International Journal of Communication 7 (2013), 1162–1184 1932–8036/20130005

Social Media and Information Conflict

BRETT VAN NIEKERK[1]
MANOJ MAHARAJ
University of KwaZulu-Natal

Social media is an integral part of the Web's evolution; it has become a nearly ubiquitous technology that can be accessed from traditional desktop computers and many mobile devices. The role of social media in shaping national and global political landscapes came to the fore in the aftermath of the Iranian elections in 2009, and then in the popular uprisings in North Africa and the Middle East in 2011. These and other incidents indicate that social media may play a significant role in future information-based conflict. This article discusses the roles of social media in civil disturbances, strategic security, and military operations to develop a model to describe the potential roles of social media in information warfare. The article also assesses the continuing use and roles of social media in information conflict.

Introduction

Social media is a subset of Web 2.0 technologies, which include all online social networks, weblogs, and wikis. However, Twitter and Facebook have become synonymous with Web 2.0 (O'Reilly, 2005). These technologies are centred on the concept of user-generated content, online collaboration, information sharing, and collective intelligence (Davidson & Yoran, 2007; O'Reilly, 2005). Social media can therefore be seen as a many-to-many communications tool providing interactivity and content on demand, especially when coupled with mobile devices (Coyle & Meier, 2009).

Social media and related technologies have proved to be effective tools in advocacy and emergency communications (Pillay, van Niekerk, & Maharaj, 2010). Mobile phones were a key communications tool in the aftermath of the 2004 Indian Ocean tsunami. This was also the first time mobile phones were used as a fund-raising tool (Coyle & Meier, 2009). Social media also played a significant role in the aftermath of the 2011 Japanese earthquake and tsunami: more than 1,200 Twitter messages per hour were emanating from Tokyo within an hour of the earthquake (Vinson, 2011; Wallop,

[1] A scholarship was awarded to the first author by the University of KwaZulu-Natal for publishing. This article forms a portion of the publishing requirements.

Brett van Niekerk: vanniekerkb@ukzn.ac.za
Manoj Maharaj: maharajms@ukzn.ac.za
Date submitted: 2012–05–14

2011). Twitter was used to provide information on available shelters for stranded people and to raise funds (Vinson, 2011). The "tcktcktck" organization was reported to have mobilized more than 4,500 bloggers in 2009 to raise awareness of climate change issues during the United Nation's 15th Congress of the Parties Summit (Graves, 2009). A Kenyan organization, Ushahidi, has developed free, open-source platforms that crowdsource information during times of crisis. It operates with Twitter, mobile Short Message Service (SMS), and Google Maps and has been used succesfully in many countries for both natural disasters and tracking political violence, including being used to track racist graffiti in the Middle East (Ushahidi, 2012a; Ushahidi Community, 2012). Examples of Ushahidi's free online mapping tool, Crowdmap, include mapping violence against women in Syria (https://womenundersiegesyria.crowdmap.com/) and mapping cyberstalking in Canada (http://crowdmap.cyberstalking.ca/). Despite these benefits, social media has been seen to play a negative role according to some in that it has been used to instigate violence and disorder, such as riots in Greece and England (Taylor, 2011; World Movement for Democracy [WMD], 2009). Such tools can conceivably be used to map traditional and information-based conflicts or accidentally provide information to aggressors in a conflict.

This article discusses the role of social media in information conflict, where information conflict is considered to be an application of information warfare concepts in both military and civilian contexts. Information warfare is defined as "all actions taken to defend the military's information-based processes, information systems and communications networks and to destroy, neutralize or exploit the enemy's similar capabilities within the physical, information and cognitive domains" (Brazzoli, 2007, p. 219). Although information warfare is traditionally a military concept, as this definition indicates, Cronin and Crawford (1999) and Schwartau (1996) have shown it to be relevant to social, corporate, and personal spheres. Information warfare can be seen to encompass various other concepts; for the purposes of this article, the following concepts are considered (Brazolli, 2007):

- Network warfare (or cyberwarfare)—offensive and defensive actions in relation to information, communications, and computer networks and infrastructure.
- Command and control warfare—actions taken to manage, direct, and coordinate the movement and actions of various forces; seeks to protect this ability in friendly forces and disrupt the ability for an adversary.
- Intelligence-based warfare—actions to degrade an adversary's intelligence cycle while protecting one's own.
- Psychological operations— intended to alter the perceptions of a target audience to be favorable to one's objectives.

Information warfare may be applicable to nonmilitary environments; in this case, the term *information conflict* will be used to encompass both military and nonmilitary applications of information warfare tactics. For the purposes of this article, information conflict will include strategic information security and influence operations. Information assets often provide nations or organizations with a strategic advantage. These assets may be attacked by an adversary or competitor to alter the strategic value of these assets (Denning, 1999). Strategic information security seeks to protect these assets.

Influence operations can be seen as an extension of psychological operations to include public affairs, corporate communications, perception management, and similar activities (Larson et al., 2009).

The following discussion of social media in civil disturbances, the impact on strategic security, and the implications for military operations proposes an updated descriptive model of social media in information warfare. The focus will be on the roles of social media in the four aspects of information conflict (network warfare, command and control, intelligence-based warfare, and psychological operations), which will be illustrated by examples.

Social Media and Civil Disturbance

Web technologies first showed promise for political disturbances and advocacy in the 1994 Zapatista campaigns in Mexico. The movement took its struggle online in an effective campaign after being defeated militarily (Mann, 2008), which Ronfeldt and Arquilla (1998) termed a "social netwar." Subsequently, social media has played a significant role in a number of large-scale civil disturbances. These social disturbances initiated through social media are a form of psychological operations or influence operations, where the instigators attempt to sway the perception of the general population into taking physical protest action against the government. These activities, and the government attempts to disrupt protestor dialogue via social media, also can be seen as a form of command and control warfare. The incidents described in this section illustrate the potential for psychological operations and command and control warfare.

The first major incident occurred in Greece in December 2008, when social media was used to orchestrate demonstrations and gain foreign support following a police shooting and to raise economic concerns in the country (WMD, 2009). In April 2009, Moldova hosted the "Twitter Revolution" due to suspicions of fraud during the national elections; this was followed by another in June, when Iranians protested against suspected election fraud (WMD, 2009). The Iranian authorities initially cracked down on conventional media, leaving social media as the primary means of communication outside the country. Subsequently, SMS and social media websites were also blocked. The value of social media as an information source during a media clampdown is demonstrated by the U.S. State Department requesting a delay in Twitter's scheduled maintenance to monitor events in Iran (Coyle & Meier, 2009; WMD, 2009). A month later, Urumqi in the Xinjian province of China, was subjected to Twitter-based demonstrations. However, strong Chinese censorship of the Internet enabled the Chinese authorities to shut down mobile and social media services, preventing their further use (WMD, 2009). SMS was only restored the following year ("SMS Restored," 2010).

Probably the largest SM-induced demonstrations occurred in early 2011 in what became known as the Arab Spring. Massive demonstrations in Tunisia and Egypt resulted in a change of government, and as the "revolution fever" spread, civil war started in Libya and continues in Syria at the time of this writing. Figure 1 shows a screenshot of tweets related to the Syrian violence. The events in Tunisia and Egypt are analyzed in more detail in van Niekerk, Pillay, and Maharaj (2011), yet some mention should be given to the attempted online response by the respective governments. Tunisian authorities attempted to hack into or delete the Facebook accounts of the suspected instigators (Madrigal, 2011), and Egyptian

authorities instituted a full-scale blackout of Internet and mobile services (Kessler, 2011; Kravets, 2011). These countermeasures were not sufficient to end the protests in either country. In the aftermath of the Arab Spring, many African countries experiencing or expecting to experience political unrest (for example, Uganda) proactively blocked access to social media (Malakata, 2011). In the wake of the Arab Spring and a cyberattack against the blogs of Russian political figures, Russian intelligence agencies proposed to block access to social media; however, this was rejected by the Russian government (Isachenkov, 2011). Subsequent calls for protest via social media in North Africa were unsuccessful. This failure can be attributed to the overall context not being sufficient for more protests. Sheldon (2011) comments that

> online social networks did not cause the uprising in the Arab world that began in Tunisia in late 2012, but they certainly played significant roles in accelerating awareness and dialogue among protestors on one hand, and in providing critical intelligence about those very same protestors to savvy security services. (p. 45)

Figure 1. Screenshots of tweets regarding violence in Syria.
Source: Twitter.com (2012).

Although nations affected or threatened by social media–instigated political uprisings have attempted to block social media, it is not clear that these forms of censorship can be sustained for protracted periods. It is likely that the effectiveness of social media in popular uprisings will result in workarounds being implemented to circumvent censorship by governments; in the case of the Egyptian unrest, Google provided a workaround by providing a phone number that people could call and leave a voicemail message, which was then posted as a Twitter message (News24, 2011).

SMS for mobile phones also has been used to facilitate demonstrations. In 2003, demonstrations in the Philippines resulted in a change of government (Rigby, 2008; Rogers, Singhal & Quinlan, 2008). In 2010 riots in Mozambique due to food shortages were orchestrated by SMS (Jacobs & Duarte, 2010). SMS were used in an attempt to incite racial violence in Kenya (Okeowo, 2008). SMS is not part of the Web 2.0

technologies usually associated with social media; however, in these cases, SMS can also be seen as a tool for mass communications and widespread social impact. In 2011 Blackberry's messaging service was the primary communications tool used in orchestrating riots across England. These were similar to the Greek riots in that they were in a response to a police shooting (Potter, 2011; Taylor, 2011). Although Facebook was used in an attempt to further incite violence, this was not successful and the culprits were arrested and sentenced to imprisonment (Carter, 2011). Pakistan reportedly used social media for "rumour campiagns" and to insitgate mobs against other countries in the region (Abbas, 2012). These examples illustrate the use of social media for psychological operations to instigate riots and command and control warfare as demonstrators use social media communications for coordination while affected governments try to hinder this.

Other groups use social media models to advocate for transparency. The main group, WikiLeaks, is responsible for releasing many potentially sensitive documents on the conflicts in Afghanistan and Iraq and diplomatic cables (Goodwins, 2010; Stewart, 2010). The security implications of this are discussed later in this article. In a response to the releases, the U.S. government, financial institutions, and social media websites froze WikiLeaks accounts, and WikiLeaks suffered a series of denial-of-service attacks (Goodwins, 2010; Walker, 2010). This prompted a response by the hacktivist group Anonymous, which conducted denial-of-service attacks against those hindering WikiLeaks, and a series of counterattacks occurred between pro- and anti-WikiLeaks hacktivist groups (Walker, 2010). These events are analyzed in more detail in van Niekerk and Maharaj (2011) and can be considered a form of low-scale cyberwarfare. The WikiLeaks case is significant because it illustrates that online activity in providing information via online social media can result in a more aggressive online response in the form of denial-of-service attacks, which relates to network warfare.

The Anonymous group, inspired by the Arab Spring events, advocated peaceful protests that evolved into the Occupy movement, orchestrated through the use of social media (Kamzi, 2011). The movement went global in October 2012, with protests planned in 82 countries (Agence France-Presse, 2011). Similar groups to the Occupy movement, such as Take Back South Africa, have received moral support from Anonymous. In South Africa and Australia, video messages were posted on YouTube (anonymous21695917, 2012; AnonymousZa65, 2011a; 2011b; windsofchangersa, 2011) supporting the national groups and demonstrating antigovernment sentiment. However, these activist groups do not necessarily represent a majority. Figure 2 shows a screenshot of an Anonymous YouTube video. Often these activities are driven by a minority, yet through the use of social media, they receive as much exposure as a movement representing the majority of a nation's population. Social media can therefore be seen as an equalizer, providing a global voice to small groups.

Figure 2. Anonymous YouTube video against the Australian government.
Source: anonymous21695917 (2012).

Twice in 2009, Twitter itself was targeted by hackers, and stolen Twitter corporate documents were released on a popular IT news website after the second attack in May 2009. The social engineering methods used by this hacker to eventually access credit card information (Carr, 2010) illustrates that criminal elements seeking to fraudulenly access and use credit card or banking information for financial gain may use social media to identify and target susceptible individuals. In August 2009, Twitter and other social media websites suffered a series of denial-of-service attacks. It was reported that these attacks were intended to silence bloggers who were making political statements related to the 2008 Georgian cyberattacks or the denial-of-service attacks on South Korea (Adhikari, 2009; Menn & Gelles, 2009). As with the retaliatory denial-of-service attacks due to WikiLeaks' releases, commentary on social media resulted in an aggressive response further illustrating its relevance to network warfare.

Hackers often use social media and related technologies, partiularly discussion forums. Chinese hackers, however, appear to favor instant messaging platforms rather than Facebook and similar social networks. Hackers in the Middle East (typically pro- or anti-Israeli) use many websites and discussion forums. A Pakistani hacker group used social networking to conduct an attack on and deface an Indian

website. Due to the hackers' poor security, the group's discussions were easy to find, including the order to attack the website (Carr, 2010).

These incidents indicate that social media can play a role in both online protests and instigating physical demonstrations due to ideological differences. In some cases, the social media itself may become a target to silence opposing ideological views. Social media has clearly changed the dynamics of protest actions, where physical demonstrations on the street are held in conjunction with, and even coordinated by, online protest actions that have the ability to reach a global audience. Social media also provides a global platform for protest actions to be held completely online. However, some of the protest or advocacy actions can have implications for information security, and incidents in which this was the case are discussed in the next section. For the demonstrators, social media provides a convenient tool for psychological operations (making their cause known) and the command and control platform (coordinating protest actions).

Social Media and Strategic Information Security

Because social media is based on information sharing, a potential exists for careless posting of information that could result in security risks (Grobler, 2010). The very nature of social media results in it having more vulnerabilities than traditional Web pages. It has scripts for uploading and playing media files, online applications, and other aspects that all can contain vulnerabilities or malicious code that are not visible to the end user (Lawton, 2007). The most common attack types on social media are discussed in the Trustwave (2011) *Global Security Report 2011*: exposure of personal information is at the top, accounting for 30% of recorded incidents, followed by malware, contributing 25% of recorded incidents. Data mining and exposure of corporate information each contributes 20% of recorded incidents, and attacks on reputation account for 5%. This section discusses such attacks in terms of information conflict, particularly considering the requirement for cybersecurity with relation to social media and its use in offensive cyberoperations. The primary focus of this section, therefore, is on the network warfare and intelligence-based warfare aspects of information warfare.

An example of accidental exposure of personal information becoming a strategic security risk is when the wife of a British intelligence head posted personal family details on Facebook. Shachtman (2009a) questions the seriousness of this; however, this information could be used to indirectly attack or influence the intelligence officer through his family (Grobler, 2010). The Slovenian government suffered a breach when recordings of closed government sessions were released on YouTube in December 2011 (Praprotnik, Podbregar, Bernik, & Tiar, 2012). Social media also can be used as a platform for open-source and business intelligence. By searching for listings mentioning a specific organization, it is possible to identify current and past employees and what they listed as their position and expertise. This enables profiling of the organization's employee requirements and potentially gives insights into major projects being conducted.

The WikiLeaks concept of publishing possibly sensitive information to promote transparency in itself is a security breach as the major releases were facilitated by an insider who had access to the intelligence networks (Poulsen & Zetter, 2010). However, other groups have begun attacking

organizations' networks to obtain this information. An example is the hack on the HBGary network, where details of projects for military online operations were released. A project to develop a rootkit code-named "Magenta" (laurelai, 2011) and social network profile management software named Persona (Kerrigan, 2011) were exposed during this breach. These incidents illustrate the possibility of information intentionally being breached through aggressive information warfare tactics and exposed on social media websites. The Persona software is significant in that it indicates the military's interest in using social media to sway perception, a point discussed later in this article.

Specific individuals also may be targeted to gain access to sensitive information or to unwittingly download malicious software. In early 2011, a warning was released on LinkedIn by the U.S. Department of Defense to alert members of the U.S. information operations community of an attempted "false-flag" operation; a fake profile, purporting to be a colonel, was attempting to add these members as contacts (Harding, 2011). Subsequently, a second warning was released by members regarding suspicious profiles (Meeks, 2011). Research shows that high-level personnel may be compromised by fake social media profiles. An example is the "Robin Sage Experiment" described in the *Cisco 2010 Annual Security Report* (Cisco, 2011). This fake profile appeared to be a woman in her 20s with an advanced degree and employed by the U.S. Navy as an analyst focusing on cybersecurity. Within a month, the fake profile made approximately 300 connections, many of whom did not realize the profile was fake. Many of those deceived by the fake profile were high-level employees (Cisco, 2011), which indicates the security risk that social media presents and its possible role as an intelligence-gathering tool. Kerrigan (2011) notes that it is feasible to impersonate an acquaintance from the target's school or college in an attempt to gain access to him or her on social media. Should an individual with access to sensitive information fall victim to such a social engineering or false-flag attack, the consequences could be very serious. Dhanjani, Rios, and Hardin (2009, pp. 223–240) discuss methods of hacking executives in more detail, including via the use of social media. Carr (2010, p. 93) also notes that "social networks are an ideal hunting ground for adversaries looking to collect actionable intelligence on targeted government employees." These examples illustrate the possibility that social media can be used to breach strategic security and gain sensitive information on employees and projects.

As noted above, 25% of recorded attacks on social media were due to malware. The Pushdo botnet used Facebook to distribute malicious e-mails (Westervelt, 2009), and the KoobFace malware tricked users into clicking on a link that redirected them to trojans that hijacked the Web browser (Villeneuve, 2010). Social media may be used in a network warfare scenario to distribute malicious code to either deny network services or gain illegitimate access. Initially, the U.S. military considered banning service personnel from using social media due to the possibility that malware could be pushed to users and compromise the networks (Shachtman, 2009b). This obviously has implications for network warfare, where social media can be used to distribute the malware. This malware also can be used for cyberespionage and can therefore also be considered an intelligence-gathering method.

Social media also may be used to damage or improve the reputation of an organization or individual; Gaines-Ross (2010) labels this "reputation warfare." The speed with which information spreads through social media makes it difficult to contain the released information (accidental or intentional) that could be damaging. Dutta (2010) provides an example of a CEO who was misquoted; Gaines-Ross (2010)

provides examples of how social media platforms were used against corporations, suggests ways to counter such actions, and describes how some strong reactions resulted in poor public relations for an organization. It was noted that social media is not necessarily only a threat, because it also may be used effectively to promote positive public relations (Gaines-Ross, 2010). The implications for corporations is that quality and customer satisfaction need to be carefully controlled, because large numbers of dissatisfied customers complaining on social media will be very damaging for the corporate image, and there may be very little that can be done to recover from this. The use of social media for reputation also applies in the military context, which will be discussed later in this article.

In Somalia, social media is used by pirates and the Al-Shabaab insurgent organization, providing researchers with a tool to monitor and research their activity (Laje, 2012). Additional sources are used to confirm the truthfulness of attack claims posted by the pirates. However, there is still a problem with confirming all the pirates' posts. This provides intelligence to begin modeling piracy activity, indicating the ability to track strategic threats affecting strategic and regional security.

Several online tools are available for managing and monitoring social media campaigns, such as TweetDeck (www.tweetdeck.com), HootSuite (hootsuite.com), Social Mention (socialmention.com), Silobreaker (www.silobreaker.com and news.silobreaker.com), and Addict-o-matic (addictomatic.com). Many of these are free or have trial versions that can be used to gather open-source information or business intelligence on a rival campaign or organization. Google Search and Google Trends also provide information-gathering abilities. Maltego is a downloadable application that allows users to search for information (such as e-mail addresses, phone numbers, social media accounts, and websites) that is associated with the search term. Backtrack is a freely downloadable Linux-based operating system that can be used for penetration testing and hacking. It also contains a social engineering toolbox that allows users to target e-mail and social media accounts. With such an array of freely available tools it is possible to profile organizations and persons, especially if they have a large online footprint. Those with little or no online presence may not be detected by some of these tools, especially those designed for campaign management, where the focus is on aggregating large quantities of information. However, organizations that have strong public-facing online profiles will likely be vulnerable to such intelligence gathering.

Awareness education of employees regarding the security risks of social media is suggested as the best countermeasure to possible attacks. Employees may still access social media from their personal mobile devices or at home, even if the websites are blocked at the workplace, and monitoring access does not prevent a breach (Trustwave, 2011). Humans are often regarded as the weak link in information security (Schwartau, 2010). van Niekerk, Ramluckan, and Maharaj (2011) argue that awareness training may be limited by apathy and human error, and they suggest using a combination of the three techniques: restrict access on sensitive systems or networks to prevent them from being compromised, monitor access to detect whether a potential breach has occurred to respond to it effectively, and educate to raise the awareness of the latest attack methods and countermeasures.

The incidents and concerns discussed in this section illustrate methods through which social media may be used to target high-profile individuals or systems in government, the military, and other organizations. These include false-flag operations using fake profiles, malware, and malicious insiders.

Such activities can be considered as intelligence gathering and network warfare tactics of information-based conflict, and they may have severe consequences should they be successful. The next section discusses the specific impact of social media on military operations.

Social Media Implications for Military Operations

Due to the ubiquitous nature of social media, it is inevitable that military operations will be affected by this technology. This section discusses the benefits and risks of social media in the military environment and explains the implications of social media in a military context. This is a precursor for using social media in an information warfare scenario.

Disaster relief is among the conventional operations that the military conducts. The benefits of social media in emergencies were described above; here, the military perspective will be presented. Even though the military has its own communication systems, social media may be coordinated with civilian relief efforts. A member of the U.S. Marine Corps stated:

> I cannot overemphasize to you what the work of the Ushahidi/Haiti has provided. It is saving lives every day. I wish I had time to document to you every example, but there are too many and our operation is moving too fast. (C. Craig quoted in Ushahidi, 2012b, para. 7)

The Ushahidi crowdsourcing platform (described in the introduction) also provided some benefit to the military operations. Another incident during the Haiti relief operation involved the use of Twitter as an indirect communications platform. An aircraft carrying aid was unable to land and posted this on Twitter; others using the platform saw this and flooded the U.S. Air Force account with tweets. The Air Force responded, and the aircraft landed within an hour (Kennedy, 2010). These incidents indicate that social media may have a beneficial role in military relief operations. Pillay, van Niekerk, and Maharaj (2010) suggest that military units participating in such activities should incorporate social media platforms into their communication procedures to improve their ability to communicate, coordinate, and share information with other national military and civilian relief workers. However, they suggest that it may be difficult to keep military movements secret due to mobile devices with integrated digital cameras and social media applications. Anyone with such a device could take a photo and upload it onto the social media platform, possibly with geolocation information. Once the photos have been uploaded and the movement becomes common knowledge, others may keep watch and take photos. This could provide intelligence just as satellite photos do. Mobile phone cameras may be able to capture unit insignia, and with geolocation data and multiple uploads, the movements of these units could be traced. Although the military may attempt to control the postings of soldiers, it is more difficult to control what is uploaded by outsiders. A denial-of-service attack against popular social media websites could slow the propagation of such images. However, this would require a coordinated network warfare attack with the physical movement of forces. These concepts will have implications for command and control, intelligence, and network warfare.

The Persona software indicates an intention by the U.S. military to actively use social media in perception management or influence operations. This software is reportedly intended to manage fake social media accounts for the purpose of infiltrating groups on social networking sites and posting blogs in an attempt to appear to create a consensus favorable to the United States on controversial issues (Stein, 2011). This software is significant in that it allows an operator to manage up to 10 fake social media accounts. Therefore, each operator has 10 times the influence of a single person. This has the potential to significantly magnify the psychological influence a small group of covert operators can have on a broader audience. However, due to the leaks revealing this software (and inhibiting its effectiveness) and its covert nature, it is unlikely that its full potential will be analyzed in a public forum in the near future. Since 2008, the Israeli Defense Force has been actively using social media for perception management by posting tweets from embassies and videos of precision air strikes (Hodge, 2008). Figure 3 shows a screenshot of the Israeli Defense Force Twitter page. When Israeli troops raided a ship carrying aid, social networking websites were effectively used to sway perceptions against Israel, which responded with its own posts and videos (Shachtman, 2010). The Israeli Defense Force is also reportedly forming specialist "Web 2.0" units by recruiting social media experts (Pfeffer & Izikovich, 2009). It was later reported that a unit had been commissioned to "plug leaks" through social media (Pfeffer, 2010). This may be in response to the careless post by the Israeli soldier mentioned above. Subsequently, social networking sites have been banned for active personnel, because the awareness and warning messages did not appear to prevent careless posts (StrategyPage, 2010b).

Figure 3. The Israeli Defense Force Twitter page.
Source: IDFSpokesperson (2012).

The U.S. military appeared unsure whether to ban access to social media. Initially, it was banned as described above; then the Marines were provided access (StrategyPage, 2010a); then it was reported that social media would not be banned (Ackerman, 2011). As with the Israeli military, the U.S. Army also provided a social media program where soldiers could post their experiences and allow direct interaction with the troops in a public affairs exercise (Gaines-Ross, 2010). The Kenyan army is also "engaged in online exchanges" with the Somali insurgent group, Al-Shabaab (Laje, 2012). Although banning or restricting access may have some impact, it does not prevent posts after the person has left the service. A former Israeli soldier posted a photo of herself posing with prisoners, causing a public outcry. She was no longer serving in the military, so the legalities were not clear; however, the pictures were removed (Wood, 2010). The Russian Federal Security Service has banned its active members from certain social media websites over security concerns. These concerns are well founded, because more than 50 mentions of Russian strategic military assets were found by researchers on Russian social networks, including the location of nuclear weapons bases and major warships (Carr, 2010). A similar study conducted by the U.S. Air Force found that 60% of active-duty members posted sufficient information on Myspace to be vulnerable to targeted attacks, such as blackmailing or kidnapping of deployed personnel (Carr, 2010). These incidents indicate an intended use of social media for perception management and an underlying concern that adversaries can gain intelligence through information leaks.

Social media also can be used as an intelligence tool for gauging public response to operations. An unannounced flight by Air Force One and its fighter escort over New York City caused public panic and then a severe backlash, because it appeared that a commercial airliner was being chased by the fighters; another 9/11-style attack was feared. The U.S. Air Force monitored the public reaction on Twitter (Lardner, 2009). As described in the previous section, careless posting on social media presents a security risk, which holds true in the military sphere. An example is that of a planned raid by Israeli forces that had to be cancelled after the time and place were carelessly posted by a soldier (Hodge, 2010). The references to the location of Russian strategic military assets mentioned above could provide any competing military with useful intelligence (Carr, 2010).

Often the military are deployed in emergency situations, such as during the Arab Spring mass demonstrations. In such situations the military and security services can monitor demonstrator activity via social media, enabling them to react quickly to potential violent outbreaks to maintain peace. Because mobile networks and Internet connectivity can be blocked at the national level, military capability is not required. However, blocking the social media forces the demonstrators into using other methods of communication, which may not be as easily monitored.

The openness of social media and the fact that the technology is constantly upgraded by the owning corporations make it a cheap and stable platform for communications and a convenient platform for deployed personnel to contact their families. The greatest disadvantage is the lack of security that social media provides for scenarios where potentially sensitive information may be accidentally released. This may be circumvented by developing and employing applications that provide end-to-end encryption from the devices to allow secure communications via social media.

Social media has obvious implications for the military, which needs to adapt to this technology and its advocacy of open information. In some cases, the military is actively seeking to employ social media to enhance its public communications and perception management. Because social media also can propagate malicious code, it can be a valuable tool in information warfare applications, in the topic of the next section.

Potential Roles of Social Media in Information Warfare

It is apparent that social media can be used to gain intelligence, propagate malicious code, and sway perceptions. This section examines the role of social media in these activities from an information warfare perspective. The objective is to further develop a descriptive model illustrating the role of social media in information warfare and conflict.

As social media has been employed in perception management and to orchestrate large-scale demonstrations, it has demonstrated its relevance to psychological operations. The active use of social networking by the Israeli military and the Persona software project reveal a clear military application. Johnson (2011) proposes a framework for using social media in a general cyberattack, and van Niekerk, Ramluckan, and Maharaj (2011) propose a framework for conducting a targeted attack and psychological operations through social media. This may not be an effective tactical tool, because its application is tailored more to strategic scenarios in which governments and the general population are targeted. The opposing military forces will also have access to the psychological operation, which may reduce morale.

The Persona software, and social media in general, may be used for targeted attacks against individuals; examples of false-flag operations were provided above. Such social-engineering attacks can be seen as a form of psychological operation. These attacks can trick or coerce the target into providing information in an intelligence-gathering operation or downloading malicious code.

Because cases exist of malicious software propagating through social media, it is feasible that this technology may be employed as a network warfare tool. Malware can be propagated to compromise and illegitimately control systems for attacks or to disrupt the availability of specific systems or networks. The vulnerabilities present in social media also provide attackers with multiple avenues to compromise systems. The rapid propagation of messages through social networks may be ideal to compromise many systems in a short span of time.

Figure 4 illustrates the roles of social media in achieving objectives in various areas of information warfare. Social media can be used in network warfare to exploit vulnerabilities to insert malicious code or gain intelligence and in psychological operations to influence populations and individuals into behaving favorably toward the attacker's objectives, to gain open-source intelligence, and for a convenient communications and collaboration platform for command and control.

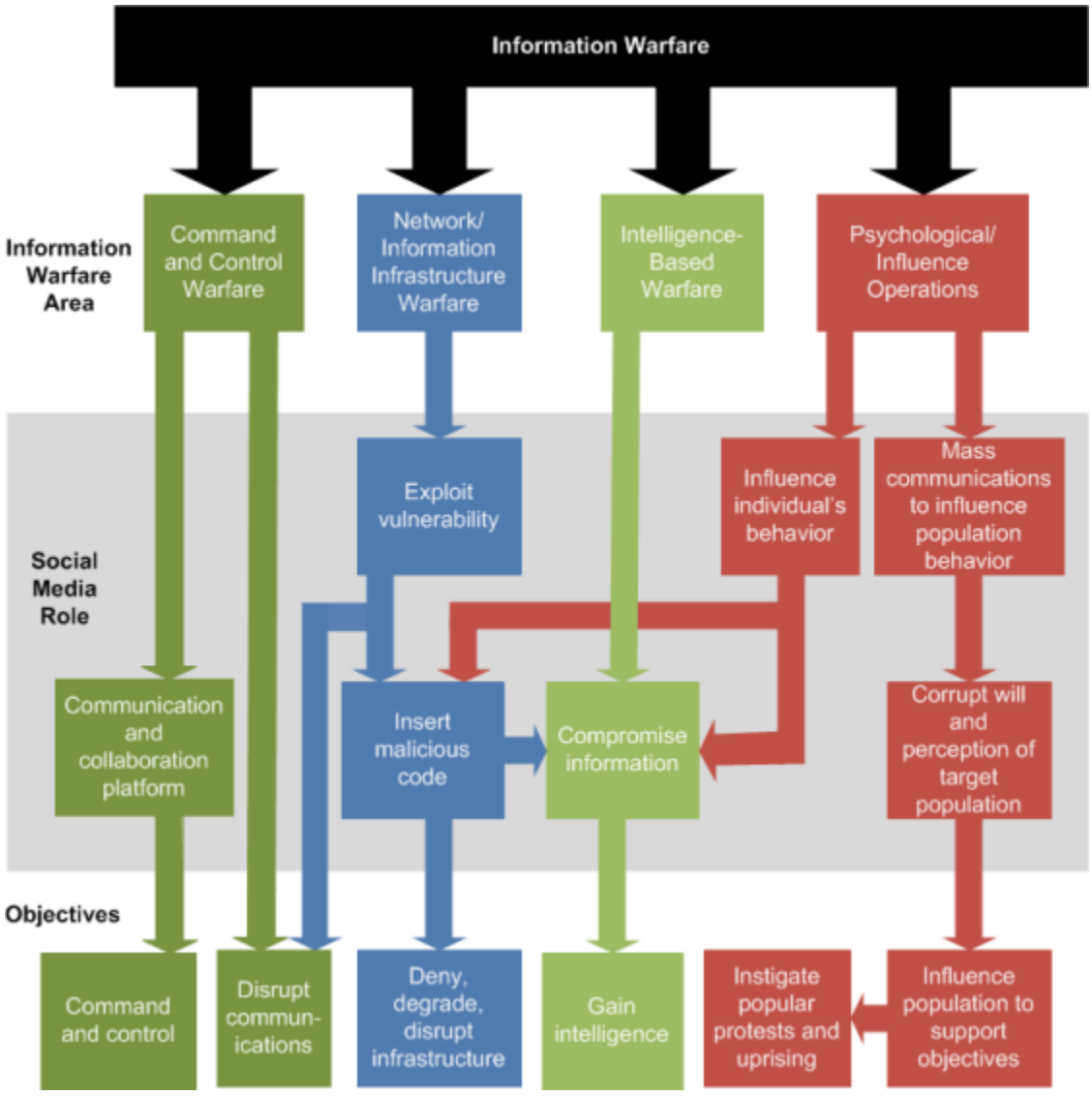

Figure 4. Social Media in information warfare.
Adapted from van Niekerk, Ramluckan, and Maharaj (2011).

Information warfare includes defensive capabilities; therefore, the countermeasures against social media–enabled attacks need to be considered. Blocking access to social media websites on an organizational network may appear to be an obvious solution. However, employees are still able to access social media through personal mobile devices and home computers, thereby reducing the effectiveness of this technique (Trustwave, 2011). The blocking of social media and mobile communications at a national level has achieved mixed results. It failed in the Arab Spring events, yet succeeded in China. Such tactics

may be more successful the earlier they are implemented, prior to the mass demonstration becoming independent of social media. Therefore, the concerned African nations that blocked social media (Malakata, 2011) may have prevented the unrest from gaining widespread popularity and forming mass demonstrations of the scale seen in the Arab Spring. In an organization, restricting access to certain time periods and blocking access to sensitive systems will reduce the likelihood of a serious incident and provide the organization with some control over employees' use of social media.

Although monitoring cannot prevent a leak or attack, it can detect them. This ability facilitates a quick response to an incident. For example, warnings could be distributed in the event of a false-flag incident. Educating users about the threats posed by social media is still considered the best defense (Trustwave, 2011), but, as demonstrated by the Israeli military banning social media access, this is not always fully effective due to apathy and human error. Social media should be included in the reporting of potential threats, such as instituted by the U.S. Army's Threat Awareness and Reporting Program (U.S. Department of the Army, 2010). It has also been proposed to use games on social media platforms to aid awareness training and education (Labuschagne, Veerasamy, Burke, & Eloff, 2011).

The concept of a social media honey pot was proposed by van Niekerk, Ramluckan, and Maharaj (2011). The concept is to use social media profiles and groups to intentionally entice false-flag operations and record and analyze these engagements. Applications to manage fake profiles, such as the Persona software mentioned above, may be used to set up these honey pots and automatically record any activity or invitations on the profiles. Analysis will aid in discovering attack patterns, allowing for the profiling of the attackers, such as their regional origins, or provide signatures to identify the attacker in future incidents. This intelligence may prove to be crucial in awareness training, as specific attack signatures and examples can be provided, allowing for better identification and improved reporting of false-flag attempts.

Several methods may be used to provide layered protection, known as defense-in-depth (Carr, 2010). Awareness training and restricting access are preventive measures; they create a mind-set and reduce the possibility of leaks or successful attacks. Monitoring activity provides the ability to detect and react to incidents. Implementing a honey pot or active analysis of suspicious social media activities will aid in identifying signatures of attacks, which will provide intelligence to improve awareness training and monitoring. Implementing all four solutions will reduce the likelihood of an incident occurring and improve the detection of and reaction to any incidents that do occur.

The Future of Social Media in Information-Based Conflict

Because social media encompasses a diverse range of communication styles, including multimedia and short messages, and connects a wide range of actors, it is a complex network. When looking at complexity theory with regard to information systems, the networked world is an adaptable complex system with the potential to self-organize (Merali, 2006). Likewise, complexity can be seen in military systems, information warfare, and uprisings (Schneider, 1997) such as Arab Spring, where a complex political system is thrown into chaos when it spontaneously reorganizes into a different state. Therefore, information conflict is changing and spontaneously reorganizing due to the disruptive influence of another complex system: social media. The relationship between social media and information conflict

has not yet reached its final state, making it difficult to predict the future with any degree of certainty. However, social media is an ideal tool for information-based conflict.

The use of social media is not always successful in the complex system of politics and conflict. The false-flag operation described was discovered and ultimately failed. Subsequent calls for uprisings in North Africa through social media did not reach the scale of the Arab Spring. Aday, Farrell, Lynch, Sides, and Freelon (2012) warn that the role of social media in the Arab Spring uprisings and similar events should not be overestimated, because traditional media also played a significant role. Similarly, government attempts to block access to mitigate riots had varying degrees of success. Clearly, social media is not the main factor, and the overall context is important. Riots and uprisings cannot be instigated through social media unless the political and social climate is conducive to such events. Social media can therefore be considered a tool for supporting or facilitating information-based conflict, and probably will not be sufficient to create social uprisings on its own.

Given its ubiquitous nature, it can be expected that social media will become more prevalent in information-based conflict, and its roles may initially become more significant. However, social media will, at least for the foreseeable future, remain as a tool to facilitate such activity rather than the primary instigating factor. Social media is one of many variables in a complex system, and it has the capability to facilitate changes of state within that system rather than acting as a catalyst for the state change.

Social media will eventually become less of a network warfare threat or intelligence tool as users become more aware of the information security threats it poses and as the technical controls improve. Because the main purpose of social media is to facilitate communication, its ability to serve as an impromptu command and control network or mass communication platform for psychological operations will remain. Due to its influence in society being in flux, the final state of social media in information conflict is yet to be determined.

Conclusion

Social media has become a ubiquitous communication media; however, it presents security threats and has a role in information conflict. These threats—particularly the vulnerabilities, malicious code, and social engineering—illustrate that social media is a tool that can be used offensively in information warfare. To defend against such attacks, it is recommended that vulnerable people and organizations implement a layered defense with multiple techniques to minimize the likelihood of a security incident from occurring. Social media is likely to continue being a tool in information conflict, but is unlikely to be the prime instigating factor. Its use as a network warfare tool may eventually wane, but it will still be useful for mass influence operations.

References

Abbas, M. (2012, August 21). Web 2.0: Pakistan's new weapon? Retrieved from http://www.ciol.com/News/News-Reports/Web-20-Pakistans-new-weapon/165107/0

Ackerman, S. (2011, January 14). Tweet away, troops: Pentagon won't ban social media. Retrieved from http://www.wired.com/dangerroom/2011/01/tweet-away-troops-pentagon-wont-ban-social-media

Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2012). *New media and conflict after the Arab Spring*. Washington, DC: United States Institute for Peace.

Adhikari, R. (2009, August 13). Another day, another DDoS blitz for Twitter. *E-Commerce Times.* Retrieved from http://www.ecommercetimes.com/story/67851.html#

Agence France-Presse. (2011, October 15). Indignant protests to go global on Saturday. Retrieved from http://www.france24.com/en/20111015-indignant-protests-go-global-saturday

anonymous21695917. (2012, January 6). Anonymous message to the Australian government. Retrieved from http://www.youtube.com/watch?v=tSBXBLH-k8g

AnonymousZa65. (2011a, August 23). Anonymous message: Dear Julius Malema. Retrieved from http://www.youtube.com/watch?v=zG3gCcbX77k

AnonymousZa65. (2011b, August 25). Anonymous message to fight the ANCYL. Retrieved from http://www.youtube.com/watch?v=1O4EJQaaPiw

Brazzoli, M. S. (2007). Future prospects of information warfare and particularly psychological operations. In L. le Roux (Ed.), *South African army vision 2020* (pp. 217–232). Pretoria, South Africa: Institute for Security Studies.

Carr, J. (2010). *Inside cyber warfare*. Sebastopol, CA: O'Reilly.

Carter, H. (2011, August 16). England riot: Pair jailed for four years for using Facebook to incite disorder. Retrieved from http://www.guardian.co.uk/uk/2011/aug/16/uk-riots-four-years-disorder-facebook

Cisco. (2011). *Cisco 2010 annual security report.* Retrieved from http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf

Coyle, D., & Meier, P. (2009). *New technologies in emergencies and conflicts—The role of information and social networks*. Washington, DC: United Nations Foundation; London, UK: Vodafone Foundation. Retrieved from http://www.globalproblems-globalsolutions-files.org/pdf/UNF_tech/emergency_tech_report2009/Tech_EmergencyTechReport_full.pdf

Cronin, B., & Crawford, H. (1999). Information warfare: Its application in military and civilian contexts. *Information Society, 15*(4), 257–263.

Davidson, M. A., & Yoran, E. (2007). Enterprise security for Web 2.0. *Computer, 40*(11), 117–119.

Denning, D. E. (1999). *Information warfare and security.* Boston, MA: Addison-Wesley.

Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The next generation.* Beijing, China: O'Reilly.

Dutta, S. (2010). What's your personal social media strategy? *Harvard Business Review, 88*(11), 127–130.

Gaines-Ross, L. (2010). Reputation warfare. *Harvard Business Review, 88*(12), 70–76.

Goodwins, R. (2010). WikiLeaks shows US cyber intelligence at work, gets DDoS attack. *ZDNET.* Retrieved from http://www.zdnet.co.uk/blogs/mixed-signals-10000051/WikiLeaks-shows-us-cyber-intelligence-at-work-gets-ddos-attack-10021175

Graves, R. (2009, October 9). Blog action day will reach over eleven million readers on climate. Retrieved from http://tcktcktck.org/stories/campaign-stories/blog-action-day-will-reach-over-eleven-million-readers-climate

Grobler, M. (2010). Strategic information security: Facing the cyber impact. In J. Phahlamohlaka, L. Leenen, N. Veerasmay, M. Modise, & R. van Heerden (Eds.), *Workshop on the ICT Uses in Warfare and the Safeguarding of Peace* (pp. 12–21). Bela Bela, South Africa: Council for Scientific and Industrial Research.

Harding, J. (2011). *Warning: IO professionals are being targeted in a false-flag operation*. Retrieved from http://www.linkedin.com/groupItem?view=&gid=2195454&type=member&item=39479605&qid=b3d6de4e-1421-4b62-8b8b-ceb65ef75243&goback=%2Egmp_2195454

Hodge, N. (2008, December 30). *YouTube, Twitter: Weapons in Israel's info war*. Retrieved from http://www.wired.com/dangerroom/2008/12/israels-info-wa

Hodge, N. (2010, March 3). *Israelis nix op after Facebook fiasco.* Retrieved from http://www.wired.com/dangerroom/2010/03/israeli-military-cancels-raid-after-facebook-fiasco

IDFSpokesperson. (2012, August 20). *Israeli defense forces*. Retrieved from http://twitter.com/idfspokesperson

Isachenkov, V. (2011, April 9). *Kremlin rejects FSB proposal to ban Skype, Gmail*. Retrieved from http://news.yahoo.com/s/ap/20110409/ap_on_hi_te/eu_russia_internet_ban

Jacobs, S., & Duarte, D. (2010, September 16). *Protest in Mozambique: The power of SMS*. Retrieved from http://www.afronline.org/?p=8680

Johnson, C. W. (2011). Anti-social networking: Crowdsourcing and the cyberdefence of national critical infrastructures. In G. Grote, M. Bourrier, B. Fahlbruch & G. Motet (Eds.), *Proceedings of the New Technologies and Work Network*. Toulouse, France: NetWORK Consortium. Retrieved from http://www.dcs.gla.ac.uk/~johnson/papers/Gudela/Cyberdefence_And_Anti_Social_Networking.pdf

Kamzi, A. (2011, September 27). How Anonymous emerged to Occupy Wall Street. *The Guardian*. Retrieved from http://www.guardian.co.uk/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous

Kennedy, H. (2010, January 18). Twitter used to help land plane with aid for Haiti earthquake victims. *New York Daily News*. Retrieved from http://www.nydailynews.com/news/world/2010/01/18/2010-01-18_twitter_used_to_help_land_plane_with_aid_for_haiti_earthquake_victims.html

Kerrigan, S. (2011, February 18). US gov. software creates "fake people" on social networks. *The Examiner.* Retrieved from http://www.examiner.com/social-media-in-national/us-gov-software-creates-fake-people-on-social-networks-to-promote-propoganda

Kessler, S. (2011, January 25). *Twitter blocked in Egypt as protests turn violent.* Retrieved from http://news.yahoo.com/s/mashable/20110125/tc_mashable/twitter_blocked_in_egypt_as_protests_turn_violent

Kravets, D. (2011, January 27). Internet down, tens of thousands protest in "Friday of wrath." *Wired.com Threatpost.* Retrieved from http://www.wired.com/threatlevel/2011/01/egypt-internet-down/#

Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. (2011, August 15–17). Design of a cyber security awareness game utilizing a social media framework. Presented at *Information Security South Africa (ISSA) 2011*. Johannesburg, South Africa.

Laje, D. (2012, March 15). #Pirate? Tracking modern buccaneers through Twitter. *CNN Online*. Retrieved from http://edition.cnn.com/2012/03/15/business/somalia-piracy-twitter/index.html

Lardner, R. (2009, August 10). Air Force used Twitter to track NY flyover fallout. *ABC News*. Retrieved from http://abcnews.go.com/Technology/Politics/wireStory?id=8290402

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., et al. (2009). *Effective influence operations: A framework for enhancing army capabilities.* Santa Monica, CA: RAND Corporation.

laurelai. (2011, February 14). HBGary INC. working on secret rootkit project. Codename: "MAGENTA." Retrieved from http://crowdleaks.org/hbgary-inc-working-on-secret-rootkit-project-codename-magenta

Lawton, G. (2007). Web 2.0 creates security challenges. *Computer, 40*(10), 13–16.

Madrigal, A. (2011, January 24). The inside story of how Facebook responded to Tunisian hacks. *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/#

Malakata, M. (2011, April 28). Uganda moves to block social networks. *Computer World Kenya.* Retrieved from http://www.computerworld.co.ke/articles/2011/04/28/uganda-moves-block-social-networks

Mann, A. (2008). Spaces for talk: Communication technologies (ICTs) and genuine dialogue in an international advocacy movement. *Asian Social Science, 4*(10), 3–13.

Meeks, D. (2011, August 9). Warning! Suspicious contacts on LinkedIn. Electronic Warriors Network group on LinkedIn. Retrieved from http://www.linkedin.com/groups/WARNING-Suspicious-Contacts-on-LinkedIn-1705277.S.65284431

Menn, J., & Gelles, D. (2009, August 6). Concerted cyber-attack takes down Twitter. *Financial Times.* Retrieved from www.ft.com/cms/s/.../038b9b54-82a6-11de-ab4a-00144feabdc0.html

Merali, Y. (2006). Complexity and information systems: The emergent domain. *Journal of Information Technology*, *21*(4), 216–228.

News24. (2011, February 1). Google launches Twitter workaround for Egypt. Retrieved from http://www.news24.com/SciTech/News/Google-launches-Twitter-workaround-for-Egypt-20110201

Okeowo, A. (2008, February 19). SMSs "tool of hate in Kenya." *Mail & Guardian Online.* Retrieved from http://www.mg.co.za/article/2008-02-19-smss-used-as-a-tool-of-hate-in-kenya

O'Reilly, T. (2005, September 30). *What is Web 2.0?* Retrieved from http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1

Pfeffer, A. (2010, January 20). *IDF sets up "Facebook" unit to plug media leaks*. Retrieved from http://www.haaretz.com/hasen/spages/1143897.html

Pfeffer, A., & Izikovich, G. (2009, December 1). *New IDF Web 2.0 unit to fight enemies on Facebook, Twitter*. Retrieved from http://www.haaretz.com/hasen/spages/1131918.html

Pillay, K., van Niekerk, B., & Maharaj, M. (2010, October 11). Web 2.0 and its implications for the military. In J. Phahlamohlaka, L. Leenen, N. Veerasmay, M. Modise, & R. van Heerden (Eds.), *Workshop*

on the uses of ICT in warfare and the safeguarding of peace (pp. 50–57). Bela-Bela, South Africa: Council for Scientific Research.

Potter, N. (2011, August 9). London riots 2011: Protestors use Blackberry Messenger; hackers support them. *ABC News.* Retrieved from http://abcnews.go.com/Technology/london-riots-2011-protesters-blackberry-messenger-hackers-back/story?id=14264839

Poulsen, K., & Zetter, K. (2010, June 6). U.S. intelligence analyst arrested in WikiLeaks video probe. *Wired.com Threatlevel Blog.* Retrieved from http://www.wired.com/threatlevel/2010/06/leak

Praprotnik, G., Podbregar, I., Bernik, I., & Tiar, B. (2012). A Slovenian perspective on cyber warfare. In D. Ventre D. (Ed.), *Cyber conflict: Competing national perspectives* (pp. 251–278). London, UK: ISTE Wiley.

Rigby, B. (2008). *Mobilizing generation 2.0: Technologies to recruit, organize, and engage youth.* San Francisco, CA: Jossey-Bass.

Rogers, E. M., Singhal, A., & Quinlan, M. (2008). Diffusion of innovations. In D. Stacks & M. Salwen (Eds.), *An integrated approach to communication theory and research*. New York, NY: Routledge.

Ronfeldt, D., & Arquilla, J. (1998). *The Zapatista social netwar in Mexico.* Santa Monica, CA: RAND Corporation.

Schneider, J. J. (1997). Blacklights: Chaos, complexity, and the promise of information warfare. *Joint Forces Quarterly* (Spring), 21–28.

Schwartau, W. (1996). *Information warfare: Chaos on the information superhighway* (2nd ed.). New York, NY: Thunder's Mouth Press.

Schwartau, W. (2010, February 2). *Simply security: You cause data breaches. TheSACompany.* YouTube. Retrieved from http://www.youtube.com/watch?v=5ks2Iz2qeGA

Shachtman, N. (2009a, July 6). UK spy chief's Facebook fail: Big deal, or big whoop? *Wired.com DangerRoom Blog.* Retrieved from http://www.wired.com/dangerroom/2009/07/uk-spy-chiefs-facebook-fail-big-deal-or-big-whoop

Shachtman, N. (2009b, July 30). Military may ban Twitter, Facebook as security "headaches." *Wired.com DangerRoom Blog.* Retrieved from http://www.wired.com/dangerroom/2009/07/military-may-ban-twitter-facebook-as-security-headaches

Shachtman, N. (2010, June 1). Israel turns to YouTube, Twitter after flotilla fiasco. *Wired.com DangerRoom Blog.* Retrieved from http://www.wired.com/dangerroom/2010/06/israel-turns-to-youtube-twitter-to-rescue-info-war

Sheldon, J. B. (2011). Why cyberpower matters to both developed and developing countries. In K. Vignard, R. McRae, & J. Powers (Eds.), *Disarmament forum—Confronting cyberconflict* (pp. 41–50). Geneva, Switzerland: United Nations Institute for Disarmament Research.

SMS restored. (2010, January 18). *The Daily News,* p. 4.

Stein, J. (2011, March 2). Spy bloggers not "friending" U.S. targets, Centcom says. *The Washington Post*. Retrieved from http://voices.washingtonpost.com/spy-talk/2011/03/spy_bloggers_not_friending_us.html

Stewart, P. (2010, October 25). *Pentagon braces for huge WikiLeaks dump on Iraq War*. Retrieved from http://news.yahoo.com/s/nm/us_usa_iraq_leaks

StrategyPage. (2010a, April 1). *Marines return to Facebook*. Retrieved from http://www.strategypage.com/htmw/htiw/articles/20100401.aspx

StrategyPage. (2010b, November 1). *Facebook will be shot at dawn.* Retrieved from http://www.strategypage.com/htmw/htiw/articles/20101101.aspx

Taylor, C. (2011, August 9). *London riots: Blackberry Messenger used more than Facebook or Twitter.* Retrieved from http://mashable.com/2011/08/08/london-riots-blackberry-messenger

Trustwave. (2011, January 19). *Global security report 2011.* Retrieved from https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

Twitter.com. (2012, August 20). #Syria. Retrieved from http://twitter.com/#!/search/%23syria

U.S. Department of the Army. (2010, October 4). Army regulation 381-12. *Threat awareness and reporting program*. Washington, DC.

Ushahidi. (2012a). Retrieved from http://www.ushahidi.com

Ushahidi. (2012b). Testimonials. Retrieved from http://www.ushahidi.com/about-us/newsroom/testimonials

Ushahidi Community. (2012). Deployments. Retrieved from http://community.ushahidi.com/deployments

van Niekerk, B., & Maharaj, M. (2011). The IW life cycle Model. *South African Journal of Information Management, 13*(1). Retrieved from http://www.sajim.co.za/index.php/SAJIM/article/view/476

van Niekerk, B., Pillay, K., & Maharaj, M. (2011). Analysing the role of ICTs in the Tunisian and Egyptian unrest from an information warfare perspective. *International Journal of Communication*, *5,* 1406–1416.

van Niekerk, B., Ramluckan, T., & Maharaj, M. (2011, July). *Web 2.0 as an attack vector against strategic security.* Presented at the *Fifth Military Information and Communications Symposium South Africa (MICSSA 2011)*, Pretoria, South Africa.

Villeneuve, N. (2010, November 12). *Koobface: Inside a crimeware nework.* Retrieved from http://www.infowar-monitor.net/koobface

Vinson, J. (2011, March 11). Social networks become preferred lines of communication during Japan earthquake. *WebProNews.com*. Retrieved from http://www.webpronews.com/japan-earthquake-social-networkin-2011-03

Walker, R. (2010, December 9). A brief history of Operation Payback. *Salon.com.* Retrieved from http://mobile.salon.com/news/feature/2010/12/09/0

Wallop, H. (2011, March 13). Japan earthquake: How Twitter and Facebook helped. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/twitter/8379101/Japan-earthquake-how-Twitter-and-Facebook-helped.html

Westervelt, R. (2009, October 27). Pushdo botnet uses Facebook to spread malicious email attachment. *SearchSecurity.com.* Retrieved from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1372558_mem1,00.html

windsofchangersa. (2011, August 25). *Message from Anonymous: To the South African people.* YouTube. Retrieved from http://www.youtube.com/watch?v=53tCd4jusxo

Wood, P. (2010, August 17). Israeli woman soldier denies Facebook photos wrongdoing. *BBC.* Retrieved from http://www.bbc.co.uk/news/world-middle-east-10997011

World Movement for Democracy. (2009). *Twitter case study*. Retrieved from http://www.wmd.org/resources/whats-being-done/information-and-communication-technologies/case-study-twitter