REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11/05/2017	Master's Thesis	JUNE 2016 - MAY 2017

4. TITLE AND SUBTITLE
SOCIAL MEDIA'S ROLE IN SHAPING WARFARE

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Buchanan, Christopher M., LCDR, USN

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC COMMAND AND STAFF COLLEGE
MARINE CORPS UNIVERSITY
2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
A revolution in online relationships, social media is shaping warfare by providing an immediate communication platform with global reach and effect, unbounded by age, religion, or language. Social Media is evolving and integrating rapidly worldwide shaping warfare in both positive and negative waves.

15. SUBJECT TERMS
Social media, Internet of Things, lone wolf, Warfare, Facebook, Ukraine, Terrorist, Cyber Terrorism.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	28	(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Social Media's Role in
Shaping Warfare

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

LCDR Chris Buchanan US Navy

AY 16-17

Mentor and Oral Defense Committee Member: Matthew Flynn
Approved: 5/2/17
Date:

Oral Defense Committee Member: Daniel M Bishop
Approved: 2 May 2017
Date:

J.W. Gordon
5/5/17

Executive Summary

Title: Social Media's Role in Shaping Warfare

Author: Lieutenant Commander Chris Buchanan, United States Navy

Thesis: A revolution in online relationships, social media is shaping warfare by providing an immediate communication platform with global reach and effect, unbounded by age, religion, or language. Social Media is evolving and integrating rapidly worldwide, shaping warfare in both positive and negative waves. This reality bends the information war in favor of western states willing to embrace the small risk of being connected to an open Internet

Discussion: Fifty percent of the world population has access to the internet and as wireless networks expand as expected to do, so will total internet penetration. Cyber security, and the challenge to keep pace with changes, presents a significant threat to national security. Cyber-attacks, internet information campaigns, and terrorist activities are prevalent throughout the internet. From a belligerent's perspective, the internet, and social media in particular, offer a vital target in US national infrastructure, which can also be used operationally to achieve political agendas. Social media has emerged as a global phenomenon with a massive and diverse audience. Facebook alone has almost two billion users a month and over a billion daily users. The mass communications that social media offers could be a weapon of words that can influence the hearts and minds of a targeted audience. A terrorist organization can use social media for mass disruption in cyberspace that can have effects in the physical world. It is an extremely low-cost, easily accessible force multiplier that requires expensive technology and highly trained cyber security experts to properly counter.

Conclusion: Instant worldwide communications through the internet utilizing the tools that social media provide have changed the information environment. While just a tool, the potential for both good and bad present undeniable potential and will have to be a constant consideration for warfighters**.** As the speed of news cycles increase, users will be injected with headlines meant to entice clicks and fund advertisement campaigns. Education and cyber security investment will ensure this new information environment builds more than it destroys. Warfare will continue to be shaped by people with agendas, and now, with social media accounts. Continued investment in cyber security and educating social media users will strengthen and instill ethical values and enlighten the filter social media puts on reality.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Page

Table of Contents

Introduction

The Internet of things (IoT) is a new term used to describe the concept of anything having an on or off switch connected to the World Wide Web and sharing information.[1] Fifty percent of the world's population has access to the internet, and as wireless networks continue to grow, so will total population access.[2] Two factors that have contributed significantly to this rapid growth are the creation of social media sites and ultra-portable, cheap Personal Electronic Devices (PED). Near instant communication in an affordable PED has drastically reduced the time and distance of communication making the world a little bit smaller and easier for anyone regardless of age, education, or experience to use. Wireless networks blanket the world and create an environment where everything connected will send information, ideally to improve quality of life. While the IoT provides many opportunities for connections not fully comprehended, the adherent openness of the IoT presents a security challenge as well.

Cyber security, or lack thereof, presents a significant threat to US national security. The hazards of cyber attacks, information warfare, and terrorist activities are prevalent in this growing phenomenon. From a belligerent's perspective, the IoT, and social media in particular, offer a vital national infrastructure target and can also be used operationally to achieve political agendas.[3] Social media has emerged as a global phenomenon with a massive and diverse customer base. Facebook alone has a dedicated monthly user base of 1.7 billion people, and just over one billion of those users log in every day.[4] The Multinational Capability Development Campaign (MCDC) defines social media as, "internet based platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content, that can influence awareness, perception, and acceptance and can promote behavior indirectly as a means of interaction."[5] Mass communications offer a weapon of words that can

influence the hearts and minds of a targeted audience, and social media offers the tools to screen, recognize, and exploit that audience. In the hands of a terrorist organization social media can be a weapon of mass disruption that can have effects in the physical world. In the hands of nations favorably disposed to democratic ideals, the same platform dispenses an ideological challenge. Emerging technology that is tremendously easy to use can connect to the IoT at an extremely low cost, and is readably available acts as a force multiplier that requires expensive technology and highly trained cyber security experts to properly counter. A revolution in online relationships, social media is shaping warfare by providing an immediate communication platform with global reach and effect, unbounded by age, religion or language. This reality bends the information war in favor of western states willing to embrace the small risk of being connected to an open Internet.

Social Media is Shaping Conflicts

Social media has taken war to the hearts and minds of anyone plugged into the internet. This evolving online experience is shaping conflicts by bringing enormous amounts of information to civilian populations. It provides a platform to reach large audiences instantly and anonymously, and has created a layer of opportunity for online battles to affect the physical domain in computer systems and cognitively in people's attitudes.[6] Carl von Clausewitz famously wrote that war is the continuation of politics by other means.[7] As one of the main channels of communication used today, social media has amplified how actors use a hybrid approach of cyber attacks and information campaigns to further their political agendas. At a rate of twelve new users a second, social media sites are increasingly shaping hearts and minds through sheer volume of surfing traffic. Fifty-four percent of all internet users log in to Facebook, and 1.15 billion of those users log in daily from a mobile device.[8] This rapid growth

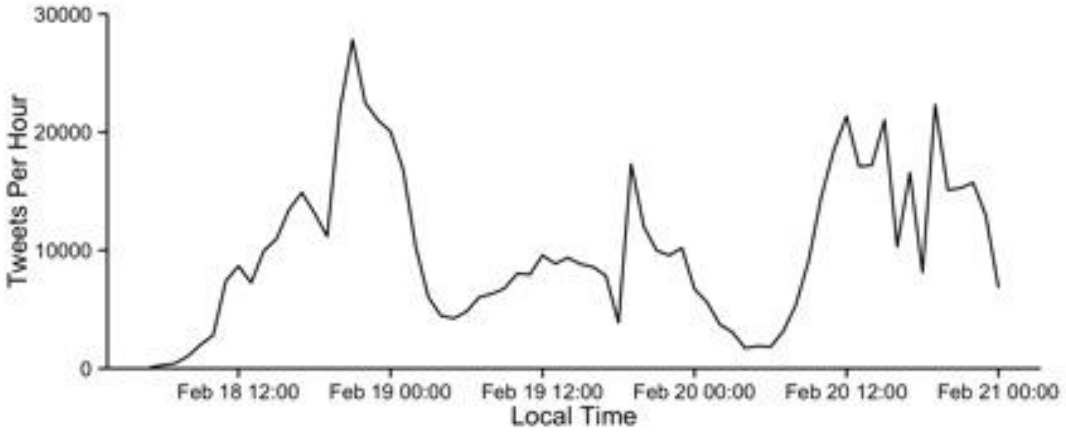
has a very tangible downside. Social Media is being used by terrorist organizations to mobilize an audience for action and recruit isolated and susceptible individuals to train for, and carry out, lone wolf terrorist plots.

While social media has the potential to frame and vocalize the popular opinion it can also dilute the truth, spinning support for radical agendas. Operational planners, key leaders, and even consumers must take into consideration what is driving the media fury in the moment. However, this capability can also be used to harm those who launch terrorist attacks. This duality means that efforts to curb terrorism online may well erode freedoms online, and in turn, erode civil liberties of states trusting in democratic governance and rule of law. Clearly, threats and advantages lurk in the cyber domain, and a balance must be struck between each.

Conflicts in Ukraine and Syria have demonstrated social media's abundant information collection abilities for intelligence use, the opportunity to influence beliefs and attitudes of a select target audience, and the tools to coordinate and rally that audience for action. The civil unrest in Ukraine, referred to as 'Euromaidan' as that nation looked to align closer with Western Europe, arguably started with a Facebook post offering a time and location for assembly from well-known journalist Mustafa Nayyem[9]. The post triggered a movement calling together protestors that ignited an uprising that lasted three months and involved hundreds of thousands of citizens. A few months prior to this firestorm, several opposing political parties combined and organized a regional protest against the current president to demonstrate the critical dissatisfaction of the people. Initial planning supported 100,000 protestors but drew less than thirty thousand rendering the effort futile. While this event went flat, the Euromaidan movement went viral, gaining momentum and spreading by the second ultimately toppling the elected president.[10] The seemingly instant communication social media enables all types of groups to

connect and coordinate, including the previously sidelined spectator by bringing political movements into their internet news stream. The average Joe, or Ukrainian in this example, can become influential organizer simply by knowing how to use social media sites better than politically minded activist. Social media tools also educate and inform the global community as events are unfolding, helping protest movements secure international support or, at the very least, attention that helps sustain activists.

Twitter and Facebook played an interesting role in keeping observers abreast about developments on the ground in Ukraine. The number of tweets using a Euromaidan type hash tag



in the initial days exceeded 8,000 per hour. Tweets per hour fluctuated as events unfolded peaking during the most violent times.[11] Euromaidan established a Facebook page that drew in more than 200,000 followers in the first ten weeks setting a Ukraine Facebook record.[12] This remarkable progression is visually depicted in the graph above.[13]

Those supporting the movement in Ukraine organized Twitter storms to bring Euromaidan hashtags to the top of the world wide trending topics bolstering the movement's popularity. In a survey conducted by Oxford University Political Scientist Olga Onuch,

participants explained that Facebook provided more reliable information than television.[14] Onuch hypothesized that social media sites played an important role in diffusing escalating broadcasted news information and helped protestors frame their complaints balancing trending topics with multiple sources. The Social Media and Political Participation (SMaPP) Lab of New York University posted results from analyzing social media contributions during the crisis and highlighted key factors trending from the most popular sites. One conclusion drawn from the Ukrainian protests was that:

> social media users strategically adapt the tools available to them to the situation on the ground as well as to the local social media context. In a country where Twitter is less used than Facebook, organizers employed Facebook as a tool for informational exchange and strategic planning, as well as to mobilize needed resources and to fill gaps or supplement on the ground strategies.[15]

By comparing the language used, Facebook being mostly the local language, and Twitter fragmented with English, Twitter targeted the international audience. Feeding the international community trending headlines, sparked support from key leaders across the globe. U.S. Assistant Secretary of State Victoria Nuland visited Independence Square in the Ukrainian capital Kiev, in December the day after Secretary of State John Kerry issued the following statement:

> disgust with the decision of Ukrainian authorities to meet the peaceful protest ... with riot police, bulldozers, and batons, rather than with respect for democratic rights and human dignity. As church bells ring tonight amidst the smoke in the streets of Kyiv, the United States stands with the people of Ukraine. They deserve better.[16]

Additionally, the UN, NATO, and several other nations condemned publicly the violence against pro-European demonstrations.[17]

Social media sites can support strong messages representing popular opinion, and they can also carry a government diplomatic message at large, efficiently and cheaply. The risk is, the

message can be tainted by cyberattacks and the unexplainable science behind what can actually "go viral." This mix of information from opposing views diminishes the reliability of true information, an excellent tactic for someone who simply needs to keep information away from the sway of public opinion or shape it while it develops in cyberspace. Ukrainian government networks were targeted by "patriotic hackers" using social media sites to organize efforts, according to Catherine Theohary, a specialist in national security policy and information operations. [18] Theohary noted that both sides tried to control the information environment. "The Russian government has used the blogosphere to control the narrative of the conflict, allegedly by mobilizing hacker collectives and encouraging them to maintain several accounts and to post and comment on multiple social media outlets per day," she wrote.[19] The tools social media offers to rally disgruntled citizens are nonrestrictive and could be used against a popular movement as seen in Syria.

The Assad government is using social media to track and eliminate opposition members by using tactics and equipment received from Iran. [20] Surveillance and communications gear in conjunction with technical networking support enable the Syrian government to control the viral narrative and quietly oppose rebel forces. This is Assad's intent, but social media outlets have shown to work against as well as for Assad even with Iranian technology support. Social media has diminished the Syrian uprising momentum where many Syrians believed that if social media could help Egyptians during the 2011 revolution, then it would help their cause.[21]

Both sides in Syria are dedicating personnel to manage social media profiles, promoting their side of the story and influencing the international information. Interestingly, Twitter has been a key factor in raising funds for the rebel forces. Hajaj al-Ajmi, a Kuwaiti sheikh with 347,000 followers, has been so effective in raising funds that other rebel groups have named

themselves after him.[22] While it is difficult to track the amount raised, a few 'thank you' videos have been posted to Facebook and YouTube acknowledging amounts up to $600,000.[23]

Terrorists Use Facebook

Technology available in smartphones or other hand held devices allows anyone to film, and share in near real time, cheaply and with very little knowledge. The mobile phone has taken over as the most popular web surfing tool, shrinking required equipment to a single hand held device that is easily concealable.[24] The advances in technology have given an edge to motivated individuals allowing them to spread their message online. This capability could alter armed conflict and its reach simply by being so readily available. The recruitment of terrorists for lone wolf attacks clearly marks the extent and risks of such a simplistic networking capability. Terrorist organizations have effectively weaponized social media for recruitment and training by seeking vulnerable people, exposing them to infectious philosophies and encouraging them to join abroad or inflict terror locally in lone wolf attacks.[25]

The Islamic State (IS) "essentially has outsourced terrorism by filling the digital world with propaganda."[26] Terrorist organizations before social media had a hard-enough time finding new recruits, not to mention where and how to train them. They often settled for rudimentary training camps in barely tolerable locations in which they could thoroughly indoctrinated their ideology. "That is old school terrorism," writes Johnnie Moore an expert in terrorist organizations. [27] New school terrorism is utilizing social media networking tools to digitalize the training ground and essentially open doors to sympathizers in cities and countries worldwide. "You no longer have to live in a city you do not know with a language you do not speak to join this war. ISIS has eliminated this barrier of entry by turning the Internet into its training camp,"

says John Arquilla and David Ronfeldt, experts on cyber terrorism and national security.[28] Social Media's spread of information has effectively reduced the boundaries of time and distance for mass communication. Mark Wallace, CEO of the Counterterrorism Extremism Project, cited a study in testimony to the US House Foreign Affairs Subcommittee that 90% of terrorist organizations online activities occur on social media sites.[29] Counter terrorism units at least know where to look. Using communication networks to track terrorist online poses fewer legal restrictions and could be done with an automated surveillance program.[30] This poses a dilemma where cyber terrorism risk via social media platforms exist but so does the opportunity to catch, stop, and prevent that terrorist actions. The US is winning the cyber war and as long as Cyber capabilities can keep up, tracking terrorist online makes sense. CyberSquirrel1 is a project that gathers information on cyber attacks of critical infrastructure of disrupted electrical grids often considered the most vulnerable opportunity for cyber terrorists. As of January 8th, squirrels have more successful attacks on power grids than any state actor.[31]

The European Union defines terrorism as "intentional acts that are committed with the aim of seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization."[32] The Department of Homeland Security declared lone wolves and small group attackers as the most dangerous threat to national security in the US.[33] IS and Al-Qaeda are actively recruiting by playing on easily manipulatable fears, such as gun control or economic collapse, inciting fear against government and local law enforcement. By encouraging decentralized terror through acts of violence, at the discretion of the attacker, terrorist organizations can cost-effectively push their agenda with little to no immediate physical threat,

except for that of the sacrificial lone wolf.[34] They are predominantly interested in recruiting disgruntled military veterans, capitalizing on their military training and experience to enhance their success in carrying out violent attacks.

IS and Al-Qaeda openly encourage lone wolf attacks on dense tourist destinations in their online training camps and acknowledge that any form of violence against law enforcement or government is accepted.[35] Execution plans and advice on how to conduct an attack are provided online and include directions to make household bombs like the pressure cooker bombs used by the Tsarnaev brothers during the Boston Marathon in 2013.[36] During an interview with spokesman NYPD Counterterrorism Bureau and New York Daily news, Stephen Davis discussed the awareness of similar online postings but does not consider it to be an overt and direct threat.[37] Capability and intent are obviously present, but he concludes that lone wolf terrorist attacks are rare. Since 2004, more attacks have been logged than in the previous thirty-three years, but this includes non-terrorist related attacks.[38] Discerning the difference between a self-motivated individual murderer and a terrorist lone wolf attack takes time and investigation.

An "active shooter" as defined by the Department of Homeland Security is an individual "actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims" and often associated with suicide. [39] There is considerable gray area in distinguishing what category an attack falls under between mass murderer or terrorist motivated lone wolf, categorically summarized by ideological or nonideological motivation.[40] Lone wolf attacks are not necessarily the work or influence of a terrorist organization, but could be carried out in the same manner by a single individual due to their own ideals, mental instability, or personal

motivations. As discussed in an article by Ramon Spaaij assessing the lone wolf terrorist, he draws the following hypothesis:

> Both Ideological and non-ideological active shooters tend to be White males in their 30s, with rather dysfunctional adult lives. They tend to be single/divorced, unemployed, have low levels of education, and suffer from mental illness. These similarities suggest that "lone wolves" and "deranged shooters" may be outcomes of the same social and psychological processes. The only meaningful difference may be that for ideological shooters ideological extremism is intertwined with their personal frustrations and aversions toward society. These findings are consistent with the idea that lone wolves and deranged shooters are but a part of a larger phenomenon of lone-actor grievance-fueled violence.[41]

It is easy to see how the individual as described above could be manipulated through social media, but despite the amazing corruption potential social media offers, a person will not typically self-radicalize. Radicalization characteristically relies on group thought where individuals receive their ideological education and are supported by like-minded persons. "It is a rare individual who possesses the requisite combination of will, discipline, adaptability, resourcefulness and technical skill to make the leap from theory to practice and become a successful lone wolf," writes George Michael, an expert on terrorism and political violence.[42] This data suggest a clear vulnerability to deter lone wolf attackers in addressing or countering the group influence. However, this vulnerability is wrapped in a clock of encryption, difficult and very hard to find.

Terrorist Online and Encrypted

Terrorist organizations, led by a revolving door of survivor-leaders, do not necessarily have a strategic or synchronized cyber initiative. Reassurance, recruitment and intimidation make up the foundation for the plethora of content any terrorist with a personal electronic device chooses to upload. The tactical approach being applied is dubbed "leaderless resistance" where an individual or small group engage in terrorism attacks independently of any official movement,

leader, or network of support.[43] Each member is free to select and carry out any operation that they believe will further the group's agenda. The group cohesion and ease of global access social media offers makes small dispersed cells more effective. Chat rooms and online forums are used to create virtual communities to attract and influence those with a common interest. Advances in encryption have made these resources exploitable by terrorist organizations with little to no threat of privacy invasion from government hackers. End-to-end encryption was added to all forms of media service by the second largest self-contained communications network in April 2016.[44] More than a billion people send messages, make phone calls, or share videos using the encryption service offered by WhatsApp. With end-to-end encryption in place, not even WhatsApp's employees can access the information shared over their network.[45] Similar to the case between the FBI and Apple when the former requested Apple to unlock the IPhone of a shooter, WhatsApp has no way of complying even if a court order demanded access. Like Apple, WhatsApp is refusing to reveal what they consider protected information securing customer rights to anonymity across the board.

Social media effectiveness for a belligerent of any kind rests on technological sophistication, otherwise every offensive tactic would also be a vulnerability. Encrypted sites offer a secure environment to openly plan and train lone wolf operatives and online communities to encourage group adhesiveness that further provides power and fuels the individual's motivation.[46] The social congruence among members that stand behind a common cause act as a force multiplier. Social networking brings a very wide diversity for a message increasing the possibility that susceptible individuals will stand behind the philosophy. "When social ties are strong, building mutual trust and identity, a network's effectiveness is greatly enhanced. This can be seen most clearly in ethnically based terror, crime, and insurgent groups in which clan ties

bind together even the loosest, most dispersed organization," comments John Arquilla, and David Ronfeldt, in the RAND sponsored book, *The future of Terror, Crime, and Militancy*.[47]

Intelligence gathered in Afghanistan revealed the level of depth that Al-Qaeda was able to plan for 9/11 attacks using the internet with simple cyber security measures. Al-Qaeda covertly conducted reconnaissance and gathered information that was shared via encrypted messages on secure sites.[48] A website operated by the Muslim Hackers Club reportedly hosts links to sensitive information like radio frequencies used by the US Secret Service. The group offers to train and educate beginner hackers with basic hacking techniques and preloaded viruses set for distribution.[49] Free imaging software like Google Earth are available to anyone with an internet connection and allow terrorists to plan, in significant detail, attacks without any previous reconnaissance. A computer seized in Afghanistan contained structural engineering specifics of a dam, that allowed Al-Qaeda engineers to simulate a catastrophic failure.[50] The usefulness of a robust and detailed mapping software cannot be overemphasized. This capability gives a belligerent the freedom to "conduct a detailed reconnaissance exercise without the need to physically be at the location" and drastically reduces the opportunity security forces have to detect preemptive warnings and also cuts down on the operational cost of an attack.[51]

Cyber Terrorism or Hacktivism

Our lives are becoming more electronically integrated every day, and the internet makes up a large portion of that connection. The World Wide Web represents core American values in its adhering to freedom of expression, creativity, and innovation. Originally designed as a way to share information for scientists, the World Wide Web discourages security and privacy in its expansion into our everyday lives. Having the same password for every site visited makes things

easier to access, but it is not very secure. Internet security works against the conveniences that are appealing about the internet. State and non-state actors conduct cyber operations and commit significant resources to further political, economic, and even military objectives through the internet. Investments in cyber security and cyber defense fight an uphill battle as conveniences to internet, and its availability, spread disproportionately.

Cyber terrorism is a premeditated attack on organizations, individuals, or government information, computer programs, or systems motivated by an agenda.[52] In a hybrid approach to further political agendas, social media is being used as a tool in information warfare to influence hearts and minds with the intent to disrupt targets in the physical world. Cyberterrorism and other forms of cybercrime aim to destroy or degrade large systems of critical and noncritical infrastructure, ultimately spreading fear. Social media applications are currently being used to shape public opinion about ongoing conflicts. In a world of abundant information, being the first to deliver a message, regardless of truth, can have a significant impact.

Terrorist organizations have used social media sites against US military commands in an attempt to disrupt service and degrade confidence. Islamic State sympathizers, Cyber Caliphate hacked US Central Command's Twitter account in 2015.[53] All the group did was repost material already available to the public and send taunting posts for the troops. In doing so, that group tarnished the effectiveness of any message broadcast through the site due to the possibility of corruption. Twitter retaliated by banning over 2,000 accounts they believed to be linked to ISIS or its supporters.[54] In the larger scheme of things, the defacement of a command's Twitter page is insignificant, albeit

embarrassing. Cyberterrorism combines the fear of cyber-attacks with a psychological fear, or distrust in new and emerging technologies. The cost-effectiveness of a cyber attack cannot be understated, but 'losing' a laptop with personal identifiable information (PII) can be just as dangerous, if not more so.

As online interactions continue to grow and encompass more economic roles the potential for increased cyber attacks concurrently rises. Cyberterrorism seeks, or as a result of the attack, violence against persons or property, or at a minimum generating enough fear to validate the attack while more generic cyber attacks would be considered simply a cyber crime. Dorothy Denning, a professor of computer science, in her testimony on the subject before the Congressional House Armed Services Committee, delineated Cyberterrorism from cyber crime or 'hacktivism':

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[55]

Cyber terrorism is not limited to terrorist organizations; state actors, as seen in Ukraine, like to play this game to further their political agenda. While terrorist organizations have an interest in any vital infrastructure or vulnerable physical targets, other attackers seek opportunities to wreak havoc and are less directed at physical harm to individuals.[56] Deliberately planting misinformation in sensitive databases, alternating or deleting components in command and control systems will cause mayhem but most likely not get anyone killed. Similar to any planned operation, cyber terrorism operations are carefully planned with a clear idea of aims and

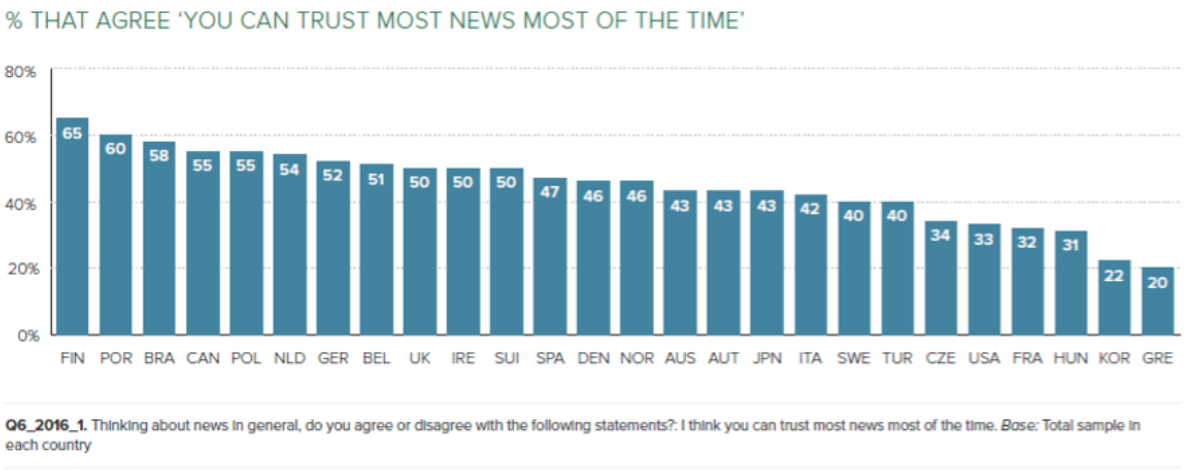
effects.[57] Further reducing the cost, only a limited number of people and equipment are involved but the results could still be devastating. A trend is shaping around the internet and social media in that cyber terrorists have added digital infrastructure to the target list ultimately altering the modus operandi.[58] The terrorist organizations cyber attacks have evolved from generally quite simple methods to very rational, sophisticated, and purposeful attacks. A successful cyber attack does not need to destroy anything, in fact simply misleading information could be just as dangerous if the false information goes viral. Similar to a military deception operation , this type of attack is directed at the public opinion, which can wreak havoc and spread distrust amongst previously unified supporters.

Social Media Shapes Our Perceptions

After the 2016 presidential election, Facebook's co-founder and CEO, Mark Zuckerberg was questioned about the prevalence of fake news thriving on the social media site. Some critics believed this misleading information helped Donald Trump get elected.[59] In response, Zuckerberg posted that Facebook is a technology company and not a media company where users determine what media to follow.[60] Free speech is a core American value that has a place of reverence in the internet and on social media. New technologies have a way to bring back old arguments with new and disastrous spins. The beginning years of television brought on a similar discussion where the nature of a medium determines the messages it carries. Television would transform all public discourse into entertainment.[61] Television has certainly diluted public discourse, but it also has brought new and informative ways to reach larger audiences. Social media by its very nature encourages social interaction and discussion, arguably for both good and bad. The capability exists to seek and find information, entertainment, and social interaction in a moment's notice with a device that is globally connected.

In 2016, Reuters Institute for the Study of Journalism (RISJ) compiled the annual *Digital News Report 2016,* polling more than fifty thousand people in twenty-six countries, making it the largest comparative study of news consumption in the world.[62] Key findings revealed that fifty-one percent of all survey participants use social media as a news source and that television news sources are declining.[63] Facebook leads the brackets as the dominant social network for news across all countries surveyed. Social networks like Facebook, Twitter, and YouTube offer more than just discovery of news headlines; they inherently encourage discussion.[64] News shares are predominantly articles or topics users approve of, which in turn increases positive stories; however, this depends on location. As indicated in the *Digital News Report 2016*, Facebook users in the UK tend to be more combative sharing headlines they do not actually like but would like to discuss.[65]

The importance of trust in news organizations is a respected core value and legitimate organizations strive to maintain a high level of trust with the public. However, anyone can post almost anything to a social media site. News brands rather than individual journalist are the main component to maintaining trust according to Nic Newman, an expert in journalism research at the Reuters Institute.[66] Displayed in the graphic below is the response by each country to the question; "thinking about news in general, do you agree or disagree with the following statements? I think you can trust most of the news most of the time." Percent that agrees "you can trust most news most of the time."[67]



Fake news is certainly a concern and this research report identifies a significant gap in trust from news sources. Mike Hanley, an expert in digital communications, wrote, "The World Economic Forum, identified the spread of misinformation online as a major risk in its Global Risks Report as far back as 2013."[68] As with any advancement in technology both good and bad uses are brought to light; a sword can protect, but it can also kill. Social Media provides the opportunity to get rich, share emotions, find treasured connections and share valuable information concurrently with the ability to inflict malice, encourage physical violence, steal money or information and spread misleading information. Information is shaping our online opinion and being utilized to define the narrative for warfare. Declining trust in news agencies increases social media users to be misled by false information as true and false news blends online.

Social media can be used effectively by terrorist organizations and state actors in gray zone conflicts to further political agendas against a superior military. Gray zone conflicts are actions short of a traditional armed conflict and fall outside the normal peace or war construct.[69] Some aggression or use of force could be used but ambiguity and confusion reign in place of decisive military action. Operation Valhalla in 2006, was an engagement between US Special Forces working jointly with Iraqi Special Forces facing a Jaish al-Mahdi (JAM) death squad also

known as the Mahdi Army.[70] US forces tracked down the death squad responsible for the brutal murders of several civilians and Iraqi troops. US forces in a joint attack killed 16 or 17, captured 17, destroyed a weapons cache and rescued a badly beaten hostage.[71] This sounds like a successful operation, except that in the time it took for the force to return to base (less than one hour) additional death squad soldiers returned to the scene and rearranged the bodies of their fallen comrades to appear as if they were unarmed in the middle of prayer when they were murdered by American soldiers.[72] Pictures and press releases in Arabic and English showing the alleged atrocity were released through social media stating the soldiers entered a mosque to kill these unarmed men.[73] Even though the Special Forces unit filmed its entire action and could prove the allegations where wildly inaccurate, they were not able to get in front of the negative press nor did they expect such a quick media response from the enemy. Combined Joint Special Operations Task Force, Arabian Peninsula (CJSOTF-AP) planned for a minimum twenty-four-hour window to release information to the media based on experiences with AQ. This assumption and due to an outdated intelligence policy that lacked social media considerations, it took almost three days before the military even attempted to tell its side of the story.[74] Considering the pace of news streams on the internet, this was too slow to make a difference, the damage had been done. Further adding to the problem, the Army was forced to launch an investigation that lasted 30 days causing the battalion to stand down from all operations.[75] The US public opinion is the center of gravity for insurgents or any actor that cannot accomplish their goals where US forces are operating. If public opinion in the US can degrade enough, US forces will discontinue or withdraw operations.

Media is increasing its effect as a weapon of war. In many emerging operations, US public opinion is continuing to be a critical vulnerability. Media is a major component of terrorist

threat capability that poses challenges to properly and effectively counter. David Lapan, a Marine Colonel and the former spokesman for II MEF – Forward, stated in a journal article written by Cori E Dauber: "Our adversaries doesn't play by rules, … the enemy has no qualms about beheading people, about torturing people….so lying isn't really a concern of theirs".[76] It is not to be understated that determining a proper counter to this type of campaign can be considerably difficult.

Conclusion

Cyber security will continue to be a challenge as the internet expands. Information warfare and its counter in operations presents a significant threat to US national security and foreign policy. For those seeking to target the United States, the IoT, and social media in particular, offer a vital national infrastructure target that can also be used operationally to achieve political agendas.[77] The global phenomenon that social media has created is pushing information abundantly to users and is shrinking the news cycle forcing news agencies fight to be the first to report a status This limits time to source check as we expect news agencies to do. Social media is being used to communicate locally and to broadcast an international narrative recruiting opinions at a phenomenal rate. Mass communications on a global scale offer a weapon that can sway the hearts and minds of a targeted audience and social media offers the tools to screen, recognize, and exploit that audience. Cyber terrorism, and a slew of other cyber terms still emerging, can be a weapon of mass disruption having effects in the physical world by both average users and terrorist organizations intent on malice. In the hands of state actors favorably inclined to democratic principles, the same platform dispenses an ideological challenge. Emerging technology designed to be intuitive for a worldwide audience, can connect to the IoT at an extremely low-cost, and is readably available, acts as a force multiplier to any organization,

group or person posting online. This capability requires expensive technology and highly trained cyber security experts to properly counter. Social media is not all doom and gloom as can be seen at times from news organizations fighting misinformation or politicians fighting an unpopular opinion. With a global reach to more than half of all internet users, social media has made the world a smaller place by increasing communications and providing a platform to keep families, friends, communities connected, albeit invasively.[78] As this revolution in online relationships grows, social media will shape warfare by providing an immediate communication platform with global reach and effect, unbounded by age, religion or language. This reality bends the information war in favor of western states willing to embrace the small risk of being connected to an open Internet.

The internet is free. Convenience of access, or just access, might come at a cost but the internet is free to use. As the internet reaches further and intertwines itself into society, the uses and abuses will have to be analyzed for a risk assessment. As with any new and developing technology, education and experience will be crucial to limiting exploitable tactics. Instant worldwide communications through the internet utilizing the tools that social media provide has changed the information environment. While just a tool, the latent for both good and bad present undeniable potential and will have to be a constant consideration for warfighters**.** As the speed of news cycles increase, users will be injected with headlines meant to incise clicks and fund advertisement campaigns. Education and cyber security investment will ensure this new information environment builds more than it destroys. Warfare will continue to be shaped by people with agendas, and social media accounts but vulnerabilities can be overcome. Education and experience will be the keys to a successful future in this fast-paced digital environment.

Education in the sense of teaching an individual to think critically and use scientific reasoning to discern truth for themselves before re-blogging, retweeting or sharing.

Notes

[1] Ovidiu Vermesan and Peter Friess, "*Internet of Things: Global Technological and Societal Trends*" (Aalborg, Denmark: River Publishers, 2011), 1-9. http://site.ebrary.com/id/10852717. accessed December 19, 2016.
[2] Internet World Stats, "Usage and Population Statistics," June 30, 2016. http://www.internetworldstats.com/stats.htm, accessed December 19, 2016.
[3] Shima D. Keene, "Terrorism and the Internet: A Double-edged Sword," *Journal of Money Laundering Control,* Vol. 14, No. 4 (2011): 359-362.
[4] "Company Info," Facebook Newsroom, last modified February 11, 2016. http://newsroom.fb.com/company-info/, accessed December 20, 2016.
[5] Home - Multinational Experiment (Public Site), (2014), https://wss.apan.org/s/MEpub/default.aspx.
[6] US Department of Defense, *Department of Defense: Cyber Strategy* (Washington, DC: April 2015),1-3. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, accessed December 20, 2016.
[7] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), Chapter 1.
[8] "Company Info," Facebook Newsroom, last modified February 11, 2016, http://newsroom.fb.com/company-info/.
[9] Tetyana Bohdanova, "Unexpected Revolution: The Role of Social Media in Ukraine's Euromaidan Uprising," *European View* 13 (1): 133-142. 2014.
[10] *Ibid*, 2.
[11] Megan Metzger,Pablo Barbera, and Penfold-Brown. *SMaPP Lab Data Report: Ukraine Protests 2013-2014.* Social Media and Political Participation Lab, NY University. February 28, 2014.
[12] *Ibid*, 4.
[13] Megan Metzger,Pablo Barbera, and Penfold-Brown. *SMaPP Lab Data Report: Ukraine Protests 2013-2014.* Social Media and Political Participation Lab, NY University. February 28, 2014.
[14] Olga Onuch, "Social Networks and Social Media in Ukrainian Euromaidan Protest," *The Washington Post*. Monkey cage, January 2, 2014. https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/02/social-networks-and-social-media-in-ukrainian-euromaidan-protests-2/, accessed April 26, 2017.
[15] Megan Metzger,Pablo Barbera, and Penfold-Brown. *SMaPP Lab Data Report: Ukraine Protests 2013-2014.* Social Media and Political Participation Lab, NY University. February 28th 2014.
[16] CBS WIRE SERVICES. "Top U.S. Official Visits Protesters in Kiev as Obama Admin. Ups Pressure on Ukraine President Yanukovich," *CBS New,* last updated December 11, 2013, http://www.cbsnews.com/news/us-victoria-nuland-wades-into-ukraine-turmoil-over-yanukovich/, accessed January 3, 2017.
[17] EURONEWS, "The UN and Washington Condemn Violence in Ukraine," *EURONEWS.com,* Last updated March 12, 2013, http://www.euronews.com/2013/12/03/the-un-and-washington-condemn-violence-in-ukraine, accessed January 3, 2017.
[18] Catherine A. Theohary, "Information Warfare: The Role of Social Media in Conflict," *CRS Insights.* IN10240 (March 4, 2015), https://fas.org/sgp/crs/misc/IN10240.pdf, accessed January 3, 2017.
[19] *Ibid*, 5.
[20] Ellen Nakashima. "Iran aids Syrian in tracking opposition via electronic surveillance, US officials say," *The Washington Post*, National Security October 9, 2012. https://www.washingtonpost.com/world/national-security/iran-aids-syria-in-tracking-opposition-via-electronic-surveillance-us-officials-say/2012/10/09/410a3cae-1224-11e2-a16b-2c110031514a_story.html?utm_term=.1686750e0055, accessed April 26, 2017.
[21] Riham Alkousaa, "How Facebook Hurt the Syrian Revolution," *Aljazeera.* Syria's Civil War December 4, 2016. http://www.aljazeera.com/indepth/opinion/2016/12/facebook-hurt-syrian-revolution-161203125951577.html, accessed April 26, 2017.
[22] Patrick O'neill. "*Why the Syrian Uprising is the First Social Media War*," The Daily Dot, September 18, 2013. http://www.dailydot.com/layer8/syria-civil-social-media-war-youtube/, accessed April 26, 2017.
[23] Joby Warrick. "*Private money pours into Syrian conflict as rich donors pick sides,"* The Washington Post. National Security, June 15, 2013. https://www.washingtonpost.com/world/national-security/private-money-pours-into-syrian-conflict-as-rich-donors-pick-sides/2013/06/15/67841656-cf8a-11e2-8845-d970ccb04497_story.html?utm_term=.b630bc6b2966, accessed April 26, 2017.
[24] Emerson T. Brooking, and P. W. Singer. *War Goes Viral*, The Atlantic, November 2016 issue 501125
[25] *Ibid*, 2.

[26] Johnnie Moore, "ISIS ON THE RECRUITMENT TRAIL," *USA Today*, 07, 22-23. 2015. https://search-proquest-com.lomc.idm.oclc.org/docview/1698197044?accountid=14746, accessed April 26, 2017.
[27] *Ibid*, *22*.
[28] John Arquilla, and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, US: RAND Corporation. 2001.
[29] 2015. "Terrorism and Social Media," *Congressional Digest. 94*, no. 4: 9. Academic Search Elite, EBSCOhost (accessed January 21, 2017).
[30] H. A. Eiselt, & J. Bhadury, "The Use of Structures in Communication Networks to Track Membership in Terrorist Groups." *Journal of Terrorism Research,* 2015. http://jtr.st-andrews.ac.uk/articles/10.15664/jtr.1073/#, accessed April 26, 2017.
[31] Sean Gallagher. "Who's winning the cyber war? The squirrels, of course," *ARS technical.* January 16, 2017. https://arstechnica.com/information-technology/2017/01/whos-winning-the-cyber-war-the-squirrels-of-course/, accessed April 26, 2017.
[32] Ramon Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict & Terrorism,* Vol 33, No. 9 2010 http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/1057610X.2010.501426?scroll=top&needAccess=true, accessed April 26, 2017.
[33] Joel A. Capellan. "Lone Wolf Terrorist or Deranged Shooter? A Study of Ideological Active Shooter Events in the United States, 1970–2014" *Studies in Conflict & Terrorism,* Vol 38, No. 6 2015
[34] *Ibid*, 395.
[35] Tracy Thomas. *ISIS has mastered social media, recruiting 'lone wolf' terrorists to target Times Square: Bratton,* New York Daily News, September 17 2014. http://www.nydailynews.com/new-york/isis-recruiting-lone-wolf-terrorists-target-times-square-bratton-article-1.1941687, accessed April 26, 2017.
[36] *Ibid*, 2
[37] *Ibid*, 1
[38] George Michael, "Counterinsurgency and Lone Wolf Terrorism," *Terrorism and Political Violence,* Vol 26, No. 1 2014. http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/09546553.2014.849912?src=recsys, accessed April 26, 2017.
[39] Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf, accessed April 26, 2017.
[40] George Michael, "Counterinsurgency and Lone Wolf Terrorism," *Terrorism and Political Violence,* Vol 26, No. 1 2014. http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/09546553.2014.849912?src=recsys
[41] Ramon Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict & Terrorism,* Vol 33, No. 9 2010 http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/1057610X.2010.501426?scroll=top&needAccess=true, accessed April 26, 2017.
[42] George Michael. "Counterinsurgency and Lone Wolf Terrorism," *Terrorism and Political Violence,* Vol 26, No. 1 2014. http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/09546553.2014.849912?src=recsys, accessed April 26, 2017.
[43] Harvey W. Kushner and Sage Publications. *Encyclopedia of Terrorism*. Thousand Oaks, Calif.: Sage Publications. 2003. http://site.ebrary.com/id/10367421, accessed April 26, 2017.
[44] Cade Metz. "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," *WIRED* April 5th 2016. https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/, accessed April 26, 2017.
[45] *Ibid*, *3.*
[46] Shima D. Keene. "Terrorism and the Internet: A Double-Edged Sword," *Journal of Money Laundering Control* Vol 14 No. 4, 2011: pp. 359-370, accessed April 26, 2017.
[47] John Arquilla and David Ronfeldt. *Networks and Netwars : The Future of Terror, Crime, and Militancy*. Santa Monica, US: RAND Corporation. 2001.
[48] Shima D. Keene. "Terrorism and the Internet: A Double-Edged Sword," *Journal of Money Laundering Control* Vol 14 No. 4, 2011. accessed April 26, 2017.
[49] Mark Hosenball. "Islamic Cyberterror," *Newsweek.* May 19, 2002. http://www.newsweek.com/islamic-cyberterror-145381, accessed April 26, 2017.
[50] B. Gellman. "FBI Fears Al-Qaeda Cyber-Attacks," *The Washington Post*, June 28, 2002. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html

[51] Shima D. Keene. “Terrorism and the Internet: A Double-Edged Sword,” *Journal of Money Laundering Control* Vol 14 No. 4, 2011.
[52] "The World Factbook," Central Intelligence Agency, accessed March 23, 2017, https://www.cia.gov/library/publications/resources/the-world-factbook/docs/notesanddefs.html, accessed April 26, 2017.
[53] Josh Constine. “ISIS “Cyber Caliphate” Hacks U.S. Military Command Accounts,” *Tech Crunch.* January 12, 2015. https://techcrunch.com/2015/01/12/cyber-caliphate/ accessed April 26, 2017.
[54] *Ibid*, 2.
[55] Gabriel Weimann. “Cyberterrorism: The Sum of All Fears?,” *Studies in Conflict & Terrorism,* Vol 28, No. 2 2005. http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/10576100590905110, accessed April 26, 2017.
[56] *Ibid*, 4.
[57] *Ibid*, 4.
[58] *Ibid*, 3.
[59] Charles Warner. "Fake News: Facebook Is a Technology Company," *Forbes*, last modified November 17, 2016, http://www.forbes.com/sites/charleswarner/2016/11/27/fake-news-facebook-is-a-technology-company/#d33c8588e1d3, accessed April 26, 2017.
[60] *Ibid*, 2.
[61] Neil Postman. *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*. New York: Viking 1985.
[62] Reuters Institute for The Study of Journalism. *Reuters Institute Digital News Report 2016*, University of OXFORD, 1-25. 2016.
[63] *Ibid*, 23.
[64] *Ibid*, 24.
[65] *Ibid*, 24.
[66] Nic Newman. “Overview and Key Findings of the 2016 Report,” Reuters Institute for the Study of Journalism. Digital News Report 2016. http://www.digitalnewsreport.org/survey/2016/overview-key-findings-2016/, accessed April 26, 2017.
[67] *Ibid*, 24.
[68] Mike Hanley and Andrea Stroppa. *“How can we defeat fake news?,” World Economic Forum,* February 8, 2017. https://www.weforum.org/agenda/2017/02/how-can-we-defeat-fake-news-automate-the-right-to-reply/, accessed April 26, 2017.
[69] *Emerging Threats and Capabilities. Hearing before the House Armed Service Subcommittee*, 117th Cong., 7 (2015) (statement of General Joseph L. Votel, U.S. Army, Commander, United States Special Operations Command).
[70] Cori E Dauber. "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations." Military Review 89, 2009.
[71] *Ibid*, 14.
[72] *Ibid*, 14.
[73] *Ibid*, 15.
[74] *Ibid*, 15.
[75] *Ibid*, 15.
[76] *Ibid*, 19.
[77] Shima D. Keene. “Terrorism and the Internet: a Double-edged Sword,” *Journal of Money Laundering Control*, Vol. 14, No. 4, 2011, Pg. 360.
[78] Internet World Stats, “Usage and Population Statistics,” June 30, 2016, http://www.internetworldstats.com/stats.htm, accessed February 17 2017, accessed April 26, 2017.

Bibliography

Active Shooter, How to Respond. Department of Homeland Security, 2008. https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf.

Alkousaa, Riham. "How Facebook hurt the Syrian Revolution." *Aljazeera*. Opinion:Syria's Civil War December 4, 2016). http://www.aljazeera.com/indepth/opinion/2016/12/facebook-hurt-syrian-revolution-161203125951577.html.

Arquilla, John, and Ronfeldt, David. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA, RAND Corporation. 2001.

Bohdanova, Tetyana. *Unexpected Revolution: The Role of Social Media in Ukraine's Euromaidan Uprising.* European View, 13 (1) (2014): 133-142.

Brooking, Emerson T. and Singer, P. W. "War Goes Viral." *The Atlantic*. November 2016. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

Capellan, Joel A. "Lone Wolf Terrorist or Deranged Shooter? A Study of Ideological Active Shooter Events in the United States, 1970–2014." *Studies in Conflict & Terrorism*, Vol. 38, No. 6 (2015) 395-413.

CBS WIRE SERVICES. "Top U.S. official visits protesters in Kiev as Obama admin. Ups pressure on Ukraine president Yanukovich," *CBS New*, (last updated December 11, 2013), http://www.cbsnews.com/news/us-victoria-nuland-wades-into-ukraine-turmoil-over-yanukovich/.

Clausewitz, Carl von. *On War*, edited by Michael Howard and Peter Paret, translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984. http://site.ebrary.com/id/10022123.

Constine, Josh. "ISIS "Cyber Caliphate," Hacks U.S. Military Command Accounts" *Tech Crunch.* (January 12, 2015). https://techcrunch.com/2015/01/12/cyber-caliphate/.

Dauber, Cori E. "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations." *Military Review,* 89, 1, (2009):13-24.

Eiselt, H. A., & Bhadury, J. "The Use of Structures in Communication Networks to Track Membership in Terrorist Groups," *Journal of Terrorism Research.* (2015). http://jtr.st-andrews.ac.uk/articles/10.15664/jtr.1073/#.

EURONEWS. "The UN and Washington condemn violence in Ukraine," *EURONEWS.com*, (Last updated March 12 2013), http://www.euronews.com/2013/12/03/the-un-and-washington-condemn-violence-in-ukraine.

Gellman, B. “FBI fears al-Qaeda cyber-attacks,” *The Washington Post*. (June 28, 2002): 1-10. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

Hanley, Mike and Stroppa, Andrea. “How can we defeat fake news?,” *World Economic Forum*. (February 8, 2017). https://www.weforum.org/agenda/2017/02/how-can-we-defeat-fake-news-automate-the-right-to-reply/.

Hosenball, Mark. “Islamic cyberterror,” *Newsweek*. (May 19 2002). http://www.newsweek.com/islamic-cyberterror-145381.

Keene, Shima D., “Terrorism and the Internet: a Double-Edged Sword,” *Journal of Money Laundering Control*, Vol. 14, No. 4 (2011): 359-370.

Kushner, Harvey W. “Encyclopedia of Terrorism.” *Thousand Oaks*, Sage Publications. (2003). http://site.ebrary.com/id/10367421.

Metz, Cade, “Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People,” *WIRED*, April 5, 2016. https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/. Accessed April 26, 2017.

Metzger, Megan, Barbera, and Penfold-Brown, *SMaPP Lab Data Report: Ukraine Protests 2013-2014.* Social Media and Political Participation Lab, NY University. February 28, 2014.

Michael, George. “Counterinsurgency and Lone Wolf Terrorism,” *Terrorism and Political Violence*, Vol 26, No. 1 2014. http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/09546553.2014.849912?src=recsys.

Moore, Johnnie. "ISIS on the Recruitment Trail," *USA Today*, 07, (2015):22-23. https://search-proquest-com.lomc.idm.oclc.org/docview/1698197044?accountid=14746.

Multinational Capability Development Campaign (MCDC) *Concept of Employment Social Media in Support of Situation Awareness*, (2014). https://wss.apan.org/s/MEpub/default.aspx.

Nakashima, Ellen. “Iran aids Syrian in tracking opposition via electronic surveillance, US officials say,” *The Washington Post*. National Security (October 9, 2012). https://www.washingtonpost.com/world/national-security/iran-aids-syria-in-tracking-opposition-via-electronic-surveillance-us-officials-say/2012/10/09/410a3cae-1224-11e2-a16b-2c110031514a_story.html?utm_term=.1686750e0055/ Accessed April 26, 2017.

Newman, Nic. “Overview and Key Findings of the 2016 Report,” *Reuters Institute for the Study of Journalism*. Digital News Report, (2016). http://www.digitalnewsreport.org/survey/2016/overview-key-findings-2016/.

O'neill, Patrick. "Why the Syrian uprising is the first social media war," *The Daily Dot*. (September 18, 2013). http://www.dailydot.com/layer8/syria-civil-social-media-war-youtube/.

Onuch, olga, "Social Networks and Social Media in Ukrainian Euromaidan Protest," *The Washington Post*. Monkey cage, (January 2, 2014) https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/02/social-networks-and-social-media-in-ukrainian-euromaidan-protests-2./

Orrick, Sarah. "Terrorism and Social Media," *Congressional Digest*, 94, no. 4, (2015). Academic Search Elite, http://congressionaldigest.com/terrorism-and-social-media/#gsc.tab=0.

Postman, Neil, Riggenbach, and Jeff. *Amusing Ourselves to Death Public Discourse in the Age of Show Business*. Blackstone Audio Inc, 2013.

Reuters Institute for The Study of Journalism. *Reuters Institute Digital News Report 2016*, University of OXFORD, 2016. http://www.digitalnewsreport.org/survey/2016/overview-key-findings-2016/.

Spaaij, Ramon. "The Enigma of Lone Wolf Terrorism: An Assessment*," Studies in Conflict & Terrorism*. Vol 33, No. 9 (2010). http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/1057610X.2010.501426?scroll=top&needAccess=true.

Theohary, Catherine A. "Information Warfare: The Role of Social Media in Conflict," *CRS Insights IN10240.* (March 4, 2015), https://fas.org/sgp/crs/misc/IN10240.pdf.

Tracy, Thomas. "ISIS has mastered social media, recruiting 'lone wolf' terrorists to target Times Square: Bratton," *New York Daily News*. (September 17 2014). http://www.nydailynews.com/new-york/isis-recruiting-lone-wolf-terrorists-target-times-square-bratton-article-1.1941687.

U.S. Congress, Senate. House Armed Service Subcommittee. *Emerging Threats and Capabilities. Hearing before the House Armed Service Subcommittee*, 117th Cong., 18 March 2015.

US Department of Defense. *Department of Defense: Cyber Strategy*. Washington, DC April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Vermesan, Ovidiu, and Peter Friess. *Internet of Things: Global Technological and Societal Trends*. River Publishers series in communications. Aalborg, Denmark: River Publishers, 2011. http://site.ebrary.com/id/10852717.

Warner, Charles. *Fake News: Facebook Is A Technology Company. Forbes*, (November 27,

2016). http://www.forbes.com/sites/charleswarner/2016/11/27/fake-news-facebook-is-a-technology-company/#d33c8588e1d3

Warrick, Joby. “Private money pours into Syrian conflict as rich donors pick sides,” *The Washington Post*, National Security, (June 15 2013). https://www.washingtonpost.com/world/national-security/private-money-pours-into-syrian-conflict-as-rich-donors-pick-sides/2013/06/15/67841656-cf8a-11e2-8845-d970ccb04497_story.html?utm_term=.b630bc6b2966.

Weimann, Gabriel, “Cyberterrorism: The Sum of All Fears?,” *Studies in Conflict & Terrorism*, Vol 28, No. 2 (2005). http://www-tandfonline-com.lomc.idm.oclc.org/doi/full/10.1080/10576100590905110.

"World Internet Users Statistics and 2017 World Population Stats," *Internet World Stats - Usage and Population Statistics*. (March 23, 2017). http://www.internetworldstats.com/stats.htm.