked into the counternarrative. Even labelling adversaries "terrorists" can separate the actor and the actions from the context and make an organisation less likely to address why certain individuals and ideas have popular support. Beyond the obvious linguistic challenges that occur when operating in the global environment, cultural divides can make getting the message across more difficult.

---

[113] *Ibid.,* 17.
[114] *Ibid.,* 17.
[115] *Ibid.,* 17.

[116] Recognizing the different points of view and finding middle ground is critical when engaging a skeptical audience. [117] Ideology can be used to manipulate the behaviour of a group and if the insurgents' motivation can be delinked from it, the counterinsurgent can, through systemically addressing key issues, negate the unity of the insurgency by placating subgroups.[118]

Winning this struggle means being able to deliver a compelling narrative that counters that of the adversary. Sometimes a direct message can be effective, especially if the goal is not to inspire love or acceptance but to generate fear. Commanders must select appropriate counter-narratives based on relative strengths, the appropriateness for various audiences in question, and their potential impact.[119] During the Operation Pillar of Defence, Israel used a combative social media posture to intimidate Palestinians adversities, an approach that generated international interest as its English Twitter feed doubled its followers during the autumn of that engagement.[120] The 140 character limit of Twitter was used to deliver concise messages that played to this theme such as: "We recommend that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead."[121]

The obstacle a passive population presents to those supporting an insurgency can be turned to an advantage when the outside force is instead supporting a government. Messaging need not necessarily ask audiences to join with those combating the insurgency; in fact doing so may

---

[116] Rohozinski and Collings, *Bullets and Blogs...,* 29.

[117] *Ibid.,* 29-30.

[118] Department of the Army, *Army Special Operations Forces...,* 2-5.

[119] Ashour, *Online De-Radicalization...,* 18.

[120] Yoel Cohen, "Social Media in war: The potential and limits," The Jerusalem Post; http://www.jpost.com/Opinion/Op-EdContributors/Article.aspx?id=297172; Internet; accessed 17 January, 2013.

[121] @IDFSpokesperson, Twitter, https://twitter.com/IDFSpokesperson/status/268780918209118208; Internet; accessed 17 January, 2013.

complicate the message to the point that it loses its impact. Sometimes simply discrediting the terrorist ideas and their ideology is enough to ensure that the cause gains no further momentum.[122]

A final alternative to consider is the use of social media as a tool of deception, as a method to divert an insurgent's attention from the main effort of the force they are combating. Commanders must be cautious of their employment of this strategy as they may risk message confusion. For instance, replicating the famous amphibious assault feint from 1991's Gulf War could potentially be achieved by having numerous Marines tweeting about getting their kit ready for a landing. This approach, however, becomes much more complicated with the kind of focused messaging that is required in dealing with asynchronous warfare with much smaller and more diverse engagements.

Building the Counternarrative – Packaging Content

An outside force, dealing with a foreign culture without the context necessary to relate to their audience may fail to win supporters because of how the message is packaged. The delivery needs to take into account the culture and language needs of different target audiences. Delivering video messages through social media is inappropriate for audiences unable to access high-speed Internet, and lengthy blog posts are ineffective with a largely illiterate audience. Seeking to target a wide audience of foreigners to promote their message, but not necessarily take specific action, Israel used a standard Internet tactic of placing simple words on captivating image. This "meme" was unleashed on social media in a manner typically used to raise awareness for cancer or poke fun at a celebrity. The graphic of missiles falling on western

---

[122] Farwell, *Jihadi Video in the 'War of Ideas,'*146.

landmarks accompanied by the text "What would you do?" appeared on social media feeds across the globe.[123] Had the message sought specific actions (buying bonds, volunteering for the Israeli army) the effect would likely not been achieved, but as an awareness tool, simply asking for this message to be shared helped shape and reinforce public opinion.

As broadband exposure and smartphone use increases throughout the globe, text messages are increasingly accompanied by photos. Given technological progress, video messaging is rapidly evolving into a medium of choice given its rich ability to tell a compelling story.   The Lebanese weekly show, *A Nation Smiles*, broadcast a satirical attack on Hezbollah leader Hassan Nasrullah that so angered him he organised a massive protest, a sign that the mockery made him vulnerable.[124] This echoes the success mockery had in the Superman campaign versus the Klan. Applying this approach to videos in the social media sphere allows a commander's forces to create mash-ups like those favoured by the jihadists conveying fake news. False images and rhetoric could be turned against the enemy with shorts clips that pokes fun at a weakness in a way that does not anger passive supporters.

Building the Counternarrative – Selecting Messengers

Videos mocking jihadists may not work well if broadcast from traditional NATO channels. A strong message delivered in a medium appropriate to the audience may still be derailed if it is presented by a messenger who the population views unfavourably. Host nations, allied organisations, or even, given the multiplicative effect of social media, a few key activists, might

---

[123] @IDFSpokesperson, Twitter, https://twitter.com/IDFSpokesperson/status/268780918209118208; https://twitter.com/IDFSpokesperson/status/269419585101512704; Internet; accessed 17 January, 2013.
[124] Farwell, *Jihadi Video in the 'War of Ideas,"*145.

serve as more able messengers. [125] Converted militant leaders can have credibility with their old colleagues as can respected academics and members of the clergy. These spokespeople can use social media to provide arguments that can modify the "extremists' worldview, thus cracking the duality of 'good' versus 'evil.'"[126] The role for "faceless outsiders" such as nations like Canada or organisations like NATO might be best on the sidelines until a more favourable impression is obtained. Foreign-looking interlopers with obvious cultural differences driven home by their way of speaking, dress, and their manner of interaction might better play a role behind the scenes offering support indirectly through technical, financial or strategic support.

Unfortunately, spokespeople do not always live up to their hype. Expatriates are a valuable resource, particularly in regions where the culture is largely unfamiliar or alien to a planner's frame of reference. However, planners should carefully ensure the individual's claims of being able to command respect are valid. An expatriate's influence in a given country can be inversely proportional to the length of time away from the homeland. [127]

It is evident from the occasional use of the word "crusade" that a good ol' boy Texan may not be the spokesperson that appeals most to the hearts and minds of residents of Iraq and Afghanistan. Given the international nature of the jihad and global demographics, western nations should first look within their borders for allies. Western Muslims are uniquely positioned to act as a voice of reason in online venues but in order for this to occur effectively they cannot be viewed as domestic threats if they visit chat rooms and discuss these topics on

---

[125] Farwell, *Jihadi Video in the 'War of Ideas,"*146.
[126] Ashour, *Online De-Radicalization?...*, 18.
[127] Department of the Army, *Army Special Operations Forces...*, 1-6.

social media.[128] Combating global jihad requires messengers that resonate with the audience and friendly Muslim governments and moderate Muslims are well positioned for this role.[129] In America, some Muslims have indicated a desire to engage with extremists on social media, but have said they felt threatened by the FBI when doing so.[130] American UW doctrine emphasises U.S. forces can "influence resistance movement characteristics, making them more appropriate to the mission. For example, U.S. UW forces could emphasize guerrilla adherence to international norms and standards of behavior."[131] If this can happen abroad, it follows that it should be even easier to achieve on American soil with American citizens, without the need to resort to the military.

Online, arguments and a posting history can establish an identity that is independent of the actual user. However, establishing this online presence takes time, while a Twitter post from the certified account, such as @IDFSpokesperson, carries with it the weight of the organisation (in this case the Israeli military). An alternative to this formal presence are "sock puppets," accounts that are unofficial. They lack the credibility of being official, but can be kept at a distance from the main part of the organisation allowing it to keep it hands clean (unless the ruse is detected). The U.S. has admitted to developing technology that would facilitate military personnel maintaining multiple false online identities permitting them to engage with insurgents in relevant Arabic, Farsi, Urdu and Pashto Internet chatrooms.[132] "Astroturffing" the process of creating an artificial online "grassroots movement" through the use of many fake accounts can

---

[128] Rohozinski and Collings, *Bullets and Blogs...,* 40.
[129] "A World Wide Web of Terror," *Economist* 384, no. 8537 (07/14, 2007), 28-30.
[130] Rohozinski and Collings, *Bullets and Blogs...,* 40.
[131] Department of the Army, *Army Special Operations Forces...*, 1-3.
[132] Neil Fielding and Ian Cobain, "Revealed: US spy operation that manipulates social media," The Guardian, http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks; Internet; accessed 17 January, 2013.

lead key parties to believe there is more support for the movement than actually exists. The speed of celebrity death rumours show that even unofficial accounts can direct the conversation in the social media sphere.   Even Canadian entertainer Justin Bieber's Twitter fan base is composed of thousands of these fake accounts.[133]

A lone legitimate account's credibility can also be very effective. Western militaries could do worse than adopt the model developed by the Israeli Defence Force (IDF) which gained significant traction when their brand was associated with 26-year old snowboarder and IDF officer Sacha Dratwa and his team of web savvy soldiers. Their goal was to ensure Israel's narrative was made public quickly, even as rockets landed in Gaza, and to cut out old media and deal directly with allied activists.[134] The use of using young and technologically adept personnel in social media roles can have a conflict-altering impact requires rethinking the traditional hierarchical mindset. These individuals have the tools to engage in the social media realm but may lack the strategic insight of more senior members of the staff who need to direct and oversee their work.[135]   The guidance they need to be provided is strategic, not tactical. The cut and thrust of the 24-hour social media environment where stories can explode if not corrected is not something that can be micromanaged. Mistakes will be made, but on the whole, being fast and right most of the time, and correcting course as needed, is better than being 100% correct when the subject is yesterday's news. When a mistake is made the organisation will have to live with it; this is simply the cost of existing in a world where information flows instantaneously

---

[133] Newsbeat, "Justin Bieber Twitter follower's '50% fake' says report," http://www.bbc.co.uk/newsbeat/22104058; Internet; accessed 17 January, 2013.
[134] Allison Hoffman, The 'Kids' Behind IDF's Media," Tablet, http://www.tabletmag.com/jewish-news-and-politics/117235/the-kids-behind-idf-media; Internet; accessed 17 January, 2013.
[135] Mayfield , *A Commander's Strategy for Social Media*, 83.

throughout the globe. Those running social media need to be both trained in the required competencies to engage on that frontier and given the authority to make the snap decisions required given the pace of modern information operations.[136]

Implications for Western Militaries

Insurgents throughout the world need not rely on expensive command and control suites in air-conditioned military bases or ships at sea. Having a core membership that can access the Internet through a smartphone and use social media to loosely coordinate actions provides a degree of unpredictability and reactivity that is difficult for a conventional force to achieve. Military leaders are recognizing that they cannot allow their adversary to become more adaptable then they are; Al-Qaeda does not have a 72-step process to approve the use of a new smartphone.[137]

Insurgents have efficiently outmaneuvered western militaries on the social media front. Their classic "starfish" strategy uses a decentralized organization to showcase examples of their opponents using disproportionate force or attacking civilians while simultaneously demonstrating their ability to influence the world through beheadings and destroying coalition vehicles.[138] Unhindered by a bureaucratic hierarchy, their front line operatives are empowered and equipped to immediately respond to opportunities.[139] At minimal cost they have video

---

[136] Rohozinski and Collings, *Bullets and Blogs...,* 67.
[137] Rob McIlvaine, "New Army Chief of Staff Says Networks Determine Future War Successes," *Army Communicator* 36, no. 2 (Summer2011, 2011), 4-5.
[138] Rohozinski and Collings, *Bullets and Blogs...,* 3.
[139] *Ibid.,* 3.

production and web transmittal capabilities at their disposal, which, when combined with

calculated attacks, can create a compelling narrative that resonates with the public. If a sub-unit

chooses a wrong approach, it can quickly be disassociated from the rest of the organisation.

Conversely, some of the most popular social media tools being developed are based in the

west and the most successful social media marketing efforts are being designed by western

minds. These nations' militaries are housed in countries that excel in implementing this

technology. Their citizens are natural netizens, and their scientists and engineers push the

boundary of this medium every day. Harnessing these resources requires commanders to step

back and recognize their traditional military may not be the best source of advice and support for

engaging in this new landscape.

Fighting a starfish organisation requires adopting some of their tactics: central planning,

coordinating kinetic events with strategic messaging and decentralized execution. Providing

social media operators their lanes and letting them operate freely within them gives subordinates

the scope they need to accomplish the mission. Insurgents will not be constrained by a

cumbersome approval process when posting to Facebook; if the organisation combating them is

so constrained it will surely falter. [140] When supporting an insurgency soldiers need to be able to

adopt the methodology of successful insurgents, and this does not mean sitting on a video for

three days awaiting approvals. Soldiers are regularly given weapons, live ammunition and

---

[140] Mayfield , *A Commander's Strategy for Social Media*, 82.

trusted not to shoot their buddy in the back because they have been trained to use the equipment and screened for loyalty. Western militaries need to train their militaries on how to engage targets effectively on social media and entrust them with the tools and authority to do so.[141]

General Petraeus' guidance to soldiers in Iraq speaks to this. He urged his subordinates to create a compelling narrative that works, and continually drive it home through all forms of media. He ordered his forces to be first with truth, let the facts speak for themselves and to turn their enemies' "bankrupt messages, extremist ideologies, oppressive practices, and indiscriminate violence against them."[142]

Petraeus recognized that failing to answer the insurgents' messages bolsters their credibility and undermines his; in a vacuum audiences believe the insurgents, even if they are providing false information. Exchanges in the social media sphere occur quickly and a commander seeking to deliver messages in that space must respond without delay to maintain relevancy. This requires a move away from reactive responses, with centralized control and permissions, toward proactive and ongoing information engagement with decentralized authorities and decentralized execution (rules of engagement), backed up by appropriate training and a clear strategic vision.[143]

Recent changes in policy in Afghanistan have increased the ability of NATO forces to dispute facts immediately and provide counterarguments as soon as the Taliban begins their information operation. To support this kind of approach allied forces need to be able to

---

[141] Rohozinski and Collings, *Bullets and Blogs...,* 58.
[142] David H. Petraeus, "Multi-National Force-Iraq Commander's Counterinsurgency Guidance," *Military Review* 88, no. 5 (Sep, 2008), 4.
[143] Rohozinski and Collings, *Bullets and Blogs...,* 2.

document their actions through imagery which is quickly shared, ensuring that reports of an engagement support the narrative with timely information. [144] This strategy, as opposed to waiting for the "full story" and providing a response several days later, has proven successful. Local media are increasingly seeking out the coalition for its side of the story and viewing the Taliban's claims with skepticism. [145]

Changing military organisations takes time, and social media is a rapidly evolving platform with a plethora of both potentially useful and essentially useless tools becoming available every year. Most modern militaries are behind the times, falling into the classic trap of fighting the last war. In contrast, an insurgent organisation does not need to ensure compatibility with decades of doctrine or legacy operational systems. [146]

Rather than just viewing social media as an avenue for soldiers to embarrass themselves and leak classified data, modern military leaders are recognizing that their approach to social media needs to be considered in all aspects of operations, incorporated into doctrine and assigned to key players on the command team. [147] As the insurgents diversify their responsibility to various cells in their organisations, conventional commanders can do likewise. Allowing Public Affairs, Intelligence or Security personnel to exclusively control the social media strategy would likely produce a less robust approach to its employment. After its introduction, radio was used for everything from entertainment, propaganda and coordinating orders of ammunition. Likewise,

---

[144] Farwell, *Jihadi Video in the 'War of Ideas,"*144.
[145] Jim Michaels and USA Today, *Pentagon Fighting Taliban on Social Media Front*.
[146] Rohozinski and Collings, *Bullets and Blogs...,* 64.
[147] Mayfield , *A Commander's Strategy for Social Media*, 81.

 social media can provide a large variety of benefits to different components of a military force. A broad social media strategy will provide the best opportunity to achieve the results commander desires.[148]

Conclusion

From celebratory videos of destroyed NATO vehicles in Afghanistan, to calls to action delivered over Facebook during protests in Egypt, to dissident suppression in Iran, social media has earned its place as a tool for a commander both to employ and to be prepared to counter. Establishing clear strategy for its employment is hampered by the diversity of its uses; a nation like Canada can be simultaneously working to suppress an insurgency in Afghanistan while supporting one in Libya. Commanders need to recognize that not only will the technology they employ change as social media evolves, but, given the diversity of asynchronous warfare, their approach to the tool must change as well. A commander may need to implement a social media strategy to neutralize the very tactics that were used successfully by allied force in a previous conflict to win the current engagement.

Taking the time to understand the environment, the nature of the insurgency, the tools available to control the network, and how outside interference is viewed will guide a commander in creating the social media strategy. Tactically, the messages, medium and messenger can then be chosen that work both within the chosen strategy and in alignment with the culture of the target audience.

---

[148] Mayfield , *A Commander's Strategy for Social Media*, 82.

Even if they provide appropriate and clear strategic direction, commanders will fail to have the desired impact on the social media component of the insurgency if those charged with implementing their direction are neither adequately trained in this space nor given sufficient authority to make the kind of rapid decisions needed to effectively engage their opponents. Wise commanders come armed with a social media strategy appropriate for the insurgency's environment and a competent team empowered to implement that strategy.

The atom bomb has had a clear short-term impact on modern warfare. Nuclear weapons, however, are relatively difficult for insurgents to acquire and have never been directly used by a nation to suppress a rebellion. In contrast, social media is accessible to billions of people, and more are becoming active online every day. While the nuclear spectre has loomed over many conflicts since 1945, it has been a key concern in only a handful. Social media however, has taken an active role in nearly every conflict in the past few years, and its importance, although initially quite minimal, is growing every day. This evolving method of communication will continue to become more accessible and relevant to insurgencies during the next decade. A message or video using whatever social channel is popular in the near future might eventually be able to have more impact on a conflict than the realization that the opponent has been refining stockpiles of uranium and has the capability to hit domestic soil with one of its missiles.

Social media is a mechanism for human interaction, and as such, the right strategy to employ when making use of it in a given situation is more complex a task than determining how best to assign forces to establish supply lines or demine a harbour. In spite of this difficulty, neutralizing a terrorist training camp, only to be unresponsive while hammered mercilessly on Twitter about that operation, is not an acceptable outcome for those fighting a modern insurgency. Commanders who decide to ignore these tools, or treat them as secondary duties

that can be delegated to a junior media relations officer who has little institutional clout, are not bringing the weight of their experience and training to the social media battlespace. That choice will cost hearts and minds and may lose the war.
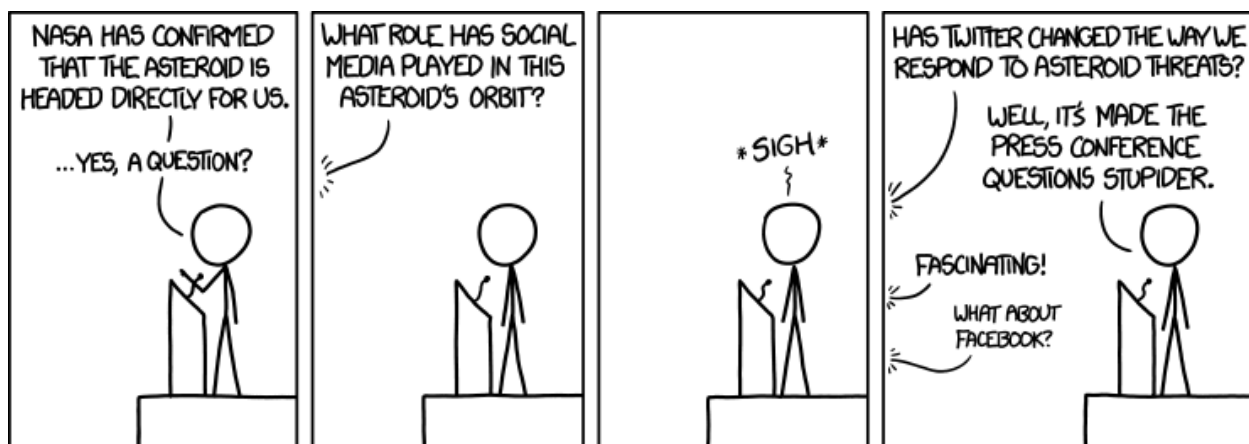
Bibliography

@IDFSpokesperson. *Twitter.* https://twitter.com/IDFSpokesperson; Internet; accessed 17 January, 2013.

"A World Wide Web of Terror." *Economist* 384, no. 8537 (07/14, 2007): 28-30.

Abouzeid, Rania. "Scenes from A Revolution." *Time* 178, no. 8 (08/29, 2011): 40-43.

Ashour, Omar. "Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy." *Perspectives on Terrorism* 4, no. 6 (12, 2010): 15-19.

Beaubien, Greg. "Facebook Playing a Vital but Reticent Role in Middle East Revolts." *Public Relations Tactics* 18, no. 3 (03, 2011): 4-4.

Bowden, Mark. *Worm: The First Digital World War*. 1st ed. New York: Atlantic Monthly Press, 2011.

Brafman, Ori and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Portfolio, 2006.

Campante, Filipe R. and Davin Chor. "Why was the Arab World Poised for Revolution? Schooling, Economic Opportunities, and the Arab Spring." *Journal of Economic Perspectives* 26, no. 2 (Spring, 2012): 167-188.

Certo, Peter. "Israel's Real-World Flame War." *Foreign Policy in Focus* (11/16, 2012): 2-2.

Challand, Benoit. "The Counter-Power of Civil Society and the Emergence of a New Political Imaginary in the Arab World." *Constellations: An International Journal of Critical & Democratic Theory* 18, no. 3 (09, 2011): 271-283.

Cohen, Yoel. "Social Media in war: The potential and limits," *The Jerusalem Post.* http://www.jpost.com/Opinion/Op-EdContributors/Article.aspx?id=297172; Internet; accessed 17 January, 2013.

Comninos, Alex. "User-Generated Content and Social Networking in the Arab Spring and Beyond." *Military Technology* no. 7 (07, 2012): 16-18.

Corstjens, Marcel & Umblijs. "The Power of Evil: The Damage of Negative Social Media Strongly Outweigh Positive Contributions." *Journal of Advertising Research* 52, no. 4 (12, 2012): 433-449.

Curtis, Anthony. "The Brief History of Social Media." http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html; Internet; accessed 17 January, 2013.

DeFeyter, Bruce E. "The Lion, the Starfish and the Spider Hitting Terrorists Where it Hurts." *Special Warfare: The Professional Bulletin of the John F.Kennedy Special Warfare Center & School* 23, no. 2 (Mar, 2010): 26-29.

Dominiczak, Peter. "Enemies Wage a War of Words on Twitter Battlefield." *Evening Standard* (11/15, 2012): 6.

Farwell, James P. "Jihadi Video in the 'War of Ideas'." *Survival (00396338)* 52, no. 6 (Dec2010, 2010): 127-150.

Fielding Neil & Cobain, Ian. "Revealed: US spy operation that manipulates social media." *The Guardian*, http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks; Internet; accessed 17 January, 2013.

Fisher, Len. *The Perfect Swarm: The Science of Complexity in Everyday Life*. New York: Basic Books, 2009.

Ghitis, Frida. "In Iran, Stage Set for Uprising and Violence." *World Politics Review* (03/03, 2011): 1-1.

Gvosdev, Nikolas. "Politics Vs. Social Media in the Arab Uprising." *World Politics Review* (03/04, 2011): 1-1.

Hattem, Julian . "Why do We Laugh at North Korea but Fear Iran?," *The Atlantic*, http://www.theatlantic.com/international/archive/2013/04/why-do-we-laugh-at-north-korea-but-fear-iran/274680/; Internet; accessed 17 January, 2013.

Headquarters, Department of the Army. "Army Special Operations Forces Unconventional Warfare." Unites States of America. https://www.fas.org/irp/doddir/army/fm3-05-130.pdf, 1-4, Internet; accessed 17 January, 2013.

Hoffman Allison. "The 'Kids' Behind IDF's Media," *Tablet*. http://www.tabletmag.com/jewish-news-and-politics/117235/the-kids-behind-idf-media; Internet; accessed 17 January, 2013.

Huesmann, L. R., Eric F. Dubow, Paul Boxer, Violet Souweidane, and Jeremy Ginges. "Foreign Wars and Domestic Prejudice: How Media Exposure to the Israeli-Palestinian Conflict Predicts Ethnic Stereotyping by Jewish and Arab American Adolescents." *Journal of Research on Adolescence (Blackwell Publishing Limited)* 22, no. 3 (09, 2012): 556-570.

International, Business Times. "Meet the Man Responsible for the IDF's Twitter Feed." *International Business Times* (11/22, 2012).

Lipin, Michael. "Chinese Video Game Lets Players Seize Japan-Controlled Island." *Voice of America*. http://www.voanews.com/content/chinese-video-game-lets-players-seize-japancontrolled-islands/1715532.html, Internet; accessed 3 August, 2013.

Lynn, John A. *Battle: A History of Combat and Culture*. Boulder, Colo.: Westview Press, 2003.

Mayfield III, Thomas D. "A Commander's Strategy for Social Media." *JFQ: Joint Force Quarterly* no. 60 (2011, 2011): 79-83.

McIlvaine, Rob. "New Army Chief of Staff Says Networks Determine Future War Successes." *Army Communicator* 36, no. 2 (Summer2011, 2011): 4-5.

Michaels, Jim and USA TODAY. "Pentagon Fighting Taliban on Social Media Front." *USA Today* (.

Mitchell, S. "Web Terrorism: Fact Or Fiction?" *PC Pro* no. 178 (08/01, 2009): 112-114.

Morozov, Evgeny and Inc Books24x7. *The Net Delusion*. 1st ed. New York: PublicAffairs, 2011.

Motadel, David. "Waves of Revolution." *History Today* 61, no. 4 (04, 2011): 3-4.

Mutter, Paul. "Can LOL Cats Help Avert World War III?" *Foreign Policy in Focus* (03/20, 2012): 2-2.

Najjar, Abeer. "Othering the Self: Palestinians Narrating the War on Gaza in the Social Media." *Journal of Middle East Media* 6, no. 1 (09, 2010): 1-30.

Newsbeat. "Justin Bieber Twitter follower's '50% fake' says report." http://www.bbc.co.uk/newsbeat/22104058; Internet; accessed 17 January, 2013.

Papic, Marko & Noonan, Sean. "Social Media as a Tool of Protest." http://www.stratfor.com/weekly/20110202-social-media-tool-protest, Internet; accessed 17 January, 2013.

Petit, Brian. "Social Media and Unconventional Warfare." *Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School* 25, no. 2 (Apr, 2012): 22-28.

Petraeus, David H. "Multi-National Force-Iraq Commander's Counterinsurgency Guidance." *Military Review* 88, no. 5 (Sep, 2008): 2-4.

Pradhan, Sushil. "Internet, Social Media and Terrorism." *USI Journal* 141, no. 585 (Jul, 2011): 366-374.

Pradhan, Sushil. "Social Media as a Catalyst in the Egyptian Unrest." *USI Journal* 141, no. 583 (Jan, 2011): 39-50.

Radwan, Abeer Bassiouny. "Egypt's Facebook Revolution." *American Diplomacy* (02/21, 2011): 1-3.

Rawal, Rajash and Paul Nixon. "Re-Tweet to Democracy? the Social Media #Revolution in Perspective." *Proceedings of the European Conference on e-Government* (01, 2012): 600-607.

Reading, Anna. "Mobile Witnessing: Ethics and the Camera Phone in the 'War on Terror'." *Globalizations* 6, no. 1 (03, 2009): 61-76.

Rose, Charlie. "Charlie Rose Talks to Wael Ghonim." *Bloomberg Businessweek* no. 4267 (02/20, 2012): 20-20.

Salem, Arab, Edna Reid, and Hsinchun Chen. "Multimedia Content Coding and Analysis: Unraveling the Content of Jihadi Extremist Groups' Videos." *Studies in Conflict & Terrorism* 31, no. 7 (07, 2008): 605-626.

Schaar, Stuart. "Revolutionary Challenges in Tunisia and Egypt: Generations in Conflict." *New Politics* 13, no. 3 (Summer2011, 2011): 19-26.

Schipul, Ed & Keeney, Daniel. "War of Words: Social Media's Role in Provoking Revolutionary Change." *Public Relations Tactics* 18, no. 4 (04, 2011): 10-11.

Smith, Tom. "The Social Media Revolution." *International Journal of Market Research* 51, no. 4 (07, 2009): 559-561.

Stefanidis, Ioannis D. "The Fourth Arm." *History Today* 62, no. 9 (09, 2012): 28-34.

Stein, Janice and Colin Robertson. *Diplomacy in the Digital Age: Essays in Honour of Ambassador Allan Gotlieb*. Toronto, Ont.: Signal, 2011.

Venable, Barry E. "The Army and the Media." *Military Review* 82, no. 1 (Jan, 2002): 66.

Weisburd, A. A. "Comparison of Visual Motifs in Jihadi and Cholo Videos on YouTube." *Studies in Conflict & Terrorism* 32, no. 12 (12, 2009): 1066-1074.

"Web terrorism: fact or fiction," PC Pro, http://www.pcpro.co.uk/features/262084/web-terrorism-fact-or-fiction; Internet; accessed 17 January, 2013.

Zahorsky, Ingmar. "Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum." *Peace & Conflict Monitor* (08, 2011): 3-3.

Social Media

https://www.xkcd.com/1239/