AIR COMMAND AND STAFF COLLEGE

DISTANCE LEARNING

AIR UNIVERSITY

UTILIZING SOCIAL MEDIA AND PROTECTING MILITARY MEMBERS AND THEIR FAMILIES

by

Jennifer M. Piggott, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Proposal Advisor: Dr. Stephen Harris

Project Advisor: Dr. Andrew Niesiobedzki

Maxwell AFB, AL

February 2016

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Table of Contents

List of Figures

Preface

I am grateful for the assistance on this project from my two advisors. First, my research advisor, Dr. Stephen Harris, who helped ensure my research proposal was moving in the right direction, and secondly, my project advisor, Dr. Andrew Niesiobedzki, who was instrumental in helping me build this paper. He asked the hard questions, making sure my paper turned into a logical, flowing research paper. Both of their contributions greatly contributed towards this paper and my overall writing and research experience.

I would also like to thank a few of my Public Affairs career field peers, specifically Lt. Col. (retired) Susan Romano, Maj. Brooke Brander, and Maj. Stacie Shafran, who allowed me to talk through the original idea of this paper in the early days, helping frame my research question and overall objectives of my research.

Most importantly, I would like to thank my husband, and my daughter. Your patience over the past two years it has taken to complete the ACSC program has been phenomenal. Thank you for always being there to help out, listen as I tried to figure out a concept or idea, and provide your operational fighter pilot wisdom. This greatly expanded my strategic thinking and overall experience throughout this program. We are quite the team! I'm so glad I no longer have to miss out on the weekend family fun. Now, let's go on a vacation to celebrate before we welcome our second child in June!

Abstract

Social media is rewriting the rules of modern warfare, making it more difficult to analyze and predict our enemies and control the information that is in the public domain. It is essential to ensure the safety of military members and their families when using social media, all while continuing to tell the U.S. Air Force (Air Force) story. The purpose of this study is to evaluate if social media, specifically Facebook, poses a threat to military members and their families. A subset of this study is to evaluate if the education provided by Public Affairs is adequate to protect military members and their families in an ever-evolving technological society.

Terrorist groups depend on open media systems, such as social media, to further their message, actively recruit, and promote propaganda. A 2012 study showed that approximately 90 percent of organized terrorism on the Internet use social media to carry out their threat or cause. As of 2014, Islamic State of Iraq and Syria (ISIS) supporters used at least 46,000 accounts on Twitter. ISIS released more than 100 service members' names through social media in March 2015, and charged its members to kill those service members whose names, photos, and addresses were posted online. The threat is significant and growing at a rapid pace.

Continuing the status quo does not decrease the threat of social media to military members and their families. The Air Force must incorporate a multi-tiered approach to reduce the threat social media poses to military members and their families. This includes establishing a course at the Defense Information School (DINFOS) that focuses on social media and the associated threats of this growing communication; creating a risk communication strategy or case study; and updating policy and guidance in a timely manner to reflect the growing threat and the pace in which social media is emerging.

"It is the policy of the Department of Defense to make available timely information and accurate information so that the public, Congress and the news media may assess and understand the facts about national security and defense strategy."

Donald H. Rumsfeld, Secretary of Defense, 2001[1]

INTRODUCTION

Overview of the Study

Social media is a great avenue for staying connected with family and friends; it is also a great tool for sharing the Air Force story and the stories of its Airmen. Social media is rewriting the rules of modern warfare, making it more difficult to analyze and predict U.S. enemies' behavior and control the information that is in the public domain. How to utilize social media effectively will continue to be a hot topic for the Air Force and the Department of Defense (DoD) for years to come. As social media evolves, Air Force Public Affairs will continue to search for an appropriate balance between maintaining a credible line of communication with the American people and the requirements of force protection, security, and protecting military members and their families. This balance becomes increasingly difficult given today's connected world, specifically in protecting personal information targeted on Facebook, while ensuring public transparency in telling the Air Force story.

The Nature of the Problem

The Past

Society is living in an era of unprecedented global power, where technology is ever advancing and humanity is hard-pressed to keep up. Nearly 250 years ago, none of these technological advances existed, but mass dissemination of information to inform and influence people dates back to the 1700's, where in 1776, Thomas Paine published the pamphlet "Common

Sense." This 47-page pamphlet sold some 500,000 copies and had a powerful influence on American opinion.[2] Although rarely used today, pamphlets were an important medium for the spread of ideas in the 16th through 19th centuries; they were the Facebook posts or Twitter feeds of their time.

The Present – A Growing Influence

In 2010, Laura Fitzpatrick said in an article in Time Magazine, "today, more video is uploaded to YouTube in 60 days than all three U.S. television networks have created in 60 years."[3] Social media platforms continue to flourish at an astonishing and unprecedented rate. Today, 65 percent of adults use social networking sites – a nearly tenfold jump in the past decade and social media is a leading mechanism to receive information, disseminate information, and form public opinion.[4] Figure 1 below highlights the social networking growth seen in the U.S. in the past decade and shows that as of 2014, nearly 20 percent of the world's population logs into Facebook once a month.[5]

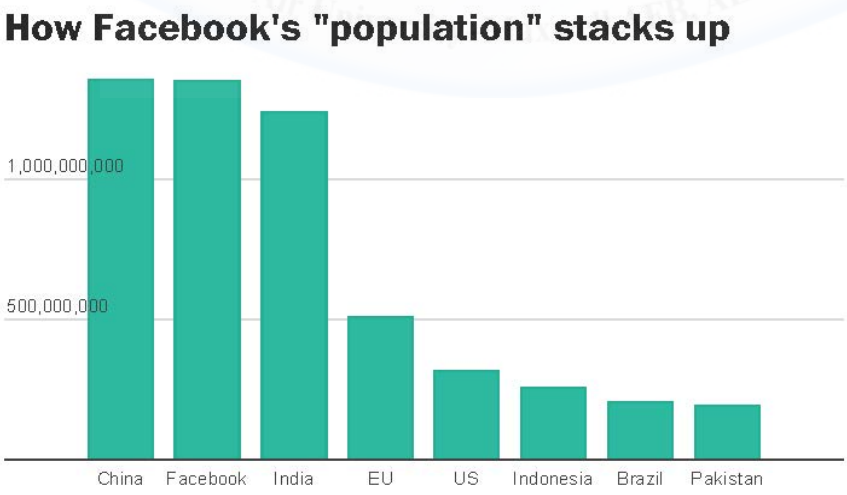

Figure 1 Worldwide Percentage of People Using Facebook (2014).[6]

According to Facebook, it had 12 million active users in 2006, 500 million active users in 2010, and 1.65 billion active users in 2014.[7] The DoD authorized military members to use social media, including Facebook, in 2010, as long as their activity did not compromise operational security or involve prohibited activities or websites.[8] Although a comprehensive study has not been conducted showing how many Airmen use Facebook, in 2010 studies indicated that 50 percent of military members were on Facebook. The average number of daily social media users is growing worldwide. With the ease of a button, social media serves as a way to communicate internally with Airmen, and also as a means of telling the story of military members to external audiences who themselves are actively engaged in social networks.[9] If Facebook were a country, its population would rival the single most populous country on Earth. Almost as many people use Facebook as live in the entire country of China.[10] Social media is here to stay. It is essential to ensure the safety of military members and their families when using social media, all while continuing to tell the Air Force story.

The Future – Emerging Technology

With the emergence of social media, information sharing continues to be dynamic and evolving. Social media is a global cultural phenomenon, and for many Americans it has become such a part of their daily activities, they cannot imagine living without this form of social interaction and communication. One out of every six minutes spent online is on a social network, and 73 percent of the U.S. Internet population visits Facebook each month.[11] Figure 2 shows the growing trend from 2006 to 2014 of American adults who use the Internet and at least one social networking platform. Millennials, who are ages 18 to 34 and the largest generation in the U.S. (approximately 75.3 million people), use social media. Sixty-one percent of millennials use social media to get the majority of their news from sites such as Facebook.[12]

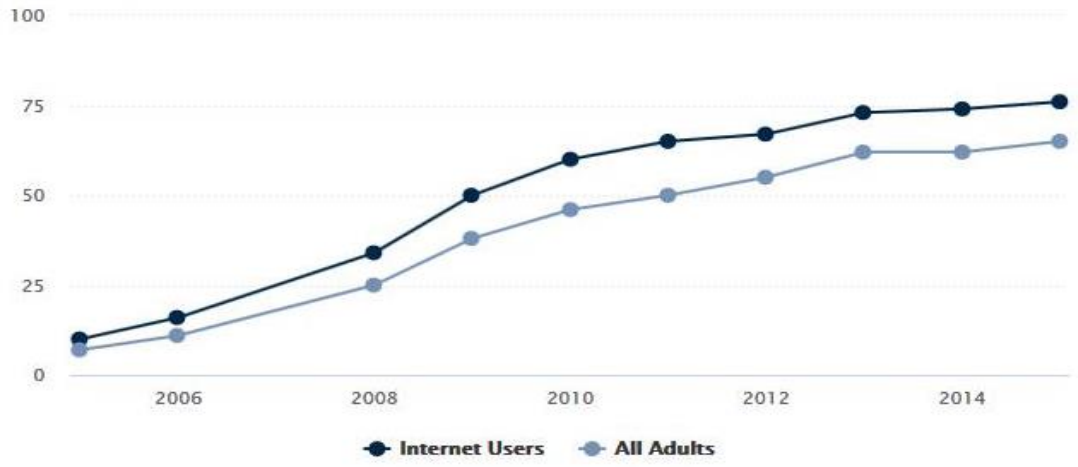

Figure 2 Percentage of U.S. Adults Using Social Media (2006 – 2014).[13]

There is individual risk associated with military members and their families using social media, specifically Facebook, but there is also global risk to the Air Force's ability to drive the message by not using it. In 2015, Pentagon Press Secretary Rear Admiral John Kirby said in response to a question about the risks of using social media, "to ignore it, to shut it down simply because someone with ill intent might exploit it would be to risk losing our share of an important conversation out there on national security issues." Education is paramount, and although Air Force Public Affairs educates social media users now, this research will explore if the current education and training is enough to protect military members and their families. This education and training is multi-tiered. One, is the education and training provided to Air Force Public Affairs professionals sufficient, and two is the training properly communicated to military members and their families? Social media is a critical piece in telling the Air Force Story. In 2014, during a graduation speech to the U.S. Military Academy, President Barack Obama said, "when we cannot explain our efforts clearly and publicly, we face terrorist propaganda and international suspicion, we erode our legitimacy with our partners and our people, and we reduce accountability in our own government."[14] Communication is essential and Air Force Public

Affairs professionals must be trained on how to safely convey the message, particularly when using social media. Figure 3 below shows the number of registered Air Force social media accounts as of January 27, 2016.

Figure 3 Number of Air Force Social Media Accounts (2016).[15]

Purpose of the Study

The purpose of this study is to evaluate if social media, specifically Facebook, poses a threat to military members and their families. A subset of this study is to evaluate if the education provided by Air Force Public Affairs is adequate to protect military members and their families in an ever-evolving technological society. The problem is not whether the Air Force will continue to use social media; rather, it is how it will use social media. Discontinuing the use of social media is not a solution to the issue or potential associated threat. Social media is a critical tool for the Air Force to keep up with mainstream media and it is an efficient means of communications for senior leaders. Social media has changed the conversation. Leaders not only support the use of social media, but readily use it in their daily interactions. "I've watched social media's role in exposing the military experience to the citizens we defend, ranging from humor to debate. I'm impressed with how our nation's understanding of the military has changed especially since 2001," said General Martin Dempsey, Chairman of the Joint Chiefs of Staff during a Facebook town hall in December 2013.[16] Secretary of the Air Force, Deborah Lee James, is constantly interacting with Airmen, both in-person and virtually, because it is an essential part of her decision-making process.[17] James has been innovative in her approach

using social media to communicate effectively with Airmen. As of January 2015, James has 3,805 followers on Twitter and 35,396 people who have liked her Facebook page, with 5,045 people actively talking about her Facebook posts.

While individuals can choose to disconnect, social media will continue to be a necessary means of communications for Air Force Public Affairs and Air Force leaders to tell the Air Force story. However, there is inherent risk in using social media and making personal information readily available in the media. This risk increases as social media technology continues to evolve. For instance, when MySpace began, it was a basic social network. Now social networking sites such as Facebook have the ability to locate individuals, geotag, and provide real-time data, increasing the potential security risks associated with social media. Enemies can now see where Airmen are and what Airmen are doing in real-time.

This study will also explore the best methods and practices for Air Force Public Affairs personnel to follow, to more safely use social media, to better protect and educate military members and their families, while continuing to engage the American people.

Research Question

Social media is rewriting the rules of modern warfare, making it more difficult to analyze and predict adversaries and control the information that is in the public domain. A critical factor involving social media and the military is security. The proliferation of social software has ramifications for U.S. national security, spanning future operating challenges of a traditional, irregular, catastrophic, or disruptive nature.[18] Failure to adopt social media as a tool may reduce an organization's relative capabilities over time. Globally, businesses, individuals, activists, criminals, and terrorists are using social software effectively. Governments that harness their potential power can interact better with citizens and anticipate emerging issues.[19] "Social media

allows for agility because of the vehicle itself, which allows for risks and capabilities," said Pentagon Press Secretary Rear Admiral John Kirby, during a Pentagon Press Briefing in 2015.[20] It is from this perspective that this paper will examine the relationship between social media and the security of military members and their families. In order for the U.S. military to maintain public trust and support of the American taxpayer, its public interface must remain relevant and continue to provide open lines of communication. Therefore, the research question for this study is: Is the training and education by Air Force Public Affairs sufficient to safeguard against the threat of social media?

Definition of Terms

Geotagging. Geotagging adds geographical identification data to photos, videos, websites, and text messages through location based applications. This technology helps people find images and information based on a location from a mobile device or desktop computer.[21]

Public Affairs. Public Affairs are communication capabilities and activities with external and internal audiences.[22]

Social media. Tools and platforms people use to publish, converse, and share content online. These social media tools include social networking sites, blogs (weblogs), wikis, podcasts, and sites to share photos and bookmarks.[23]

Social networking. Social networking promotes social interaction among users through posts, commentaries, links, photos, and videos (e.g., Facebook, Twitter, Google+).[24]

Twitter handle. A Twitter handle is the Twitter name. The handle (or username) is the name that you respond to when tweeting someone and people identify you. A handle is always proceeded immediately by the "@" symbol.[25]

The Anticipated Significance of the Study

The populations that will be best served by this study are senior decision makers, particularly those in Air Force Public Affairs, advising the Secretary of the Air Force on Public Affairs policies and procedures and the potential needs for increased education and training. This will in turn serve Airmen and their families, helping to educate and inform them on best social media practices, safeguarding them from potential threats associated with social media. In 2014, a military advocacy group performed a study that found 75 percent of 6,200 respondents considered social media very important, and Pew Research shows that military families appear to use social media at a higher rate than civilians.

Social media is rewriting the rules of modern warfare, making it more challenging to analyze and predict U.S. enemies' behavior, and to control the information in the public domain. This study will help senior decision makers determine how to balance protecting military members and their families in a connected world, specifically personal information targeted on Facebook, while helping ensure public transparency in telling the Air Force story.

Research Methodology

An evaluation methodology is used in this study to objectively assess how the Air Force can employ social media and protect their members and families by using a mixed method of quantitative and qualitative data. This unique issue will ultimately have many possible solutions. The evaluation framework will allow for an in depth analysis, several possible solutions, and recommended approaches for the Air Force to best utilize social media. The study will start by highlighting the background of social media in the Air Force and provide an evolution of the use of this interface. It will also give historical examples of organizations (such as ISIS) that have used social media against the Air Force and its members.

The study will then evaluate the effectiveness of social media against the security risks currently facing Air Force members and their families resulting from their social media use. Based upon the analysis of the evaluation, this paper will provide recommendations on how to use social media while protecting Air Force members and their families.

LITERATURE REVIEW

History of Air Force Use of Social Media

In February 2010, the DoD released a social media memorandum, granting all unclassified computers access to Facebook, YouTube, MySpace, and other social networking sites. "This directive recognizes the importance of balancing appropriate security measures while maximizing the capabilities afforded by 21st Century Internet tools," said Deputy Secretary of Defense William J. Lynn III (in office from 2009 to 2011). This was the first step in embracing technology and the use of collaborative, communication platforms to engage Airmen and the American public. This memorandum suggested a deeper level of trust in telling the military story than was provided to embedded reporters in Operation IRAQI FREEDOM in 2003. This trust expanded to external publics and stakeholders by encouraging openness and transparency, and it also reached a new level of trust in the men and women serving in the military. Plato once said, "those who tell the stories rule society."[26] Stories are packed with something even more powerful than hard data: emotional data. Since 2010, the Air Force's use of social media has continued to grow, allowing a new way to tell the Air Force story, and now holding a prominent place in both the Public Affairs career field and the communication toolbox of senior military leaders.

Social Media Policy

Policies governing social media use have evolved over the years, and in 2013 the Air Force published its fourth edition of its Social Media Guide. This guide serves as an aid to help Airmen share information effectively, while following Air Force instructions and protecting operational security (OPSEC). Unfortunately, very little has been published since 2013, causing the Air Force to fall behind the quickly evolving technology, increasing the risks that come with it. Because of the slow evolution of Air Force Public Affairs guidance regarding social media, the Air Force has not maximized the capabilities of its use and has lagged behind the social media explosion in mainstream media. A goal of social media is to provide an efficient avenue for Airmen to tell the Air Force story, and to allow for a cost-effective and efficient way for senior leaders to communicate with Airmen across the globe. This evolution is part of the paradigm shift taking place with communications becoming a two-way street instead of just a message pushing process. In order for the Air Force to effectively use social media and maximize this evolution, it must have up-to-date policies and guidance.

The 2013 Air Force Social Media Guide includes tips for leaders, Airmen, and families using social media, emerging trends, common platforms, and frequently asked questions.[27] Additionally, the sheer volume of social media users in the military and operational concerns surrounding social media has allowed it to become more than just a Public Affairs policy. The annual OPSEC training that all Airmen are required to accomplish has a social media component, as do many elements of the Intelligence Community.

Security and Social Media

Security concerns associated with social media have gained momentum in recent years. According to the U.S. Department of Justice and Federal Bureau of Investigation (FBI), Internet-

based social networking sites have created a revolution in social connectivity. However, con-artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes. Humans are a weak link in cyber security, and hackers and social manipulators know this.[28] One of the greatest risks in using social media is that once information is published, there is no way to remove it from the Internet, it is permanent. Specifically, once information is posted to a social networking site, it is no longer private and the more information posted, the more vulnerable users become. Although studies have shown that specific attacks have not come by way of social networking sites, information gleaned from social networking sites may be used to design specific attacks. Social media has an enormous influence over political and activists' movements, media literacy, and privacy, which can add to the security issues surrounding social media and military members.

In 2012, countries such as the U.S., Canada, and the United Kingdom instructed their military personnel to remove personal information from Facebook in case al-Qaeda was monitoring it.[29] In late November 2015, the FBI issued a warning to U.S. military members because ISIS was calling for attacks against U.S. military members. The warning asked members to review their online social media presence for any information that might attract the attention of violent extremists.[30] Brian Jenkins, senior advisor from the RAND Corporation, agreed with the dominance of al-Qaeda on the web. While almost all terrorist organizations have websites, al-Qaeda is the first group to fully exploit the Internet. This reflects al-Qaeda's unique characteristics. Al-Qaeda regards itself as a global movement and therefore depends on a global communications network to reach its perceived constituents.[31]

THE THREAT OF SOCIAL MEDIA

When considering the research question: "Is the training and education by Air Force Public Affairs sufficient to safeguard against the threat of social media?" The Air Force must pay attention to this growing "threat" through the emerging technology that has gone global. Due to the convenience, affordability, and broad reach of social media platforms such as Facebook, more people are using social media than ever before. American citizens, military and government organizations, and terrorist groups have increasingly used social media to further their goals and spread their message. Terrorist groups depend on open media systems, such as social media, to further their message, actively recruit, and promote propaganda, especially to Westerners. A 2012 study showed that approximately 90 percent of organized terrorism on the Internet is using social media to carry out their threat or cause. As of 2014, ISIS supporters used at least 46,000 accounts on Twitter.[32]

A Brief History

Terrorist groups have long used social media, but many associate the start with Osama Bin Laden. A notable example was with the release of his audio and video recordings, which were sent directly to mainstream Arabic television networks, including Al-Jazeera. These tapes began back in 2007 and continued regularly until 2011. In 2001, Bin Laden released a tape stating, "terrorism against America deserves to be praised because it is a response to injustice, aimed at forcing America to stop its support for Israel, which kills our people." In the recording, Bin Laden describes attacks by the U.S. against Islamic people. He describes his message as a review of events following the 9/11 attacks, and in this statement, he neither admits nor denies responsibility for the 9/11 attacks.[33]

According to the Homeland Security Committee, al-Qaeda is the first terrorist group to fully exploit social media, with the number of websites devoted to the movement growing from a few to thousands in recent years.[34] ISIS uses the reach of social media to their advantage to release threatening videos of beheadings. As of 2015, there have been at least six recorded executions of westerners kidnapped and executed by ISIS. Posting the executions online gave ISIS the power to manipulate the message and cause havoc among viewing audiences. This is one of many examples of a terrorist group displaying something through social media with the hopes of invoking fear in Americans, especially military members and their families.

The Taliban has been active on Twitter since 2011 and has more than seven thousand followers. Although the Taliban account is currently suspended, it did tweet under the handle @alemarahweb frequently, sometimes nearly hourly. Since 2011, Somalia-based terror cell al-Shabab has been tweeting under the handle @HSMPress, an account that has tens of thousands of followers. Social media use by terrorist organizations is on the upswing and appears to be here to stay, with the continued hope of creating fear in the minds of Americans and attempting to target military members and their families.

Targeting Military Members and their Families

In June 2015, Michael Steinback, assistant director of the FBI's counterterrorism division, told the Homeland Security Committee, "the foreign terrorist now has direct access into the United States like never before." Using social media as well as encrypted online communications beyond the reach of law enforcement surveillance, terror organizations increasingly reach sympathizers and encourage attacks on western soil.[35] Since 2015, more than 3,500 westerners have traveled to join ISIS in its quest to establish an Islamist state in Iraq. The Department of Homeland Security is aware of over 100 U.S. citizens who have traveled to Syria

or sought to travel to Syria to join terrorist groups operating there, including ISIS.[36] Even though an estimate of the number of sympathizers on U.S. soil continues to be a difficult number to discern, it could be hundreds or it could be thousands; it only takes one to be sympathetic and assist with an attack on U.S. soil. "There are thousands of messages being put out into the ether sphere and they're just hoping that they land on an individual who's susceptible to that type of terrorist propaganda," said John Carlin, the assistant attorney general heading the Justice Department's national-security division.[37] In 2003, Defense Secretary Donald Rumsfeld observed that an al-Qaeda training manual recovered in Afghanistan said, "by using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[38] Social media is considered such an open public source, which can be specifically used to target military members.

The Internet provides terrorists with anonymity, command and control, and a host of other measures to coordinate and integrate attacks.[39] With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the U.S. They can spot, assess, recruit, and radicalize, either to travel to or conduct homeland attacks. According to the National Counterterrorism Center, of all the terrorist organizations using social media to promote their cause and increase fear, ISIS is by far the most sophisticated propaganda machine of any terrorist organization to date.[40] "Importantly, the group also views itself as the now-leader of a global jihadist movement," said Matthew Olsen, director of the National Counterterrorism Center (from 2011 to 2014). Additionally, Matthew Olsen said, "it turns out timely, high-quality media, and it uses social media to secure a widespread following."[41] ISIS is far more than an organization that merely uses social media. ISIS has a global communications

strategy that has stumped counterterrorism officials while continuing to make significant progress among U.S. sympathizers.

In 2015, the U.S. Central Command's Twitter and YouTube accounts were hacked for approximately 30 minutes. The Twitter announcement read: "American Soldiers, We are Coming, Watch Your Backs. ISIS." The Twitter announcement was also linked to a statement that said, "We won't stop! We know everything about you, your wives and children. U.S. soldiers! We're watching you!"[42] In February 2015, ISIS posted its horrific video that showed the burning of a captured Jordanian pilot, instilling fear throughout the military pilot community. Additionally, in March 2015 the ISIS Hacking Division released a "hit list" containing more than 100 current and former U.S. service members. The personal information on this list included names, addresses, and photographs.[43] The release also contained a message from ISIS, encouraging its "brothers residing in American to kill those named on this list." Defense officials stated that hackers likely pieced together the profiles from information ISIS found in public databases rather than government services, since many of the names on the "hit list" have previously appeared in media coverage of airstrikes against the militant group.[44]

Although DoD officials concluded these names were drawn from open sources, such as Google, military members and their families were again encouraged to be mindful of what they post on social media, especially showcasing military connections or service on social media, and were encouraged to change their names on social media (i.e. changing their Facebook name to an alias). The effort by ISIS was a clear attempt to intimidate and to dissuade military forces participating in the counter-ISIS campaign, and while unsettling, this type of invasive tactic was not unexpected and is likely to happen again in the future.

Social media continues to grow, and despite threats and increased concern, military members and their families, especially millennials, heavily use it. A 2014 Pew Research survey showed that 86 percent of those surveyed were willing to discuss politics or controversial topics in person but were not willing to do so online, which indicates a trend of fear of what is said in social media platforms as a result of the terrorist threat that continues against westerners.

ANALYSIS, CONCLUSIONS AND RECOMMENDATIONS

Analysis

This study explores three solutions to address the research question. The first proposed solution is to keep things as they currently are: status quo. The second proposed solution is to increase the training and education provided to Air Force Public Affairs professionals. The third proposed solution is to make a change to either DoD or Air Force Policy when it comes to the use of social media. When considering each proposed solution, the analysis consists of two simple criteria based on the background information provided thus far. Question one, could the solution decrease the threat of social media to military members and their families? Question two, could the solution aid in better protecting military members and their families in the future. If the answer is yes, then the solution could be an effective approach for Air Force leaders to consider. Each of the solutions could then warrant additional analysis and independent studies, to determine how to specifically implement the solution.

Proposed Solutions

The question at hand is if the training and education provided by Air Force Public Affairs is sufficient to safeguard against the threat of social media. Simply disconnecting from social media is not an option for the Department of Defense, the Air Force, or its members. This emerging technology has proven over the years that it is here to stay, and it is expected to

continue to grow in leaps and bounds. Social media has also proven to be a highly effective platform to tell the Air Force story and for senior leaders to communicate with Airmen. From the start of Wikipedia in 2001, LinkedIn in 2003, and Myspace in 2004, the world has seen social media evolve at an enormous rate. Social media reaches audiences around the world and connects the world in a whole new way. While most social media interactions are positive in nature, enemies are using social media as part of a master plan. Rather than a centralized Commander or single focal point being in charge, terrorist's social media campaigns are decentralized, reflecting the networked nature of cyberspace. It is this lack of a centralized point of contact or chain of command that has changed the face of modern warfare.

Option 1 – Status Quo

The first proposed solution to the threat of social media to military members and their families is to continue in the current state – status quo, or operations normal. The use of social media has become prevalent among government employees, military members, and their families. Keeping the use of social media the same as it is today would allow military members and their families to continue to use social media and continue to post content about their units and missions. Air Force Public Affairs is actively using social media as a forum to tell the Air Force story, and in turn, Airmen are using social media to tell their Air Force story. Social media has made every Airman a spokesperson in some way or another. From posting photos of a change-of-command ceremony to a video about a successful mission, Airmen are a large voice of today's Air Force. Recognizing that social media is the primary source of news and information among millennials, military leaders are using social media now more than ever to communicate with Airmen.

A disadvantage of this solution is the continued threat to those using social media. Terrorist groups depend on open media systems, such as social media, to further their message, actively recruit, and promote propaganda, especially to westerners. A 2012 study highlighted that approximately 90 percent of organized terrorism on the Internet is using social media to carry out their threat or cause. This is a trend that continues to grow at a rapid pace.

The National Security Agency, Defense Department, Department of Homeland Security, and even the Internal Revenue Service monitor social media sites regularly, but with more than one-billion active daily users and 934 million mobile daily users on Facebook alone,[45] it would be impossible catch everything. Similarly, with more than 320 million Twitter's monthly users, and more than one-billion unique monthly tweets, it is equally impossible to monitor everything streaming on Twitter.[46] By keeping the current social media policies in place, the Air Force (and DoD) could expect to see continued threats made by terrorists and adversaries against military members and their families. An example of this threat was seen when insurgents in Afghanistan captured a U.S. Army soldier in 2011. The Army quickly realized that the soldier's Facebook page contained information his captors could use in psychological torture. This situation reinforced the Army's determination to better inform their warfighters, commanders, and Public Affairs professionals about the potential dangers of putting too much information online. "Our adversaries are trolling social networks, blogs, and forums, trying to find sensitive information they can use about our military goals and objectives," said U.S. Army Sgt. Maj. Kenneth O. Preston following this incident.[47] Since monitoring the social media platforms of every military member is not a realistic option, the importance of education and training must again be stressed. As technologies advance and emerge, adversaries' capabilities continue to grow and the dangers facing military members and their families will continue to become greater and more frequent.

In addition to military members using social media, military families rely heavily on social media to build relationships, keep in touch with their loved ones, and even learn about military operations and the military way of life. While social media has allowed for increased communication and understanding among military families, it brings forth another concern – the use of private social media channels, such as private Facebook pages. These are pages that are "invite only" and not accessible to the general public or even other Facebook members. Many military spouse groups use these private pages to communicate information, and since they are private, these pages create a false sense of security about what can and cannot be talked about in these forums. Like any social media medium, even private pages can be hacked and can be monitored by Facebook itself, so there is risk associated with discussing operational details such as aircraft land times, locations, and deployment information in private pages – even if they are not open to uninvited social media users.

Continuing the status quo does not decrease the threat of social media to military members and their families. In fact, it decreases the urgency associated with the threat of social media. By changing nothing and remaining silent on the issue, senior leaders are saying there is not a problem or threat associated with social media use. Additionally, this solution does not aid in better protecting military members and their families in the future. Not changing rules or policy as it relates to social media use inadvertently makes military members and their families think the threat is not significant and that social media use without restrictions is safe in the face of modern cyber threats.

Option 2 – Increased Training and Education

A second proposed solution is to increase the education provided to Air Force Public Affairs professionals and therefore the training that Air Force Public Affairs is able to execute.

Increased education would in turn allow the Public Affairs community to better train and inform military members and their families.

The goal of Air Force Public Affairs is to communicate the Air Force mission, and with emerging technology, an efficient and effective way to do that is through social media. Communicating the mission (and message) is not the problem; being able to do it in a safe manner is the challenge. Air Force Public Affairs professionals are provided guidance and training on their core responsibilities, but it is limited and often outdated. The primary purpose of DINFOS, the joint schoolhouse for DoD Public Affairs professionals, is to train members of all branches of the U.S. military in the fields of broadcasting, journalism, public affairs, and visual information. In addition, selected DoD civilians and international military personnel can attend DINFOS for many of its courses. There are 32 different courses taught at DINFOS, and the courses can last from five to 124 days. DINFOS trains approximately 3,200 students annually, and it has trained more than 1,000 international students from over 75 countries.[48] Of the more than 30 classes taught at DINFOS, none are solely focused on social media and the threats associated with open media systems.

Guidance in Air Force Instructions (AFI) is scarce and struggles to keep up with the pace of technology. To date, there have been four editions of the Air Force Social Media Guide, with the latest version published in 2013. This is the primary source of information for Air Force leaders, Airmen, and their friends on how to use social media safely both professionally and personally. The AFI that governs the use of social media for Air Force Public Affairs professionals is AFI 35-113, Internal Information. Section 15 covers social media, it is less than one page long, and was last updated March 11, 2010.

Social media has evolved tremendously since 2013, but the guidance for Public Affairs, and therefore Airmen, remains largely behind the technology power curve. A decade ago, it might have been unthinkable that a militant in Syria might become pen pals with a lonely teenager in small-town America, but this is now a reality. ISIS has discovered a new way to wage war. They may have been the first to wield the cross of social media, terror and war, but they will not be the last. The evolution of social media demands increased training and education to Air Force Airmen to ensure they have the necessary tools to safeguard themselves and their families against the growing threats in the cyber media space.

A disadvantage of this solution involves manpower in the Public Affairs career field. Even if training increases within the Public Affairs community, as long as the career field keeps shrinking, it will be a challenge to properly train all Airmen. In 2015, the Air Force Personnel Center, Directorate of Manpower, advised the Secretary of the Air Force, Public Affairs to implement a Wing Public Affairs Office Standardization Plan and redistribute existing manpower to prepare the career field for a manpower study. All Wing Public Affairs Offices implemented the changes in manpower, as a result of this Standardization Plan, in April 2015. In 2002, most Wing Public Affairs Offices had eight to 12 personnel, but as of 2015, Secretary of the Air Force Public Affairs leaders has five identified key positions: Chief of Public Affairs, Superintendent or Operations Chief, Command Information, Community Engagement, and Media Operations.[49] In addition to the manpower changes over recent years, officer ranks have been reduced across Wing Public Affairs Offices, taking the typical Chief of Public Affairs position from the rank of Major to Lieutenant. Additionally, most Air National Guard Wing Public Affairs Offices do not have a full-time Chief of Public Affairs position, which as seen in Figure 4 below, is a critical component to integration and synchronization of the Public Affairs

team. Public Affairs Airmen can be well trained, but if there are not enough people to effectively perform the mission and educate others, then the training is unable to be fully utilized and effective. Increased social media training is a necessity, but adequate Public Affairs staff must be accounted for in order for this training to be communicated to the larger force.

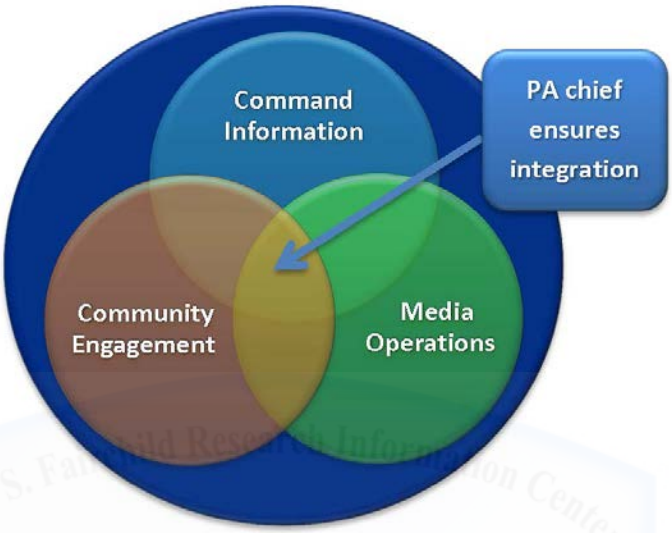

Figure 4 Public Affairs Operational Model.[50]

First, the solution of increasing training and education within the Public Affairs community would likely decrease the threat of social media to military members and their families by providing a solid foundation of understanding for social media. Increased training would allow Public Affairs professionals the expertise to assist members (and their families) with the correct usage of social media, techniques, and ideally case studies that demonstrate the ramifications of their social media posts. A case study would allow the Public Affairs and Intelligence Community to come together to paint a road map for military members, demonstrating the domino effect of posting something "right on the edge" of what should be posted and how enemies can take hold of that tidbit of information and use it against military members and their families. This would go beyond the current guidance that says to "be honest

about your unit and mission without violating OPSEC."[51] The current threat demands more than just telling Airmen to remember OPSEC.

Additionally, this solution will aid in better protecting military members and their families in the future by arming them with the necessary tools to make smart decisions regarding the use of social media. Social media posts are permanent. What you post is online forever, making it even more critical to make smart decisions and have the right guidance prior to posting. Airmen and their families are encouraged to tell their unique Air Force stories, but specific guidance can aid in their protection. Military members and their families must understand what enemies are searching for and how the wrong information can help become a small piece of the large puzzle terrorist groups are trying to put together in order to threaten families and gain access to personal information. Requiring Public Affairs professionals to attend a specific course focused on social media at DINFOS, in addition to a specific course on the threat of social media as part of the annual required military auxiliary training, would allow for an increased understanding and help reduce the threat towards military members and their families. One of the fundamentals of Public Affairs is to practice security at the source,[52] and by having increased training on the risks associated with social media, Public Affairs professionals can both practice and educate members on how best to safely tell the Air Force story, while utilizing social media.

Option 3 – Change in Policy

A third proposed solution is to change the policy currently governing social media use in the Air Force. The DoD issued a policy in March 2010 which authorized the use of Facebook, Twitter, YouTube and other social media sites from unclassified computers, as long as the activity did not compromise operational security or involve prohibited activities or sites.

As stated above, Air Force guidance on social media is largely outdated and not keeping up with the pace and evolution of social media usage. On March 23, 2015, DoD published a video about keeping Airmen safe in the social media world, with many critiquing the video because it was delivered by a junior enlisted Navy sailor verses a senior ranking military leader.[53] The video simply states there are risks associated with social media and to learn how to protect yourself and your family, visit <www.defense.gov.> In an obscure location on the defense.gov website resides the 2015 Guide to Keeping Your Social Media Accounts Secure. While the guide gives protective measures, preparation checklists, Facebook, Twitter, Google+, YouTube, Instagram, and Flickr do's and don'ts, it does not provide any real-life scenarios or examples to help users understand the ramifications of posting the wrong material online. While the specific mediums, platforms, and technologies may change over time, the overall trend of people connecting with one another enabled by technology only increases.[54] To date, the DoD and Air Force have yet to provide a risk communication strategy or case study that shows what can happen when military members and their families "post before they think" and how quickly terrorists can take that information and use it against them. Again, one small post can become part of the bigger puzzle terrorist organizations are trying to piece together.

Social media is evolving at a startling rate, and guidance and policy must keep up with this evolution. Beyond the guide discussed above, the DoD and Air Force should revisit the 2010 policy, providing limitations on social media use and stronger recommendations on how to stay safe using social media platforms. In 2015, military members working at the Pentagon were encouraged to change their Facebook profile names from their first and last name to an alias. Many Pentagon employees heeded this recommendation, but it stopped there. This

recommendation only somewhat trickled down to individual Wings, and only in a few instances reached the Air Force Reserves or the Air National Guard.

The advantage of a larger policy and guidance change is that it would force education and training and come from a position of command rather than simply the Air Force Public Affairs community. A disadvantage of this solution, along with any solution, is the military cannot control what Airmen and their families do on their own time (to a certain extent). While there is specific guidance on how military members may not use social media to express political opinions and endorse candidates, similar stringent guidance still does not exist in terms of how social media use could pose a threat to military members and their families.

This option would not necessarily reduce the threat of social media to military members and their families, but it would assist in better protecting military members and their families because it would force a top down approach. The DoD sees the need for increased guidance, which is obvious in the 2015 release of Joint Publication 3-61, which includes an Appendix dedicated to Social Media. This publication is the most comprehensive guidance to date, and includes discussion on social media risks, but it still does not go deeply into the risks of posting ABC, which could result in XYZ, a case study of sorts. Social media is a significantly more open and global communication platform than has been experienced before, and it has demonstrated real power and benefits in reaching stakeholders and publics. With this openness comes some risks, but these risks can be mitigated through training. In today's environment, the real risks are found in not being present.[55]

Conclusion

Social media is rewriting the rules of modern warfare, and this paper has highlighted how this emerging technology has made it more difficult to analyze and predict enemies' behaviors

and control the information that is in the public domain. Social media is a growing influence that is here to stay. "The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner," said Ban Ki-moon Secretary-General of the United Nations.[56]

The Air Force has utilized social media since 2010 and in most cases has maximized this capability to increase communication with Airmen and tell the Air Force story. With the ease of a button, social media serves as a way to communicate internally with Airmen, and also as a means to tell the story of military members to external audiences who themselves are actively engaged in social networks.[57]

The military has entered a new era of warfare, a new threat unlike anything combatted in the past. Social media is changing warfare, it is changing the game, and the military must adapt to protect against the emerging threat associated with open media systems. The goal of this paper was to evaluate if social media, specifically Facebook, poses a threat to military members and their families and to evaluate if the education provided to Air Force Public Affairs professionals is adequate to protect against this threat. Additionally, this paper explored possible avenues for the Air Force to consider, balancing the inevitable use of social media, with the increasing threat to military members and their families from social media. To do this, a level of understanding had to be established and a road map had to be built to show the past, present, and potential future of social media and the growing threat surrounding social networking.

A multitude of examples and scenarios throughout this paper have shown that social media does pose a threat to military members and their families. Terrorist organizations use social media to target military members, and this opens Airmen up to vulnerabilities while off duty, inherently putting their families at risk as well. This is a real and growing threat. As a

communication medium, social media is a critical tool for terrorist groups to exploit. "ISIS is an extremely dangerous organization. It's public messaging and social media tactics are as slick and as effective as any I've ever seen from a terrorist organization," said Jeh C. Johnson, Secretary of the U.S. Department of Homeland Security in 2014. "We know that ISIS is prepared to kill innocent Americans, just because they are Americans." [58]

Recommendation

The recommendation presented in this paper is multi-tiered. Initially, the DoD should establish a course at DINFOS that focuses on social media and the associated threats of this growing communication medium and should require all Public Affairs Officers and Enlisted Superintendents to complete the course. This would accomplish multiple objectives. First, it would educate the Public Affairs career field (across the entire DoD since DINFOS is a joint school) and therefore allow Public Affairs to better train military members and their families and safeguard them against the threat. Additionally, by creating a course at a joint schoolhouse, it would demonstrate a high level of support of senior DoD leaders and understanding of the threat and need for additional education and training.

A follow-on step to the social media-centric DINFOS course is for the Air Force to create a risk communication strategy or case study, built jointly between the Public Affairs and Intelligence Community. This strategy or study would provide a road map to use in training sessions that shows a step-by-step guide of what can happen if the wrong information (or even too much of the right information) is posted on social media and how a small piece can add to the larger puzzle terrorist are trying to piece together to threaten military members and their families. Air Force Public Affairs could utilize this strategy or study at wing level training

sessions, or the Air Force could incorporate it into the annual online training course requirements of all Airmen through the Advanced Distributed Learning Service (ADLS).

The next and final tier comes with updating policy and guidance, to include AFIs, in a timely manner to reflect the growing threat and the pace in which social media is emerging. This includes revisiting the 2010 social media policy, updating AFI 35-113 (dated March 11, 2010), providing annual updates to the Air Force Social Media Guide (dated June 1, 2013), and using the Public Affairs 2015 Joint Publication 3-61 to further expand on social media risks and management. This tier allows for a top down approach to the issue and therefore will allow the Public Affairs career field to have senior level support when implementing policy, conducting training, and helping to further educate Airmen and their families.

Ultimately, any of these recommendations would better train and educate the Public Affairs community and therefore help safeguard military members and their families, but ideally a multi-tiered approach would be utilized to best address this emerging threat. Social media is here to stay, and so is the reliance on social media by enemies of the U.S. and terrorist organizations. Safeguarding military members and their families against the threat is paramount. The evolution of social media demands increased training and education to Air Force Airmen to ensure they have the necessary tools to safeguard themselves and their families against growing threats in the cyber media space. It is essential to ensure the safety of military members and their families when using social media, all while continuing to tell the Air Force story.

Endnotes

[1] Department of Defense, "Principles of Information," November 9, 2001.
[2] "This day in Military History, 1776, Thomas Paine," wordpress.com, January 10, 2014.
[3] Laura Fitzpatrick, "Brief History YouTube," Time Magazine, May 31, 2010.

[4] Andrew Perrin, "Social Media Usage: 2005-2015," Pew Research Center, October 8, 2015.
[5] Caitlin Dewey, "Almost as many people use Facebook as live in the entire country of China," The Washington Post, October 29, 2014.
[6] Caitlin Dewey, "Almost as many people use Facebook as live in the entire country of China," The Washington Post, October 29, 2014.
[7] Ibid, page 2.
[8] Washington Press Desk, "U.S. Military OKs use of online social media," CNN News, March 5, 2010.
[9] U.S. Air Force, "Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013, page 2.
[10] Caitlin Dewey, "Almost as many people use Facebook as live in the entire country of China," The Washington Post, October 29, 2014.
[11] U.S. Air Force, "Navigating the Social Network," Air Force Public Affairs Agency, Social Media Division, July 18, 2012.
[12] George Ago, "15 Striking Findings from 2015," Pew Research Center, December 22, 2015.
[13] Pew Research Center, 2005-2006, 2008-2015 survey data. No data are available for 2007.
[14] Department of Defense, "Joint Publication 3-61: Public Affairs," November 17, 2015, page I-1.
[15] U.S. Air Force, "Social Media Sites," www.af.mil, January 27, 2016.
[16] Department of Defense, "Joint Publication 3-61: Public Affairs," November 17, 2015, page F-1.
[17] Randy Roughton, "SecAF Relies on Face-to-Face Engagement," Airman Magazine, November 9, 2015.
[18] Drapeau, M. & Wells, L, "Social Software and National Security: An Initial Net Assessment," National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, D.C., 2009, page 5.
[19] Ibid, page 6.
[20] John Kirby, "Press Briefing by Rear Admiral Kirby," Department of Defense, Pentagon Briefing Room, February 27, 2016.
[21] U.S. Air Force, "Air Force Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013, page 8.
[22] Department of Defense, "Joint Publication 3-61: Public Affairs," November 17, 2015, page GL-5
[23] U.S. Air Force, "New Media and the Air Force," Air Force Public Affairs Agency, Emerging Technology Division, April 10, 2009, page IV.
[24] U.S. Air Force, "Air Force Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013, page 6.
[25] Twitter, "The Twitter Glossary," twitter.com, page 1.
[26] Habeeb Lee, "As much as think tanks, we need storytelling tanks – and a way to disperse the stories far and wide," National Review, October 22, 2013.
[27] U.S. Air Force, "Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013.
[28] U.S. Department of Justice, "Internet Social Networking Risks," Federal Bureau of Investigation, Counterintelligence, 2014.
[29] CBC, "Terrorist Groups Recruiting through Social Media," CBC News, Technology and Science Division, with contributions from the Associated Press, April 5, 2012.

[30] Ashley Frantz, "As ISIS Threats Online Persist, Military Members Rethink Online Life," CNN News, March 23, 2015.
[31] Brian Jenkins, "Is Al Qaeda's Internet Strategy Working," Testimony presented before the House of Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, December 6, 2011.
[32] J.M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter," The Brookings Project on U.S. Relations with Islamic World, Analysis Paper, No. 20, March 2015.
[33] Osama Bin Laden, "Terrorism Against America Deserves to be Praised," Transcripts of excerpts released by al Jazeera, video recording of Osama Bin Laden, Outlook Magazine, December 27, 2001.
[34] U.S. House of Representatives, "Jihadist use of social media – how to prevent terrorism and preserve innovation," Homeland Security Committee, Counterterrorism and Intelligence Subcommittee Hearing, December 6, 2011.
[35] Ray Sanchez, "ISIS exploits social media to make inroads in U.S.," CNN, June 5, 2015.
[36] Committee on Homeland Security, "Worldwide Threats to the Homeland," Hearing before the Committee on Homeland Security, House of Representatives, Serial No. 113-85, September 17, 2014, page 65.
[37] Ibid, page 3.
[38] Inside Defense, "Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security," InsideDefense.com, http:// www.insidedefense.com/, 15 January 2003.
[39] Timothy L. Thomas, "Al-Qaeda and the Internet: The Danger of 'Cyberplanning,'" Parameters, Volume 23, Issue 1, Spring 2003, pages 112-123.
[40] Committee on Homeland Security, "Worldwide Threats to the Homeland," Hearing before the Committee on Homeland Security, House of Representatives, Serial No. 113-85, September 17, 2014, page 19.
[41] Ibid, page 20.
[42] Ashley Frantz "As ISIS Threats Online Persist, Military Members Rethink Online Life," CNN News, March 23, 2015.
[43] University of Texas, "ISIS Targeting Military Members Via Social Media," Trade Journal, March 27, 2015, page 1.
[44] Daniel Costa-Roberts, "ISIS Publishes Online Hit List of US Service Members," PBS News Hour, March 22, 2015.
[45] Facebook, "December 2015 Statistics," www.newsroom.fb.com/company-info, 2015.
[46] Twitter, "Twitter Usage, Company Facts," www.about.twitter.com/company, 2015.
[47] J.R. Wilson, "Military Security Issues of Social Media: Army," Defense Media Network, June 14, 2011, page 1.
[48] Defense Information School, www.dinfos.dma.mil.
[49] U.S. Air Force, "Wing Public Affairs Office, Standardization Plan," March 2015.
[50] Ibid, page 7.
[51] U.S. Air Force, "Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013.
[52] Department of Defense, "Joint Publication 3-61: Public Affairs," November 17, 2015, page viii.
[53] Department of Defense, "Service members should use caution on social media," Defense Media Activity Video, March 22, 2015.

[54] Department of Defense, "Joint Publication 3-61: Public Affairs," Appendix F, Social Media, November 17, 2015, page F-1.
[55] Ibid, page F-5.
[56] United Nations, "The Use of the Internet for Terrorist Purposes," United Nations Office on Drugs and Crime, United Nations, New York, 2012.
[57] U.S. Air Force, "Social Media Guide," Air Force Public Affairs Agency, 4th Edition, June 1, 2013.
[58] Committee on Homeland Security, "Worldwide Threats to the Homeland," Hearing before the Committee on Homeland Security, House of Representatives, Serial No. 113-85, September 17, 2014, page 12.

Bibliography

Ago, George, *15 Striking Findings from 2015*, Pew Research Center, December 22, 2015.

Assistant Secretary of Defense, *Personally Identifying Information in Public Affairs Products*, Memorandum for Chief of Public Affairs, U.S. Army, U.S. Navy Chief of Information, Director of Public Affairs, Office of the Secretary of the Air Force, Director of Public Affairs, United States Marine Corps, Director of Public Affairs, National Guard Bureau, July 1, 2015.

Berger. J.M. and Morgan, Jonathan, *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*, The Brookings Project on U.S. Relations with Islamic World, Analysis Paper, No. 20, March 2015.

Bin Laden, Osama, *Terrorism Against America Deserves to be Praised*, Transcripts of excerpts released by al Jazeera, video recording of Osama Bin Laden, Outlook Magazine, December 27, 2001.

CBC, *Terrorist Groups Recruiting through Social Media*, CBC News, Technology and Science Division, with contributions from the Associated Press, April 5, 2012.

Comey, James B., *Statement Before the Senate Committee on Homeland Security and Governmental Affairs*, Federal Bureau of Investigations, Washington, D.C., October 8, 2015.

Committee on Homeland Security, *Worldwide Threats to the Homeland*, Hearing before the Committee on Homeland Security, House of Representatives, Serial No. 113-85, September 17, 2014.

Costa-Roberts, Daniel, *ISIS Publishes Online Hit List of US Service Members*, PBS News Hour, March 22, 2015.

Defense Information School, www.dinfos.dma.mil, 2015.

Department of Defense, *Guide to Keeping Social Media Accounts Secure*, Defense Media Activity, 2013.

Department of Defense, *Joint Publication 3-61*: *Public Affairs*, November 17, 2015.

Department of Defense, *Principles of Information*, November 9, 2001.

Dewey, Caitlin, *Almost as many people use Facebook as live in the entire country of China*, The Washington Post, October 29, 2014.

Drapeau, M. and Wells, L., *Social Software and National Security: An Initial Net Assessment*, National Defense University Center for Technology and National Security Policy, Fort Lesley J. McNair, Washington, D.C., 2009.

Facebook, *December 2015 Statistics*, Facebook Newsroom, 2015.

Fitzpatrick, Laura, *Brief History YouTube*, Time Magazine, May 31, 2010.

Frantz, Ashley, *As ISIS Threats Online Persist, Military Members Rethink Online Life*, CNN News, March 23, 2015.

Inside Defense, "Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security," InsideDefense.com, http:// www.insidedefense.com/, 15 January 2003.

Jenkins, Brian, *Is Al Qaeda's Internet Strategy Working*, Testimony presented before the House of Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, December 6, 2011.

Kirby, John, *Press Briefing by Rear Admiral Kirby*, Department of Defense, Pentagon Briefing Room, February 27, 2016.

Lee, Habeeb, *As Much as Think Tanks, We Need Storytelling Tanks – and a Way to Disperse the Stories Far and Wide*, National Review, October 22, 2013.

Perrin, Andrew, *Social Media Usage: 2005-2015*, Pew Research Center, October 8, 2015.

Roughton, Randy, *SecAF Relies on Face-to-Face Engagement*, Airman Magazine, November 9, 2015.

Sanchez, Ray, *ISIS exploits social media to make inroads in U.S.*, CNN, June 5, 2015.

Timothy L. Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, Parameters, Volume 23, Issue 1, spring, 2003.

Twitter, *Twitter Usage, Company Facts*, Twitter Newsroom, 2015.

Twitter, *The Twitter Glossary*, Twitter Help Center, twitter.com, 2015.

United Nations, *The Use of the Internet for Terrorist Purposes*, United Nations Office on Drugs and Crime, United Nations, New York, 2012.

University of Texas, *ISIS Targeting Military Members Via Social Media*, Trade Journal, March 27, 2015, page 1.

U.S. Air Force, *Air Force Social Media Guide*, Air Force Public Affairs Agency, 4th Edition, June 1, 2013.

U.S. Air Force, *Navigating the Social Network*, Air Force Public Affairs Agency, Social Media Division, July 18, 2012.

U.S. Air Force, *New Media and the Air Force*, Air Force Public Affairs Agency, Emerging Technology Division, April 10, 2009.

U.S. Air Force, *Social Media Sites*, www.af.mil, January 27, 2016.

U.S. Air Force, *Wing Public Affairs Office, Standardization Plan*, March 2015.

U.S. Department of Defense, *Service Members Should Use Caution on Social Media*, Defense Media Activity Video, March 22, 2015.

U.S. Department of Justice, *Internet Social Networking Risks*, Federal Bureau of Investigation, Counterintelligence, 2014.

U.S. House of Representatives, *Jihadist use of social media – how to prevent terrorism and preserve innovation*, Homeland Security Committee, Counterterrorism and Intelligence Subcommittee Hearing, December 6, 2011.

Washington Press Desk, *U.S. Military OKs use of online social media*, CNN News, March 5, 2010.

Wilson, J.R., *Military Security Issues of Social Media: Army*, Defense Media Network, June 14, 2011, page 1.