SOCIAL MEDIA RISK ANALYSIS:
HOW TO USE ACCEPTED RISK ASSESSMENT TOOLS TO ANALYZE SOCIAL MEDIA RISKS IN MILITARY ORGANIZATIONS

BY

WING COMMANDER BENJAMIN W. POXON

ROYAL AUSTRALIAN AIR FORCE

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2017

Approval

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

DAVID C. BENSON (Date)

_____

STEPHEN E. WRIGHT (Date)

Disclaimer

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the United States or Australian Governments, the United States Department of Defense, Australian Department of Defence, the United States Air Force, the Royal Australian Air Force, or Air University.

About the Author

Wing Commander Poxon is a Royal Australian Air Force pilot. After completing Pilot's Course in 2002, he was posted to 37 Squadron at RAAF Richmond where he qualified as a C-130J-30 Hercules pilot. During a six-year posting at 37 Squadron and 285 Squadron, Wing Commander Poxon conducted operational deployments to Timor-Leste, Cyprus, Solomon Islands, Iraq, and Afghanistan. Promoted to Squadron Leader in 2010, he remained at 37 Squadron as a Flight Commander where he commanded multiple deployments to Iraq and Afghanistan. In 2014, Wing Commander Poxon was assigned to the Executive Officer position at 84 Wing before attending USAF Air Command and Staff College and USAF School of Advanced Air and Space Studies from 2015 to 2017. He has been selected to command 35 Squadron flying the C-27J Spartan aircraft at the completion of his studies.

Acknowledgements

I would like to acknowledge the help and support of several individuals, without which I would not have been able to complete this thesis. My advisor, Dr. David Benson, and reader, Dr. Stephen Wright, spent countless hours reviewing drafts and providing insightful feedback. I would also like to thank Group Captain Darren Goldie (RAAF), who served as a devil's advocate during all stages of development. Additionally, Lieutenant Colonel Eamon Murray (USAF), Wing Commander James Radley (RAF), Lieutenant Colonel Matthew Riggs (Armee de l'air) and Ms. Connie Heiss for their thoughtful review and advice.

Most importantly, I want to express my sincere appreciation to my wife for her love, patience, and understanding.

Contents

Illustrations

Introduction

> *It's the great irony of our Information Age – the very technologies that empower us to create and build also empower those who would disrupt and destroy...one of your greatest strengths, in our case, our ability to communicate to a wide range of supporters through the internet-could also be one of our greatest vulnerabilities.*
>
> *President Barack Obama*
> *White House Briefing*
> *29 May 2009*

This article analyzes the use of social media by military organizations. It asks, why has the United States Air Force (USAF) become more transparent regarding the use of social media, while other Air Forces remain cautious? Why, for example, does the USAF have more than one thousand official social media pages for wings, bases, and squadrons when the Royal Australian Air Force (RAAF) and Royal Air Force (RAF) limit their exposure to a few? More importantly, what are the consequences of this approach?

The accepted wisdom implies that the USAF is considerably different in size, capability, and resources when compared to other Air Forces. For example, the USAF is approximately twenty times larger in terms of active duty personnel and annual operating budgets than the RAAF.[1] These additional resources enable the USAF to develop policies, guidelines, and training to engage in a range of new media technologies. Nevertheless, all Air Forces face similar organizational objectives: creating a safe and cohesive workplace, managing a deployed workforce, recruitment, community engagement, brand management, and support for personnel and families. It appears at the outset of this study that USAF commanders utilize the ubiquitous and expressive

[1] USAF official website. "Air Force Demographics." Accessed 31 December 2016. http://www.afpc.af.mil/Air-Force-Demographics; Australian Government Department of Defence, *Defence Issues Paper 2014* (Australia: Commonwealth of Australia, 2014), 36, http://www.defence.gov.au/whitepaper/docs/defenceissuespaper2014.pdf; Secretary of the Air Force Public Affairs, "AF Presents Fiscal Year 2017 Budget," U.S. Air Force. 09 February 2016, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/652961/af-presents-fiscal-year-2017-budget.aspx; Commonwealth of Australia, "2016 Defence White Paper" (Department of Defence, 2016), 180, http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

characteristics of social media to complement their strategic communication goals and achieve their organizational objectives.

Social media represents the greatest increase in expressive capability in history.[2] During the twentieth century, the significant advances in media technology have enabled new ways of communicating, including the invention and popularization of the radio, television, and telecommunications. However, the expressive capabilities of these media are limited. The media that supported conversation could not create groups. The media that created groups did not support conversation. To illustrate, print media, television, and radio distribute one message among a group of people; while the telephone enables conversation, it is limited in distribution. The advent of social media amalgamates both groups and conversations, enabling a fusion of friends, families, interest groups, traditional media, business, politics, and military organizations alike.[3]

The new media environment presents opportunities for military organizations that have positive and negative outcomes. On the one hand, social media enables transparency, openness, and connection with a global audience. These characteristics promote accountability, participation, and collaboration.[4] On the other hand, the overwhelming digital footprint generated by social media creates an information-rich environment for adversaries to exploit.[5] Furthermore, the use of social media may have a detrimental impact on a military organization's mission, capability, reputation, and personnel.[6] The conflict between the benefits of transparency and the demands of security creates tension within military organizations. While tension existed in traditional forms of media, the ubiquitous, expressive, and permanent nature of the new media environment

[2] Clay Shirky, "How Social Media Can Make History," June 2009, pt. 2:02, https://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history#t-192111.
[3] Shirky, "How Social Media Can Make History," pt. 3:10.
[4] Managing Director, "Open Government Directive," *Federal Communications Commission*, December 8, 2009, https://www.fcc.gov/general/open-government-directive.
[5] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar*, n.d., 45.
[6] Nurul nuha Abdul Molok, Shanton Chang, and Atif Ahmad, "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats" (Edith Cowan University, November 30, 2010), 70, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism.

demands that organizations strike a balance between transparency and security to find an acceptable middle path.[7]

Upon arrival to the U.S., the author was perplexed by the level of transparency the USAF accepts with its use of social media. A cursory glance through squadron, group, and wing social media sites uncovers a wealth of information about personnel, families, missions, and emerging capabilities.[8] A few examples include airmen's names, family photos, special operations training, flight schedules, and aerial combat strikes. The use of social media by the USAF is in stark contrast to the RAAF. The RAAF employs six official sites and limits commanders within the organization by requiring 2-star approval to utilize official social media.[9] At the outset of this study, the author believed that the USAF has swung too far toward transparency and may pose an unnecessary risk to operational and personal security. However, what are these risks, and where are militaries vulnerable?

The rapid rise of social media has challenged leaders at all levels of military organizations to understand a new set of vulnerabilities and threat vectors that may impact their operations. Furthermore, there appears to be no risk analysis to inform military commanders in deciding whether to utilize social media within their organizations. This article seeks to investigate a spectrum of security risks that military commanders assume when their organizations engage in social media. By utilizing accepted risk management processes, the study will determine the residual risk that military organizations may accept and, in doing so, facilitate a discussion concerning the use of social media for military commanders in general.

The author evaluates the question regarding social media security by creating a risk model akin to risk management in military organizations. The model is framed by a *SANS Institute InfoSec Social Media Risk Report,* which identifies potential

---

[7] Mick Ryan, AM and Marcus Thompson, AM, "Social Media in the Military: Opportunity, Perils and a Safe Middle Path," Grounded Curiosity, accessed April 6, 2017, http://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/#sthash.rd2ODm2U.dpbs.
[8] The USAF permits commanders to utilize official social media to complement their communication strategies. While it is usually conducted at the wing (O6) level, a few squadrons (O5/4) also utilize the medium.
[9] Royal Australian Air Force, "Social Networking: A Guide to Effective Social Media Use," Commonwealth of Australia, *Social Networking*, 2014, 16, https://www.airforce.gov.au/docs/Social%20Media%20Booklet.pdf.

vulnerabilities associated with social media and a Center for Cyber and Homeland Security Report that identifies emerging threat actors.[10,11] Additionally, the model employs USAF policy, guidelines, and training to demonstrate potential risk mitigation strategies.[12] The model utilizes USAF risk mitigations for two reasons. First, the USAF is the most prolific user of social media amongst many militaries.[13] Therefore, the author perceives that the digital footprint the USAF creates is the most vulnerable to exploitation among peer militaries. Secondly, an Australian Defence Force review into social media stated that the U.S. policy, guidelines, and training are the "international best practice."[14] Given a set of vulnerabilities, threat actors, and mitigations, the model illustrates a range of potential risks that commanders should consider when their organizations engages in social media.

This article concludes that military organizations that participate in social media increase their risk and exposure to adversaries and threat events. Without mitigation, military organizations have the potential to be exposed to a high risk to their personnel, mission, capability, and reputation. However, for a military organization to have no mitigation would be extremely uncommon and reckless. The model demonstrates an overall residual risk of "low" given USAF controls and resources. Additionally, there appears to be no "one size fits all" use of social media for military organizations. Instead, commanders at all levels of the organization should assess the utility of social media to meet specific organizational objectives and weigh them against the risks presented in this study to decide if social media is worthwhile.

---

[10] Robert Shullich, "Risk Assessment of Social Media" (SANS Institute InfoSec Reading Room, December 5, 2011), https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749.

[11] Frank Cilluffo, "Emerging Cyber Threats to the United States" (GW Center for Cyber and Homeland Security, February 25, 2016), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HHSC_Testimony_Feb%2025-2016_Final.pdf.

[12] Appendix B: USAF Policy Review.

[13] The author investigated the use of official social media by USAF, RAAF, RAF, Royal New Zealand Air Force, Royal Canadian Air Force, Israeli Air Force, and People's Liberation Army (PLA) Air Force. There is an overwhelming difference in the number of official sites and posts from the USAF when compared to other Air Forces.

[14] George Patterson, *Review of Social Media and Defence* (Commonwealth of Australia, 2011), vii, http://www.defence.gov.au/pathwaytochange/docs/socialmedia/Review%20of%20Social%20Media%20and%20Defence%20Full%20report.pdf.

The article will progress in four sections. The first section describes the different schools of thought regarding the use of social media by military organizations. Each school of thought represents varying levels of risk tolerance and perceived utility of social media. The second section sets up a risk model by identifying common social media vulnerabilities and the threat actors that exploit them. The third section uses the model to describe how adversaries exploit social media vulnerabilities, and in doing so, measures the impact and residual risk that commanders accept. The last section describes USAF's risk acceptance and utilization of social media within the service to achieve strategic and organizational goals.

Schools of Thought

Airmen in the RAAF and USAF hold a continuum of views regarding their organizations' use of social media. The views range from acceptance of social networking and the benefits for military organizations to a rejection of them.[15] A sliding scale between security and transparency illustrates the breadth of opinion and, in many cases, the perceived benefit of social media becomes proportional to the risk leaders are willing to accept. Airmen's views also show inconsistencies and polarization based on a lack of knowledge regarding the threats present in the cyber domain.[16] Nevertheless, the USAF no longer considers social networking sites to be a fad and believes those sites form a part of most airmen's lives.

The author identified four different schools of thought that correspond to the perceived value of social media, and from this perspective, leaders deduce the various underlying risks. The schools of thought are zero tolerance, traditional media, new media, and information dominance. Leaders in the Air Force may align to one or more schools when contemplating the use of social media. The four categories are useful when explaining the level of risk that leaders are willing to accept.

A study conducted by the Australian Defence Force in 2011 identified a range of viewpoints that are representative of each school. The study analyzed the response of 900 defense personnel to the question, 'How should Defence manage social media differently to civilian business?' The report concluded that "some members view social media use as a highly risky activity that threatens operational security (OPSEC), discloses patterns of life and might bring the military brands into disrepute. Others believe that it is beneficial if guidelines, including guidance on OPSEC, personal security, and the nondisclosure of employment affiliation, are followed."[17] A selection of the study's responses, in conjunction with comments from prominent USAF leaders, will frame the discussion about the different schools of thought. Leaders may refer to these schools when debating whether, and in what manner, social media should be employed within the organization.

---

[15] Patterson, *Review of Social Media and Defence*, ix.
[16] Patterson, *Review of Social Media and Defence*, x.
[17] Patterson, *Review of Social Media and Defence*, x.

Zero Tolerance

> There should be no social networking networks available to Australian Defence Force (ADF) members. ADF members should be discouraged from using social networking sites, as 'Pattern of Life' monitoring is standard within intelligence collection. These networks present a clear and present danger in relation to potential security leaks.[18]

The zero-tolerance school holds that any engagement in social media represents an unnecessary risk to the organization and its people. Unnecessary risk comes without a commensurate return in terms of real benefits or available opportunities. Zero-tolerance believes that social media does not contribute meaningfully to future missions and needlessly jeopardizes security.[19] While many personnel within the school see the potential benefits of social media, once weighed against the potential risks, the benefits become unwarranted. Moreover, zero tolerance reinforces that the primary objective of military organizations is to prepare for future missions above all else. Zero-tolerance believes that engagement in social media at all levels risks widening the organization's digital footprint thereby increasing the amount of actionable information to adversaries. The digital footprint created by organizational and personal use of social media sets tracks in the snow to the detriment of future operations. Many advocates believe that the personal use of social media should be restricted to avoid disclosure of information to current and future adversaries. Overall, the zero-tolerance school holds a very low risk tolerance towards organizational use of social media.

Traditional Media

> OPSEC needs to catch up…The Department of Defense is, in a sense no different than any big company in America. What we can't do is let security concerns trump doing business. We have to do business.[20]

The traditional media school views social media as an extension of traditional media. Public affairs staff and senior commanders release carefully crafted messages to

---

[18] Patterson, *Review of Social Media and Defence*, 111.
[19] "Air Force Guidance Memorandum to AFI 90-802 Risk Management" (Department of the Air Force, March 8, 2016), 3, http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf.
[20] American Forces Press Service. "Social Media Sites Provide Morale Boost; Official Says," Armed Forces Press Service, Washington, DC, March 17, 2010.

educate the wider media and community about military operations. Traditional media emphasizes strict control and release of information. It prefers one-way monologs but tolerates limited public response to posts.[21] The focus of engagement concerns business related objectives, for example, brand management, recruitment, and public relations. Senior leaders and public affairs personnel restrict the release of information on social media due to its official nature and the risk of brand and reputational damage. Therefore, senior leaders are willing to accept a small digital footprint at high levels of the organization akin to a low risk profile. Personnel at lower levels of the organization express polarizing views regarding this school of thought.

On the one hand, many airmen may agree with the organization's limited engagement in social media. Some leaders cite a lack of resources, education or understanding of the risks involved with social media, which does not enable them to engage safely, or they do not find a need to use it for day-to-day communication. On the other hand, airmen express frustration by the official and formal status placed on the use of social media. They see as the same potential senior leaders do regarding its utility and wish to use it to promote unit cohesion, communicate with other units, or connect with families and the public writ large. These opinions form the basis for the new media school of thought.

[21] Mark Drapeau and Linton Wells, "Social Software and National Security: An Initial Net Assessment" (Center for Technology and National Security Policy. National Defense University, April 2009), 3, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525.

New Media

> Defence must acknowledge the ubiquity of social media in the communications age, learn to harness its power for recruiting and welfare purposes, and formulate robust guidance to soldiers and commanders in order to balance the need to safeguard our operational and communications security whilst exploiting the opportunities social media presents…We have forgotten that we are engaged in a permanent hearts-and minds operation with Australian society - one that we are currently losing. Defence has already lost too much credibility in the public eye due to its inability to keep up with the 24/7 news cycle. It needs to entrust its people with the power of their own voices, views, and opinions. Only through improved awareness of our institution, culture, and values can the Australian public truly believe that we are an organisation worthy of their loyalty, respect, and admiration.[22]

The new media school demands that organizations relinquish the control that is required for official communication and allow leaders at lower levels of the organization to harness the power of social media. The new media philosophy moves away from the traditional manicured release of information and advocates that, in addition to the traditional business objectives, the organization should educate and entrust personnel to adopt a softer and more personal tone with the public. It accepts that statements from military personnel represent an opinion rather than an official statement.

Advocates of the new media school are either unaware of social media risks and unknowingly support an increase in an organization's digital footprint, or are aware of the risks and urge leaders to accept them. The risk-aware airmen often state that most intelligence agencies already know (or can access) the information released on social media. When challenged about personal or operational information, the school often cites the capabilities and actions of adversaries, for example, the Office of Personnel Management hack that acquired millions of records about government employees, foreign intelligence agencies storing personal information, and capabilities to exploit sensitive and classified networks.[23]

---

[22] Patterson, *Review of Social Media and Defence*, 120.
[23] Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis, Maryland: Naval Institute Press, 2016), 6.

Information Dominance

> I expect airmen at all levels – especially those who are in command and leadership positions - to increase our engagement with the public via media, Congress, academia, think tanks, industry, our partner nations, and our airman.[24]

> Social Media is the way to go. If someone is not treating you properly, that will happen in fake news; it is a fast way of getting the word out…it's the modern way to communicate.[25]

The information dominance school believes that airmen and leaders at all levels of the organization should increase the use of social media (along with other forms of cyber activities) to dominate the information domain.[26] Information dominance supposes that operations, actions, and activities can affect the decision-making and behavior of adversaries to gain advantage across a range of military operations.[27] Furthermore, they prescribe to an increased digital footprint to enable timely, credible, transparent, and consistent engagement with a global audience.[28]

Information dominance holds that reducing information within the digital environment has the potential to lose control of the domain and the associated strategic narrative. The school espouses the education of leaders and airmen to mitigate and accept social media risks while increasing the amount of information released. They remain ambivalent toward the use of social media to communicate within the organization. Instead, the viewpoints focus on the use of social media as a force enabler to achieve the military's overall missions. Furthermore, losing information dominance or the strategic narrative presents a greater risk than the security concerns presented by other schools of social media.

---

[24] Dave Goldfein, "'America's Air Force: Always There' Letter of Intent," Letter, January 27, 2017.
[25] ABC Australia, "Donald Trump, Malcom Turnbull Meeting Looks like an Attempt to Mend Fractures," News, *ABC News*, 05May2017, http://www.abc.net.au/news/2017-05-05/donald-trump-malcolm-turnbull-meeting-usyd-analysis/8501058.
[26] William Lt Gen Bender, "Air Force Policy Directive 17-1 Information Dominance Governance and Management" (USAF, 12April2016), https://fas.org/irp/doddir/usaf/afpd17-1.pdf.
[27] "Strategy for Operations in the Information Environment" (Department of Defense, June 2019), 8, https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.
[28] Goldfein, "'America's Air Force: Always There' Letter of Intent."

All schools of thought require commanders to accept different levels of risk. In 2011, Lieutenant General William B. Cadwell, NATO Training Mission-Afghanistan commander stated:

> Operational security is an enduring concern for military operations. However, we cannot take counsel of our fears at the expense of new media applications. Commanders accept risk in any operation. We are not talking about rejection of risk, but rather about the parameters of the risk we're willing to accept.[29]

Commanders may see value in utilizing the schools of thought to understand how each one influences their judgment of social media risks. For instance, the zero-tolerance school may represent a commander's risk tolerance for units engaged in covert operations. Moreover, the information-dominant school may represent a view that employs social media to influence the decision-making and behavior of adversaries.

Each school of thought differs regarding the utility, objectives, and risk tolerance toward the use of social media without one being worthier than the other. Every school requires analysis of threats, vulnerabilities, and impacts to understand social media risks. Commanders utilize the risk management process to inform decision-making, integrate risk management controls into operations, make risk decisions at the appropriate level, and apply the process cyclically and continuously.[30] The study will utilize these tools to illustrate the potential risks involved when organizations engage in social media.

[29] Jimmy Hall, "Leveraging Social Networking in the United States Army" (Army War College, 2011), 10–11, http://www.dtic.mil/dtic/tr/fulltext/u2/a559960.pdf.
[30] "AFI90-802_AFGM2016-01," 12–13.

Risk Model Setup

> *For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations.*
>
> *The National Strategy for Cyber Operations*
> *Office of the Chairman, Joint Chiefs of Staff*
> *U.S. Department of Defense*
> *September 2012*

Risk assessment is one of the fundamental components of an organizational risk management process.[31] The risk management process is a continuous decision-making process, which includes identifying, assessing, mitigating, deciding, and evaluating potential hazards and vulnerabilities to an organization.[32] Leaders conduct risk assessments to inform long-term system-wide risks or specific short-duration activities. In many cases, military organizations classify risks to personnel, mission, capability, and reputation to identify their impact. Two key formulas will guide the assessment of social media risks and enable further analysis of potential threat events. The first identifies threat events.

Threat Event = Vulnerability + Threat Actor [33]

The formula illustrates that for a threat event to occur, there must be a vulnerability and a threat actor with the capability and intent to exploit the vulnerability. A threat event is a source of potential harm or a situation with a potential to cause loss. A vulnerability is a weakness in the organization, and a threat actor is an agent that has the capability and intent to exploit the vulnerability. For instance, a vulnerability alone is

---

[31] Rebecca Blank, "Information Security: Guide for Conducting Risk Assessments" (National Institute of Standards and Technology, September 2012), 1, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
[32] Blank, "Information Security: Guide for Conducting Risk Assessments," 1.
[33] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford ; New York: Oxford University Press, 2014), 37–38.

akin to leaving the front door unlocked when leaving the house. It may remain that way indefinitely without creating a threat event. When a threat actor walks through the unlocked door, a threat event occurs. Moreover, one vulnerability may lead to different threat events. A criminal may walk inside and steal the television, or an arsonist may burn down the house. An actor's objective separates them from other actors and assists in identifying and measuring organizational risk.[34] The second formula utilizes the threat event that was determined from the first and measures the likelihood and consequence of it occurring.

Resultant Risk = Likelihood (Threat Event) x Consequence [35]

A risk is a product of the likelihood of an event happening, and the consequences, should it occur.[36] Figures 3 and 4 are examples of how an organization assigns definitions to likelihood and consequence. The model will utilize both formulas to analyze a spectrum of potential social media risks and their impacts on military organizations. The next section utilizes the first formula to identify potential threat events.

[34] Singer and Friedman, *Cybersecurity and Cyberwar*, 2014, 38.
[35] Royal Australian Air Force, "Air Force Safety Manual" (Commonwealth of Australia, January 20, 2016), pt. 1 section 2 chapter 8. The author utilized the definitions to create the formula.
[36] "AFI90-802_AFGM2016-01," 29.

Social Media Vulnerabilities

Threat Event = **Vulnerability** + Threat Actor

The *SANS Institute Social Media Risk Assessment Report* provides an in-depth analysis of social media risks and vulnerabilities. Figure 1 classifies each vulnerability according to content management, information leakage, Twitter and Facebook.

Content Management	**Information Leakage**	**Twitter & Facebook**
Reputation, Brand, Representation	Data Loss *Classified or Sensitive Information	Scams/Viruses
Control *Classified or Sensitive Information	Privacy *Personal Identifiable Information (PII)	Shortened URL
Privacy *Personal Identifiable Information (PII)	Intellectual Property/Copyright	Malware/Phishing
Intellectual Property/Copyright	Location Information	Misplaced Trust
Stale or Outdated Sites		
Location Information		
Archiving		

Figure 1: Social Media Risk Categories
Source: Adapted from SANS Institute Social Media Risk Assessment Report

***** Added for military context

Content Management

Social media allows the instant exchange of information on publicly accessible sites by employees and the online public. Without information security policies, education, training, and awareness the type of information disclosed may present a vulnerability to the organization. Organizations quickly lose control of the information due to terms of service clauses or the potential for information sharing amongst users.[37] The loss of control or release of sensitive information may have adverse outcomes to the organization's reputation, personnel, capabilities, and mission. Furthermore,

[37] Adrian Bejar, "Balancing Social Media with Operations Security in the 21st Century" (Naval War College, 03May, 2010), 12.

organizations are also subject to specific laws and regulatory compliance. Privacy law, including the release of personally identifiable information (PII), is one such law that requires detailed policy. Adversaries exploit information defined as PII to distinguish or trace an individual's identity, such as his or her name, social security number, and home address. Due to the public nature of the sites, many organizations control the content of the information released by restricting the settings of each site and stipulating who can access it and what information those users may release. Regardless, social media administrators could leak information accidentally due to inadequate policy and training.

Information Leakage

Information leakage is "a breach of the confidentiality of information, typically originating from staff inside an organization and usually results in information being disclosed in the public domain."[38] Two types of leakage originate from both malicious and non-malicious insiders. Malicious insider activity is outside the scope of this study; however, it is conceivable that malicious insiders may release information on official social media sites. The non-malicious and accidental release of sensitive or classified information, which originates from well-intentioned personnel, is more likely to present a vulnerability to an organization.[39] Concerned organizations often develop governance and management procedures to review the sites and minimize exposure.[40]

Twitter and Facebook

Facebook and Twitter are the dominant platforms the USAF employs for official social media.[41] The networking sites encourage interaction by allowing users to comment on the posts. The comments section provides an opportunity for members of the public to express negative, harassing, derogatory, and threatening comments. Furthermore, social

---

[38] Molok, Chang, and Ahmad, "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," 70.
[39] Molok, Chang, and Ahmad, "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," 73.
[40] Molok, Chang, and Ahmad, "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," 72.
[41] USAF, "U.S. Air Force Social Media" (Air Force Public Affairs Agency, Addition 2013), http://www.af.mil/Portals/1/documents/SocialMediaGuide2013.pdf.

media sites may be hijacked, as well as targeted with viruses, scams, malware, and shortened URLs.

Threat Actor

Threat Event = Vulnerability + **Threat Actor**

In 2016, the Center for Cyber and Homeland Security released a report that categorized emerging cyber threats as nation-states and their proxies, foreign terrorist organizations, criminal groups, and hacktivists.[42] These actors frame the discussion and analysis regarding threat events in the model. When deciding on social media threat events, it is important to describe the threat actor, their objectives, capabilities, and the intent to exploit each vulnerability.[43]

Nation States (State sanctioned, State sponsored, and State supported)

Nation-states and their proxies continue to present the most advanced and persistent threat (APT) in cyberspace.[44] An APT is a coordinated group with sophisticated levels of expertise, significant resources, and funding. These characteristics create opportunities to achieve their objectives by using multiple attack vectors (e.g., cyber, physical, and deception). APTs target sensitive and classified information to secure a strategic advantage in areas such as defense technologies, foreign government policy, and a wide range of industry data. States may engage in activities such as online espionage, disinformation, theft, propaganda, and data destruction. [45] Each state has different capabilities and intent to conduct these operations. States also have the capability to pursue collection activities outside of the cyber domain.

Criminal Organizations

Criminal organizations possess substantial capabilities to perform nefarious activities in cyberspace. Financial gain usually drives criminal organizations' objectives. The most pervasive type of cyber crime is credential fraud or the misuse of account

[42] Cilluffo, "Emerging Cyber Threats to the United States," 3.
[43] Cilluffo, "Emerging Cyber Threats to the United States," 2.
[44] Cilluffo, "Emerging Cyber Threats to the United States," 3.
[45] Cilluffo, "Emerging Cyber Threats to the United States," 4.

details to defraud financial and payment systems including credit cards, ATM accounts, and online banking accounts.[46] Typical attacks are designed to obtain security credentials like passwords and personal information by employing phishing, malware, clickjacking, and linking to fake websites.[47]

Foreign Terrorist Groups

The new media landscape is ripe for terrorist activities because it provides a globally connected audience. The ability to connect across geographic boundaries; to create, share, and exchange information; and to exploit a broad audience enables terrorist organizations to pursue their objectives.[48] Acts of terrorism play out to an audience to intimidate or inspire.[49] Terrorist groups use the Internet and social media networks for four main reasons: 1) propaganda, radicalization, and recruitment; 2) share operational and tactical information; 3) target potential members and followers; 4) remote reconnaissance for targeting purposes.[50] While foreign terrorist organizations are yet to develop a sustained cyber-attack capability, they continue to search for and publish private or identifying information to target military personnel.[51] A report by the Director of National Intelligence to the Senate Armed Services Committee stated, "In a new tactic, ISIL actors targeted and released sensitive information about US military personnel…in an effort to spur lone wolf attacks."[52]

---

[46] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015), 92.
[47] A victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details. Phishing is a homophone of fishing, which involves using lures to catch fish. (9http://searchsecurity.techtarget.com/definition/phishing)
[48] John Arquilla, David F. Ronfeldt, and United States, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: Rand, 2001), 77.
[49] Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, 1. paperback print (Princeton: Princeton Univ. Press, 2011), 7.
[50] Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington, D.C., New York : Columbia University Press: Woodrow Wilson Center Press, 2015), 128.
[51] Cilluffo, "Emerging Cyber Threats to the United States," 2. This type of activity is known as doxing tactics.
[52] James Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Armed Services Committee, February 9, 2016, 3, https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

Hacktivists and Other Entities

The term "hacktivist" represents the blending of the two words, "activist" and "hacker." The objective of the hacktivist is to promote or resist a political or social change through non-violent, but often legally questionable cyber means of protest.[53] The objectives often relate to free speech, human rights, or freedom of information. Social media networking provides a platform to message, deface, or hijack accounts to fulfill these objectives. A group named Anonymous is an example of a hacktivist group. Anonymous is a group of hacktivists with no central leader, who are frustrated by inequality, war, corruption, national politics, environmental destruction, and religious irrationality.[54] One member of the group described their actions as "ultra-coordinated motherfuckery."[55] The comment illustrates the groups disregard for social norms and civil discourse. Threat actors in cyberspace fall into one of these four groups and each actor is defined by the objective it is attempting to achieve. The USAF has developed policies, training, and guidelines in an attempt to eliminate, mitigate, and control the vulnerabilities and threat actors identified thus far.

Risk Mitigation

Akin to traditional media, the USAF limits the release of information on their official social media sites by restricting the administration of accounts to its authorized and trained personnel (e.g. public affairs and commanders). Many existing USAF policies and training courses assist in controlling content and information leakage risks. The employment of these policies attempts to reduce the number of threat events. Appendix B details a summary of USAF policy for the readers unaware of USAF risk mitigation of social media. In summary, the vulnerabilities, threat actors, and mitigations discussed thus far will inform the risk model presented in the next section, and in doing so, illustrate a range of social media risks.

---

[53] Singer and Friedman, *Cybersecurity and Cyberwar*, n.d., 77.
[54] Anonymous, "Anonymous Explains It's Objectives," YouTube, 07 February 2012, https://www.youtube.com/watch?v=WSNbImxjK3E.
[55] Singer and Friedman, *Cybersecurity and Cyberwar*, 2014, 82.

Risk Model

The model employed in this article identifies a spectrum of common risks introduced when organizations engage in social media. The outcome of each risk facilitates analysis and discussion regarding organizational risk acceptance of social media. The assessment will refer to the top two official social media sites that the USAF employs: Facebook and Twitter.[56]

Framework

The model utilizes the International Organization for Standardization (ISO) 31000 risk assessment framework illustrated in Figure 2.[57] ISO 3100 is a 5 x 5 matrix that contrasts the likelihood of an event occurring, against the consequence to determine the risk.[58] The 5 x 5 matrix provides a very high, high, medium, low, and very low-risk ranking. While comparative to the USAF Risk Management 4 x 5, it offers additional fidelity by increasing the scope of classification to five possible outcomes.

AFPAM90-803 identifies that the USAF matrix suffers from a small scope in ranking that produces only four results, extremely high, high, medium, and low risks.[59] The Air Force pamphlet illustrates that most risks fall within high or medium because extremely high will most likely be corrected, and the low is often so minor that it does not warrant serious consideration.[60] Therefore, the majority of hazards are either high or medium, which creates a prioritization dilemma when trying to discriminate between the two. The 5x5 model provides an option to overcome the dilemma by the addition of another risk outcome to discriminate between the high and medium residual risks.

---

[56] USAF, "Social Media." Facebook (598), Twitter (232), Instagram (30), LinkedIn (2).
[57] John Lark et al., *ISO31000: Risk Management: A Practical Guide for SME's* (International Organization for Standardization, 2015).
[58] For audiences outside of the U.S., The So Far as Reasonably Practicable (SFARP) functionality will not be illustrated to keep the U.S. and ISO matrix to ensure utility within the USAF risk management framework.
[59] "AFI90-802_AFGM2016-01," 16.
[60] Air Force Pamphlet 90-803, 108.

	Consequence				
Likelihood	**Minor**	**Moderate**	**Major**	**Critical**	**Catastrophic**
Frequent/Almost Certain	**L**	**M**	**H**	**VH**	**VH**
Probable/Likely	**L**	**M**	**H**	**H**	**VH**
Occasional	**VL**	**L**	**M**	**H**	**H**
Improbable/Seldom	**VL**	**VL**	**L**	**M**	**M**
Rare/Unlikely	**VL**	**VL**	**VL**	**L**	**L**

Risk Level	VL	Very Low	L	Low	M	Medium	H	High	VH	Very High

Figure 2: Assessment Scale: Overall Likelihood
Source: Adapted from ISO 3100 Risk Management

Military organizations utilize Figure 3 and 4 to assess the likelihood and consequence of a threat event. Each category informs the resultant risk in Figure 2. Figures 3 and 4 illustrate a combination of RAAF and USAF organizational risk management descriptions. The modeling in this assessment will utilize these classifications to measure the resultant risk to each threat event. Consideration of the adversary's capabilities, intent and objectives become necessary when considering the likelihood of a threat event occurring.

Likelihood	Description
Almost certain (Very High)	The adversary is almost certain to initiate the event. Is known to occur frequently in similar activities.
Probable (High)	The adversary is highly likely to initiate the event. Is known to have occurred previously.
Occasional (Moderate)	The adversary is somewhat likely to initiate the event. Sporadic but not uncommon.
Improbable (Low)	The adversary is unlikely to initiate the event. Occurrence conceivable but considered uncommon.
Rare (Very Low)	The adversary is highly unlikely to initiate the event. The occurrence is conceivable but not expected to occur.

Figure 3. Likelihood of Threat Event Initiation
Source: Adapted from RAAF/USAF Risk Management Definitions

Consequence	Definition
Catastrophic	**Personnel:** Multiple fatalities OR 10 or more injuries/illnesses categorized as 'Critical.' **Mission:** Failure to achieve a mission that is essential to a strategic objective. **Capability:** Indefinite loss of military capability provided by a core system. Loss of single asset of significant strategic value **Reputation:** Widespread public condemnation of the military. Long-term media condemnation or formal inquiry.
Critical	**Personnel:** Single fatality and permanent total disability OR 10 or more injuries/illnesses categorized as 'Major.' **Mission:** Failure to achieve an essential operational objective with significant strategic implications. **Capability:** Long-term degradation to military capability. **Reputation:** Widespread public discontent with service, prolonged adverse national media attention or government investigation.
Major	**Personnel:** Serious injury or illness requiring immediate admission to hospital as an inpatient and permanent partial disability OR 10 or more injuries/illnesses categorized as 'Moderate.' **Mission:** Failure to achieve an important operational objective with serious unit/tactical implications. **Capability:** Temporary loss or temporary severe degradation to Defense capability. **Reputation:** Negative reaction by public interest groups and short-term national media attention.
Moderate	**Personnel:** Injury or illness is causing no permanent disability, which requires non-emergency medical attention by a registered health practitioner OR 10 or more injuries/illnesses categorized as 'Minor.' **Mission:** Failure to achieve an important operational objective with significant unit/tactical implications. **Capability:** Temporary substantial degradation to the Military capability provided by a core system.

	Reputation: Local prolonged media attention and negative public reaction.
Minor	**Personnel:** Minor injury or illness that is treatable in the workplace (first aid) or by a registered health practitioner, with no follow-up treatment required. **Mission:** Partial achievement of a mission with unit/tactical implications but does not affect an operational objective. **Capability:** Temporary degradation to the Military capability provided by a core system. **Reputation:** Local short-term media attention and negative public reaction.

Figure 4. Consequence of Threat Event
Source: Adapted From RAAF/USAF Organizational Risk Management Tables

Limitations

This article is unclassified; therefore the modeling - the framework, examples, and vulnerabilities - are unclassified. The threat actors and their capabilities are general in nature. An unclassified article is advantageous when discussing common organizational vulnerabilities and risk in social media. However, using classified information would permit a deeper dive into network security mitigations and counter-cyber-attack capabilities.

Risk management is an iterative process. The SANs Institute Reading Room released *The SANs Institute Social Media Report* in 2011.[61] Since then, additional vulnerabilities, such as face recognition software, have become apparent. However, the model is limited to the vulnerabilities identified in the report. Regardless, commanders should update the risk management process when they identify additional vulnerabilities and threat actors.

Analytic Approach

The model supports either a threat actor-orientated approach or vulnerability-orientated approach. The starting point defines the difference between the two approaches. A threat actor-orientated approach begins with the identification of a threat actor and focuses on their capability and intent. A vulnerability-orientated approach starts with a vulnerability or set of exploitable weaknesses.[62] It then assigns likely threat actors that may exploit the vulnerabilities.[63] Both approaches are complementary to risk analysis when considering social media. On the one hand, a threat actor approach may uncover new vulnerabilities by analyzing the actor's capabilities. On the other hand, a vulnerability approach may eliminate vulnerabilities, and in doing so, reduce multiple threat actors. Appendix C illustrates the process. This study will utilize a vulnerability-oriented approach framed by the vulnerabilities represented in Figure 1. A threat-orientated approach is outside the scale and security classification of the study because it

[61] Shullich, "Risk Assessment of Social Media."
[62] Blank, "Information Security: Guide for Conducting Risk Assessments," 15.
[63] Blank, "Information Security: Guide for Conducting Risk Assessments," 15.

requires identification of specific capabilities of threat actors. To explore the vulnerabilities pertinent to the USAF, the model examines both defense and attack.

The defense section of this article describes a vulnerability analysis of USAF official social media sites. It measures the effectiveness of USAF policy, guidelines, and training by analyzing a random selection of 50 USAF official Facebook and Twitter accounts. The analysis spans a one-year period from February 2016 to February 2017. Appendix E tables the results of the analysis.[64] The vulnerabilities and threat actors identified in the defense section inform the threat events in the attack section. The attack section utilizes the threat events and applies them to the risk model by measuring the likelihood and consequence of the event occurring. The attack analysis describes how different adversaries exploit these vulnerabilities, and, in doing so, identifies the residual risk that the USAF is accepting. Next, the author explains a simple analysis to guide the readers through the study.

[64] Appendix E: Vulnerability Analysis of USAF Social Media

Threat Events and Risk Modeling

NO	Objective	SANS Institute Vulnerabilities	Threat Actor	Threat Event	Existing Controls	Risk Overview	Organizationally Defined Consequence - Impact		Likelihood (after mitigation)	Residual Risk Level
2	Website Disruption	Comments Section	Internet Trolls	Internet Trolls make inflammatory, extraneous, or off-topic messages in comments section	Personnel Assigned to Monitor Site, Behavior Terms, USAF Flowchart, Crisis Management Training	Inflammatory Comments	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Low
						Website Disruption, Interrupted	Capability	Minor		Low
						Discussion	Reputation	Minor		Low

Figure 5. Risk Modeling Example
Source: Authors original work

Appendices F and G explain the complete list of threat events assessed in this study. Figure 5 provides a snapshot of one event to illustrates how the author employs the formulas and risk definitions to determine threat events and analyze the residual risk. First, the threat event.

Threat Event = Vulnerability + Threat Actor

Vulnerability. As discussed within the analytic approach section, a vulnerability-oriented approach begins with an identified vulnerability. The SANs Institute Social Media Report identified that the *comments section* of social media sites facilitates two-way interaction between the public and the organization. While the conversation stimulates participation, it also presents a vulnerability, which threat actors exploit.

Threat Actor. Security analysts define threat actors by their objectives, capabilities, and intent. The emerging cyber threat actors discussed thus far are nation-states and their proxies, foreign terrorist organizations, criminal groups, and hacktivists. In this instance, all threat groups possess the capability to write messages in a comments section on an organization's social media page. Leaders may assess the risk of each threat actor against the vulnerability creating four separate threat events.

Many analysts will look to reduce the number of events based on their assessment of the adversary's objectives against the vulnerability. For example, nation states conducting espionage activities or criminals looking for financial gain may be considered unlikely to exploit a comments section of a military organization. Therefore, the analyst removes the adversaries from the modeling. On the contrary, analysts may look to include foreign terrorist organizations and hacktivists that intend to message, harass or

embarrass the military organization by commenting on their sites. Figure 5 details the threat actor to be an *Internet troll*.[65]

Risk Overview and Mitigations. Internet trolls regularly comment within the new media environment. It is common for users of social media to see the comments of internet trolls that disrupt conversations, start arguments, and post inflammatory, extraneous, or off-topic messages. Their intent is to provoke an emotional response often for their amusement. Figure 5 illustrates that the USAF mitigates the risk by 1) assigning personnel to monitor the site; 2) establish behavior expectations on the site; 3) provide a USAF flowchart to assist making decisions about comments; 4) provide training for site administrators in crisis management.

Threat Event. When an *Internet troll* exploits a *comment section* with the intent to deface or interrupt the conversation, a threat event occurs.

Resultant Risk = Likelihood (Threat Event) x Consequence

Likelihood and Consequence. To model the risk to the military organization's personnel, mission, capability, and reputation, the leader utilizes existing organizational controls and employs Figure 3 and 4 to assess the likelihood and consequence. Given the threat event, and mitigations, the author assesses the likelihood (Figure 3) as '*almost certain*.' Furthermore, the consequence (Figure 4) describes the impact to the USAF's personnel (*minor*), mission (*minor*), capability (*minor*), and reputation (*minor*).

Resultant Risk. Figure 2 utilizes the assessment of the likelihood (*almost certain*) and the consequence (*minor* in all cases) to inform a residual risk level of *low*. Leaders may add additional controls to minimize the risk further, or accept the risk and move on to the next threat event.

Social Media Schools of Thought. Each school of thought may influence the judgment of leaders utilizing the model. It is common for leaders to assess the likelihood and consequence as higher when adverse to the activity, or lower when encouraging the activity. Regardless, risk management informs decision making. It is not designed to

[65] An Internet troll is a person whose purpose is to seek out people to argue with over extremely trivial issues.

make the decision. The risk management process and the schools of thought presented in this analysis should highlight any potential bias to the leaders making the decision. The model also provides a framework for commanders to discuss social media risks.

The model setup and explanation is complete. The defense and attack phase utilizes the framework and analytic approach, mentioned thus far, to measure the residual risk to the USAF's employment of social media.

Defense Analysis

The author analyzed fifty official USAF Facebook and Twitter sites over a one year period. The assessment measured the effectiveness of the USAF social media mitigations against the vulnerabilities identified by the SANs Institute Social Media Risk Report. Appendix E details the results of the vulnerability evaluation.

The results indicate that commanders and their staffs closely follow USAF policies when releasing information on official social media.[66] The analysis found no trace of PII leakage including home addresses, SSNs, email addresses, telephone numbers, or family information.[67] Furthermore, the analysis found no video or photo meta-data, including location information, although Twitter and Facebook remove metadata from photos and videos to avoid targeting of personnel.[68] Therefore, the information distributed on USAF official social media sites regarding PII is insufficient for cybercrime activities without further aggregation of personal information.[69]

The analysis indicated no classified/sensitive documents or further breaches in operational security regarding capabilities or missions.[70] The main reason for this is that the USAF hosts official social media on the unclassified DoD network. It is air gapped from higher classification networks making it difficult for accidental information leakage of classified documents.[71] However, minor operational security breaches were apparent. The analysis identified targetable information regarding troop movements for off-base social activities and events.

The analysis illustrated no information that risks USAF's reputation.[72] The information released on official social media sites represented a thoughtful and considered approach from commanders and their staff. While there was a limited number

---

[66] Appendix E: Vulnerability Analysis of USAF Social Media. Airmen's name and rank are releasable by the USAF, given the airmen's consent IAW USAF PII policy in Appendix B.
[67] Appendix E: Vulnerability Analysis of USAF Social Media.
[68] Sin Mei, "Why Facebook and Twitter Are Stripping Out Your Context," *Sentiance*, October 11, 2013, https://www.sentiance.com/2013/10/11/facebook-twitter-stripping-context/. Both companies reserve the right to release this information based on their terms of service.
[69] An Airman's picture and name may be captured for identity theft or building trust relationships in the future. The practice requires aggregated information.
[70] Appendix E: Vulnerability Analysis of USAF Social Media.
[71] Richard A. Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 64–65.
[72] Appendix E: Vulnerability Analysis of USAF Social Media.

of videos that showed the targeting and bombing of ISIS buildings, these formed a part of approved information operations campaigns.[73] The comments from the public largely supported these videos, although there appeared to be a fine line between support and disapproval from the public. In addition to reputation vulnerabilities, there were no legal vulnerabilities (copyright, intellectual property, etc.).

The analysis found three additional vulnerabilities to the SANS vulnerability table in Figure 1. First, many of the USAF's posts release airmen's names. The USAF publishes airmen's names, which may become a vulnerability when aggregated with other personal information from other sites. The author clicked on the names of airmen (or their family members that had made a comment or 'liked' a post) to gauge a level of vulnerability. A few members had open (non-private) social media accounts that exposed the member's personal information.[74] Second, the "friends list" on Twitter presents a similar vulnerability. Many of the official sites were 'followed or friended' by military personnel. By following the military organization, airmen create a link to their personal social media site that may be exploited by adversaries. Third, the comment section within official social media sites provides an avenue for adversary messaging. In some cases, the comments were negative or derogatory. USAF policy requires monitoring of the official sites and treats undesirable messaging as stated in Appendix D.

The USAF mitigations are successful in reducing many of the vulnerabilities identified in the SANS Institute report. Figure 6 consolidates the exploitable vulnerabilities and attack vectors identified in the defense section. The vulnerabilities listed in white require further analysis. The following section provides a summary of the attack analysis.

---

[73] Appendix E: Vulnerability Analysis of USAF Social Media.

[74] The author is aware that the aggregation of unclassified information disclosed through official social media sites creates an opportunity for threat actors to conduct surveillance, gather intelligence, and craft unique cyber and "real world" attacks. While the organization may accidently release information, it is the aggregation of unclassified information through reconnaissance that is the most difficult to mitigate.

Remaining Vulnerabilities

Content Management	**Information Leakage**	**Twitter & Facebook**
Reputation/Brand/Representation	Data Loss *Classified or Sensitive Information	Hijacking
Control *Classified or Sensitive Information	Privacy *Personal Identifiable Information (PII)	Shortened URL
Privacy *Personal Identifiable Information (PII) **Names/Rank Only**	Intellectual Property/Copyright	Malware/Phishing/ Scams/Viruses
Intellectual Property/Copyright	Location Information	-Unprotected Friends List (Twitter)
Censorship	Personnel targeting for individuals or groups	Aggregation of Unclassified Information
Stale or Outdated Sites	List of Friends/Family Comments/Employee Comments	
Location Information		
Archiving (Regulatory) Resource/ Not Measured		
Comments section		

Figure 6: Remaining Vulnerabilities
Source: Adapted from SANS Institute Social Media Risk Assessment

Attack Analysis and Evidence

The attack phase introduces threat actors to exploit the vulnerabilities identified thus far. By utilizing the model, it discusses the resultant risk that the USAF accepts when engaging in social media. Figure 7 summarizes the comprehensive threat matrix compiled in Appendix F.[75] The threat matrix identifies the residual risk from each threat event. In addition to the residual risk, an assessment of the unmitigated risk is included to highlight the effectiveness of the USAF's risk mitigation strategy. Figure 7 provides the basis for analysis and discussion regarding social media risks.

[75] Appendix F: Threat Event Table 1-8Appendix G: Threat Event Table 9-14

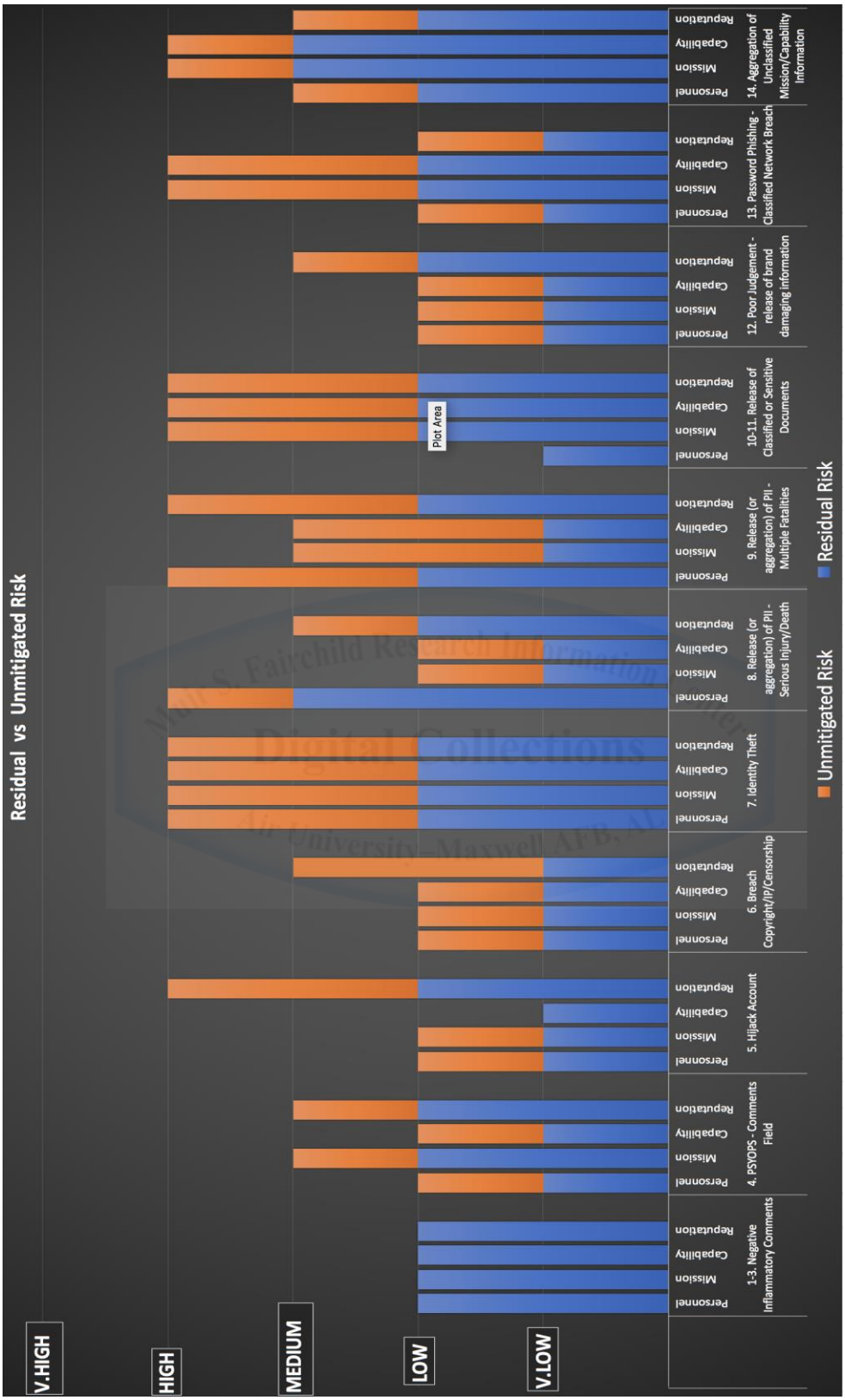


Figure 7: Mitigated vs. Unmitigated Risk
Source: Authors original work

Comments Section

Threat Events 1-3

Social media facilitates two-way interaction and conversation with the community. While the conversation stimulates participation, it also presents a vulnerability ripe for exploitation. The modeling in Appendix F identified that members of the public, cyber trolls, and issue motivated groups are almost certain to exploit the vulnerability by disrupting conversations, signposting information and harassing the online audience. However, the USAF assigns personnel to monitor the social media sites and remove unwanted comments thereby limiting exposure. The author assesses the organizational consequence to be minor regarding personnel, capability, mission and reputation. Therefore, the model describes a low resultant risk to personnel, mission, capability, and reputation.

Threat Event 4

Terrorist organizations exploit the same vulnerability as trolls, issue motivated groups, or those with the desire to exploit the comment section. In 2011, in a hearing before the Committee on Homeland Security House of Representatives, Mr. Meehan, chairman of the subcommittee, stated that;

> The same place where the average person posts photos and communicates with family and friends are being used by enemies to distribute videos. Terrorists also disseminate diatribes glorifying the murder of innocents and even make connections with each other intentionally or internationally to plot attacks.[76]

By the very character of terrorist messages, the risk to the organization's reputation may increase depending on local and national media attention. Should the comments garner local media or national attention, the risk would rise to medium and most likely require a

[76] Patrick Meehan, "Jihadist Use of Social Media - How to Prevent Terrorism and Preserve Innovation" (Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives presented at the Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives, Washington, D.C, December 6, 2011), https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm.

response from the organization. The comments may be shared and go viral before they are taken down by administrators, which may have a similar effect.

While the comment field represents a vulnerability in official social media sites, exploiting it also offers an opportunity to re-engage the adversary. By engaging on social media, these groups create a digital footprint that provides cyber organizations an attack vector to exploit. Reporting the incident to counterterrorism units may permit state based capabilities like social network analysis, targeted information operations, and the use of state-based capabilities outside of the cyber domain. Militaries have reported these instances of social media abuse to Facebook and Twitter in an attempt to close the accounts. However, the "whack-a-mole" response has proven futile because the groups make new accounts in minutes.[77] Therefore, militaries have switched to utilizing counter-narratives. For example, when a Taliban spokesperson tweeted "@isafmedia continue genocide of Afghans: ISAF terrorists beat defenseless man to death," ISAF quickly replied, "Sorry @ABalkhi: looting and beating innocents are NOT part of ISAF practices during routine searches."[78] Adversaries have also employed tactics to hijack social media accounts to control a narrative and embarrass an organization.

Hijack Account

Threat Event 5

Adversaries hijack official social media accounts to demonstrate a level of control or to embarrass military organizations. Hijacking social media accounts allows the adversary to conduct uninterrupted messaging until the account is shut down by the account owner or social media platform. The most likely adversaries are hacktivists and foreign terrorist organizations. For example, ISIS sympathizers hijacked the U.S. Central Command Twitter account in January 2015. The group changed the background pictures to black ISIS style insignias with a tweet that read, "In the name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate continues its CyberJihad…American soldiers, we are coming, watch your back…We won't stop! We know everything about

[77] Clarke and Knake, *Cyber War*, 171. Twitter has closed 25,000 accounts that supported the terrorist organization ISIS.
[78] Weimann, *Terrorism in Cyberspace*, 141.

you, your wives and children."[79] The group posted the names, telephone numbers, and home addresses of U.S. military officials. The DoD responded by closing the account forty minutes later.

The hijack embarrassed the DoD and demonstrated a heightened risk to reputation and personnel. The feed played out across most major news networks across the U.S. The model defines the reputational impact of short-term national media attention as a 'major' consequence.[80] Also, the event required a response from the DoD, White House senior leaders, and public affairs staff. [81] The incident demonstrates a potentially high risk without further mitigations by the USAF.

At the time, the CEO of the Center for Internet Security, Will Pelgrin, argued that a common vector to exploit and hijack a social media account is through the login process. Hackers take advantage of account owners who use weak passwords or the same password on multiple sites. One study reported on hacked websites found that 49% of people had reused usernames and passwords between hacked sites.[82] In addition to this vulnerability, another attack vector may be to craft phishing attacks to garner passwords from official social media account users. As a result, Twitter and Facebook have introduced additional security to mitigate account hijacking, such as two-factor authentication.[83,84] While the risk to reputation remains high, the additional security measures reduce the likelihood of the threat event occurring. Therefore, the model indicates a low residual risk for account hijacking.

---

[79] Justin Brown, "What the Centcom Twitter Hack Means to You," *Government Technology*, 23Jan2015, http://www.govtech.com/security/What-the-CentCom-Twitter-Hack-Means-to-You.html.
[80] For example, with CNBC, CNN, Fox News, The Guardian.
[81] The author accepts that there is a large cost to the organization regarding productivity and response required from the DoD/White House public affairs and senior leaders.
[82] Singer and Friedman, *Cybersecurity and Cyberwar*, n.d., 243.
[83] Barrett Brian, "Time to Lock Up Your Twitter Account with Two-Factor," *Wired Magazine*, June 9, 2016, https://www.wired.com/2016/06/twitter-hack/. In 2016 hackers released 32 million of Twitter credentials (username and password). Twitter and Facebook now offer two-factor identification.
[84] Two Factor Authentication, is an extra layer of security that is also known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token, or a code sent to a cell phone.

Breach of Copyright / Intellectual Property

Threat Event 6

The defense analysis showed no breach of copyright or intellectual property in USAF social media sites. USAF mitigations are sufficient to prevent the threat event from occurring. Therefore, the likelihood and consequence of a breach produce a low organizational risk.

Aggregation of PII

Threat Events 7, 8 and 9

There is a potential for aggregated personal information collected from personal and official social media sites to affect the personnel, mission, capability, and reputation within a military organization. While the analysis outlined in the defense section suggests that commanders and public affairs staff are successful in limiting the release of PII, USAF policy permits the release of an airman's name, photos, and videos.[85] Adversaries aggregate airmen's names found on official social media sites, with other open (or closed) sources to complement targeting activities. Military members, "unwittingly post detailed information about themselves, their careers, family members, date of birth, present locations, and photos of colleagues and weaponry" that facilitate targeting.[86] Adversaries mine the Internet for PII through techniques such as web crawling programs, trust relationships, and malware. The adversarial risks to personnel include harassment, identity theft, blackmail, personal injury, and death.

In 2008, the domestic security service MI5 released a flash message to all British service personnel to remove their personal details from social media sites. They encouraged family and known associates to do the same. British cyber-analysts reported that al-Qaeda operatives had been conducting reconnaissance that they could use to launch terror attacks.[87] In 2015, similar reports of observation took place originating from

---

85

AFI 35-104 - Media Operations

86 Weimann, *Terrorism in Cyberspace*, 134.

87 Weimann, *Terrorism in Cyberspace*, 134.

a group called Islamic State Hacking Division.[88] The team posted names, photos, and addresses of approximately one hundred U.S. troops. The group appealed to their "lone wolves" in the U.S. to attack the military personnel.[89] DoD officials stated that the information was piecemeal, dated, and gathered from open sources rather than official networks.[90] The DoD's comments focused on network security and overlooked the impact that the organization's use of social media plays toward the aggregation of PII.

The link that official social media makes between the individual and the organization, either by releasing names or mining the "friends list" remains a concerning aspect of social media. The analysis shows that it has the potential to incur a very high risk to airmen, their families, and the organization.[91] However, the likelihood of a terrorist group targeting (killing) an airman, a group of airmen, or their families using information collected from official social media remains rare.[92] Therefore, the overall risk to the organization is low. Most intelligent observers, at this stage, may correctly identify the limits of risk management in that it is not predictive, and they are right. The potential for adversaries to collect enough information from social media to take actions to injure or kill airmen marks the point of divergence for each school of thought.

The zero-tolerance school of thought views the threat event as an unnecessary risk because it is extremely tough to limit the aggregation of organizational and personal release of PII. Therefore, the school calls for organizations to disengage from social media to reduce actionable PII. Zero tolerance argues that reducing the digital footprint will increase the level of capability required for adversaries to find the information required to target individuals and their families. Similarly, the traditional media school agrees, but accepts a small organizational footprint that includes airmen's names. The

---

[88] Evan Bleier and Christopher Brennan, "A Hundred American Soldiers Named on ISIS 'Kill List' - but Servicemen Say They Are 'Unfazed by Extremists' Threats," *Daily Mail*, March 23, 2015, 1.
[89] Bleier and Brennan, "A Hundred American Soldiers Named on ISIS 'Kill List' - but Servicemen Say They Are 'Unfazed by Extremists' Threats," 1.
[90] Bleier and Brennan, "A Hundred American Soldiers Named on ISIS 'Kill List' - but Servicemen Say They Are 'Unfazed by Extremists' Threats," 2.
[91] Appendix G: Threat Event Table 9-14
[92] David Benson, "Why the Internet Is Not Increasing Terrorism," *Security Studies* 23, no. May 2014 (May 2014): 313-315. The article discusses home-grown and transnational terrorist examples and argues that the internet does not increase terrorist attacks.

small footprint enables the organization to tell their story and educate the public about the military's activities while reducing the risk of a larger footprint.

Conversely, advocates of the new media school accept the risk and point to the wider objectives of terrorists and criminal adversaries. They state that it is easier, and more effective, for a foreign terrorist to randomly select military personnel and their families in public than to coordinate an attack from aggregated PII information. Lastly, the information dominance school accepts the risk to personnel based on the requirement to dominate the domain and narrative. While the school may fall short of stating that it is the 'cost of doing business,' the focus is on achieving the mission. The author concedes that the aggregation of PII may lead to adversaries targeting airmen and their families in the future; however, each school makes a strong case to influence risk acceptance within the organization. Perhaps a more pertinent question should be asked: who is responsible for a risk?

Adversaries collect PII across a wide variety of sites. Therefore, the USAF, airmen and their families/friends share the risk accordingly. The USAF seeks to inform the airmen and their families of the risks by issuing pamphlets and by conducting annual training. The USAF also gains verbal consent from an airman within their command, or written consent for airmen (or other personnel) outside of their command to release their names. The USAF seeks written consent from people outside of the organization, (e.g. family or friends).[93] Therefore, airmen share the responsibility to protect their PII, whether it be on social media or the Internet or in the phone book.

In recognition of these threat events, some commands within the USAF place additional controls on the release of airmen's names and photos.[94] Removing names of personnel may prove beneficial in lowering the risk against low-capability actors that mine information. For instance, the public affairs department in Air Force Special Operations Command (AFSOC) does not release names of personnel and are sensitive to the types of photo and video it uses.[95]

---

[93] Kayshel Trudell, Special Operations Wing Public Affairs Office Interview, Telephone, March 28, 2017.
[94] Trudell, Special Operations Wing Public Affairs Office Interview.
[95] Trudell, Special Operations Wing Public Affairs Office Interview.

Regardless, if airmen or their families follow the organization as "friends" or if they comment on the sites, they may still expose themselves to adversaries. It appears that foreign terrorist organizations are intimately aware of this risk. A jihadi forum member issued a warning regarding the vulnerability of "friends lists" and networks by stating, "Don't make a network on Facebook…Then Kuffar will know every friend you have or had...They will know your location, how you look, what you like, they will know everything!"[96] Many of the arguments from each school of thought regarding the aggregation of PII are also apparent from the aggregation of unclassified mission or capability information.

Aggregation of Information

Threat Events 10, 11, and 14

There is a potential that aggregated information may affect an operational or tactical mission creating a high risk to the organization.[97] Like the aggregation of PII, the association or link between an organization and its airmen via friending, commenting on the organization's sites or releasing similar hashtags (or phrases) provides an attack vector for adversaries to mine both official and private accounts. While the defense section showed that the USAF is successful in limiting the release of classified or sensitive information, it also demonstrated that the aggregation of information from airmen and their families presents a vulnerability. The information sought by hackers conducting cyber espionage activities may not be classified as secret or be sensitive in isolation, but the aggregation of each datum between official and private accounts into data can prove valuable.

One defining feature of cyber espionage is that it can deal with quantity to exploit vast amounts of information in order to piece together something of value.[98] It is common for many personnel with the unit/organization, to follow or friend a unit that creates a Facebook or Twitter site. Through reconnaissance, data mining, or network analysis the adversary may have access to collect information from families, friends, and colleagues.

---

[96] Weimann, *Terrorism in Cyberspace*, 130–31.
[97] Appendix G: Threat Event Table 9-14
[98] Libicki, *Cyberspace in Peace and War*, 9.

The information collected and aggregated from these sites may impact missions to follow. Three examples demonstrate the potential of these threat events.

First, in 2007, U.S. soldiers took photos of a group of new U.S. Army helicopters parked on a base in Iraq and uploaded them. The photos were not considered classified or sensitive; however, the photos contained geotags that included location information. Insurgents used the geotags and uploaded them onto Google Earth to pinpoint the position of the helicopters. A subsequent mortar attack destroyed four of the helicopters.[99] Since the attack, Google Earth has agreed to digitally obscure or blur areas requested by governments. These mitigations also include reducing the resolution of satellite imagery. Also, Twitter and Facebook limit the metadata released in imagery, as previously mentioned.

Second, the Israeli Defence Force (IDF) canceled a raid on a Palestinian village after a soldier revealed the time and place of the operation on Facebook. He posted, "on Wednesday we clean up Qatanah, and on Thursday, God willing, we come home."[100] The IDF delayed the mission and stated that it is common for their adversaries to scan the Internet to collect information on missions. Uploading classified or aggregating unclassified information to social networks or any website exposes the information to anyone who wishes to view it, including foreign and hostile intelligence services.[101]

Third, in 2016 the Australian military analyzed the risks associated with organizational and personal use of social media during Exercise Hamel. The analysis of 680 Australian Defence Force members and their organizations found that information available on social media creates conditions that allow adversaries to generate actionable intelligence.[102] It stated:

> Using only openly available tools and techniques…Intelligence Analysts were able to identify the location, nomenclature, equipment, and organisation of deployed forces. The process of geo-location, enabled the location of images to be determined often with a very high degree of accuracy. Confirmation through the correlation of other open sources of

---

[99] Singer and Friedman, *Cybersecurity and Cyberwar*, n.d., 102.
[100] "Israeli Military 'Unfriends' Soldier after Facebook Leak," *BBC News*, March 4, 2010, Online edition, http://news.bbc.co.uk/2/hi/8549099.stm.
[101] "Israeli Military 'Unfriends' Soldier after Facebook Leak."
[102] Ryan, AM and Thompson, AM, "Social Media in the Military: Opportunity, Perils and a Safe Middle Path," 3.

> content can, in some cases, result in the production of highly accurate, actionable intelligence that could be immediately targetable.[103]

The results of the exercise sound alarming. However, analysts should be cautious about drawing too many conclusions regarding the aggregation of information in this manner. The exercise may not be perceived by the participants to be particularly sensitive or classified in comparison to a conflict or engagement with another adversary or nation state. Therefore, the release of information may have been greater when compared to actual conflict. In addition, Australian intelligence analysts conducted the analysis instead of attempting to mimic the capabilities of foreign adversaries. By the nature of their position, education, and training they already have an advantage over adversaries by knowing the language, exercise, and Australian tactics and procedures. Nevertheless, the aggregation of information remains a security concern to organizations.

The three examples demonstrate a high potential risk to military organizations when engaging in social media. The controls each organization had in place were inadequate to minimize the risks. On closer analysis, the USAF have introduced additional controls that attempt to limit and reduce the likelihood and consequences of these threat events and lower the risk to the organization.

In addition to annual social media training, the removal of location information by Twitter and Facebook, and commanders' prerogative to limit social media on operations, the USAF conducts web content vulnerability analysis (WCVA). WCVA is a formal and structured process of evaluating the information posted on the Internet by the organization and its people.[104] Operational security managers, signature managers, and coordinators conduct keyword searches and web crawling to find and reduce targetable information. The analysis employs legal and security personnel to review disclosed information.[105] Many wings will also invite information aggressor squadrons to conduct red team analysis of their organization and personnel.[106]

---

[103] Ryan, AM and Thompson, AM, "Social Media in the Military: Opportunity, Perils and a Safe Middle Path," 3.
[104] Air Force Instruction 10-701, *Operations Security*, 8 June 2011, 28, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf
[105] Air Force Instruction 10-701, *Operations Security*, 13.
[106] Trudell, Special Operations Wing Public Affairs Office Interview.

The reports inform commanders of the vulnerabilities within their organization, including specific posts and personnel. The USAF also encourages their airmen to self-regulate at the lowest level. For example, "if you find that someone has posted sensitive information on a social media platform, politely ask the individual to remove/edit his or her post. If unacceptable, you can contact your local public affairs office or use your chain of command."[107] The authority to intervene, including the use of the Uniform Military Code of Justice, is available to commanders should less formal methods be ineffective.[108]

The vast array of missions that the USAF conducts are impossible to capture within a service-level risk assessment. Instead, commanders at each level of the organization are instructed to identify and protect the sensitive mission and capability information. The information gathered by this study is insufficient to make an accurate assessment of the risk to an organizational based on aggregation of unclassified information. Privacy laws precluded the author from conducting OSINT or penetration testing of airmen's personal accounts. However, the mitigations identified by the USAF appear to address the threat event and attempt to limit the impacts to the organization. Figure 7 indicates a medium risk to highlight the event rather than provide a judgment. A commander's school of thought, mission, and analysis of vulnerability against adversary's capabilities will determine the risk of social media within their organization and determine what additional mitigations are required. Additionally, whether an organization engages or not, the risk of personal release of mission and capability information will require ongoing analysis, mitigation, and education. The USAF has accepted the risks associated with social media discussed in this analysis, although the pathway to acceptance has been challenging.

[107] USAF, "Social Media." 14.
[108] Air Force Instruction 1-1, *Air Force Standards*, 12 November 2014, 21, http://static.e-publishing.af.mil/production/1/af_cc/publication/afi1-1/afi1-1.pdf.

USAF Risk Acceptance

Social media presents a complex arrangement for organizational risk acceptance. The risk acceptance of social media for the Department of Defense required collaboration and discussion across the services, major commands, and information systems senior leaders. In the U.S., the DoD signaled that the organization was unwilling to accept the risk to host social media on unclassified computer networks in 2007. The DoD was concerned about network security, bandwidth, and information leakage of personal and operational information.[109] The early determination represented views from the zero-tolerance school of thought. Regardless, in 2008 the USAF commissioned a social media division within the Air Force Public Affairs Agency (AFPAA). The Public Affairs Agency utilized existing policies to guide the management of social media-released information in the public domain. Shortly after that, the USAF released a booklet, *New Media and the Air Force,* which guided airmen about the use of social media. It openly identified the lack of USAF policy, and therefore was vague about the rules regarding the use of social media within the service.[110] At this stage, the USAF adopted a traditional media school of thought.

Two significant events that occurred in 2009-2010 that influenced the USAF to accept the risks associated with social media, and furthermore, to permit its use at lower levels of the organization. First, President Obama signed an Open Government Directive in 2009. The intent of the directive was to increase transparency within federal departments and agencies (including the DoD). It required senior leaders to increase accountability, promote participation, and expand access to information by making it available online. Furthermore, the directive demanded a cultural change to create an unprecedented and sustained level of transparency and embrace emerging technologies to open new forms of communication between government agencies and the people.[111] Second, in early 2010, the Office of the Deputy Secretary of Defense reversed the

---

[109] NIPR is an unclassified network.
[110] The United States Air Force Public Affairs Agency. *Social Media and the Air Force*, Washington, DC, November 2009, p. 23.
[111] Social Media – DoD's Greatest information sharing tool or weakest security link? (6)

decision to restrict social networking on the NIPRNET.[112] The chief information officer directed DoD service providers to open their networks to social media, thereby accepting the risks associated with network security.[113]

In 2012, the Air Force updated its instructions (AFIs) to detail the acceptance, management, and control of social media. The Secretary of the Air Force is the signatory to these instructions, and therefore, ultimately accepts the risks associated with the orders and the risks identified in this article. The AFI's authorize USAF commanders to employ official social media to complement a wider communication strategy to assist in building unit cohesion; increase mission effectiveness, morale, and retention as well as enhance confidence, while reducing distractions, rumors, and uncertainty.[114] The USAF updated the AFIs that approved Commanders to engage in traditional forms of media to include social media platforms. Wing and base levels commanders conduct the overwhelming majority of official social media activities.[115] In addition to the organizations use of social media, airmen within the organization are encouraged to utilize social media to tell the USAF story. The combination of organizational and personal use of social media represented a move towards the new media school of thought.

Today, the USAF is transitioning to the information dominance school of thought. Airmen at all levels of the USAF are encouraged to utilize the expressive capabilities of social media in an attempt to dominate the information environment. Within the organization, senior leaders release guidance detailing the strategic message that leaders and airmen at all levels should communicate. [116] The guidance attempts to synchronize an Air Force message and encourages leaders to engage in all types of medium to connect with the public. The development of policy, guidelines, and training has enabled this approach by mitigating the risks to low levels as described by this study.

---

[112] The Non-classified Internet Protocol (IP) Router Network is a private IP network used to exchange unclassified information, including information subject to controls on distribution.
[113] "Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-Based Capabilities" (Deputy Secretary of Defense, February 25, 2010), https://fas.org/irp/doddir/dod/dtm-09-026.pdf.
[114] AFI 135-101
[115] Facebook Wing (175), Group (40), Squadron (24). An O-6 Colonel rank (O7 for higher visibility/larger wings) commands the wings. airmen trained in public affairs, operational security, and legal manage social media and inform the commander's communication strategy.[115]
[116] Goldfein, "'America's Air Force: Always There' Letter of Intent."

Conclusion

The author of this study initially believed that the USAF had become too transparent, and accepted an unacceptable amount of risk when engaging in social media. Upon further analysis, the USAF has demonstrated that an acceptable balance between security and transparency can be struck by the development of policy, guidance, and training to mitigate and control the risks of social media. The study also found that when commanders and airmen adhere to USAF's governance and training, they will incur a low risk to the organization's personnel, mission, capability, and reputation. Furthermore, it became evident that leaders also apply additional mitigations to minimize risk commensurate with their unit's objectives. Nonetheless, the USAF's use of social media within the organization does not eliminate risk altogether. The aggregation of information across official and non-official sites presents an ongoing risk to personnel, capability, and missions. This risk requires the USAF to commit resources to monitor and control the new media environment. Overall, the USAF understands that social media has become a ubiquitous part of airmen's lives, and has decided to engage, not disengage, to promote transparency and accountability and dominate the information environment.

While this study addressed a range of social media risks, it did not measure the benefits regarding the organizational use of social media. There is no shortage of commanders claiming the benefits of social media; however, the author did not find any scholarly papers that differentiated the perceived from the actual benefits. Analysts should conduct additional studies to discriminate between the many objectives of social media from leadership to brand management. Similarly, the study should also address the risk of militaries not engaging in social media from an adversarial and non-adversarial point of view.

This study aimed to investigate a range of security risks when military organizations participate in social media. Commanders should tailor the analysis to inform decision making and examine vulnerabilities and threat actors akin to their circumstance. As discussed, the model has its limitations and leaders may agree or disagree with the analysis depending on each their own school of thought, risk tolerance, and perceived utility of social media. Given this, the assessed risks may increase or decrease accordingly.

There is a lot to learn from the USAF's journey from zero tolerance to information dominance. Smaller Air Forces, like the RAAF, are right to take a cautious approach and limit its use until leaders conduct further analysis and introduce controls. The study found that military organizations that attempt to follow the leader without understanding and treating the risks has the potential to be exposed to a high risk. This study has shown that the introduction of a comprehensive policy, guidance, and training to mitigate and control the risk are successful in reducing risk levels from high to low. Smaller militaries should consider the controls the USAF have introduced if they desire increased transparency or wish to utilize social media at lower levels of their organization.

Social media and the wider cyber domain share similar characteristics to other domains, when analyzing security risks. While there are nuances that distinguish the domain from the others, understanding vulnerabilities, threat actors (including their capabilities and intent), and utilizing the risk assessment process remains useful to inform decision-making. Instead of focusing on vulnerabilities or threat actors alone, the process illustrates potential threat events and measures the likelihood and consequence of each threat event occurring. In summary, the expressive capabilities of social media make it a powerful communicative tool. Commanders that utilize the tool should continue to search for an acceptable balance between security and transparency by analyzing the security risks against the benefits. Only then will leaders be able to decide whether the "juice is worth the squeeze."

Appendices

Appendix A: RAAF Risk Management Authority[117]

Risk Level	**Risk Management Authority**
Very High	Chief of Air Force (O9)
High	Air Commander / Deputy Chief of Air Force (O8)
Medium	FEG Commander (O7)
Low	Unit Commanding Officer / Wing OC
Very Low	As promulgated by Unit Commanding Officer

Source: Adapted from RAAF Air Forepson69
ce Safety Manual

[117] Royal Australian Air Force, *Air Force Safety Manual*, pt. 1, section 2, chapter 8.

Appendix B: USAF Policy Review

AFI 1-1 Air Force Standards[118]

All airmen are on duty 24 hours a day, 365 days a year, and their actions on and off duty are subject to the Uniform Code of Military Justice (UCMJ).[119] Airmen are encouraged to make their social media accounts, and their families 'private.' USAF members are expected to adhere to higher standards than those in the wider community.[120] The USAF does not distinguish between on-duty and off-duty use of social media. Accordingly, airmen are held accountable for their actions regardless if the behavior occurred while on duty or not. Additionally, the policy states, "when you are expressing personal opinions on social media sites and can be identified as an Airman, you should make clear that you are speaking for yourself and not on behalf of the Air Force."[121] While service members may use their rank and service when acting in a personal capacity, they should not do so in situations where the context may imply official sanction or endorsement of their personal opinions.

The policy also states that airmen are encouraged to use social media, interpersonal communication, community engagements, and other methods to share experiences with the public and tell the Air Force story while maintaining operational security. Airmen must obtain necessary security and policy review before releasing official imagery, documents, information, or proposed statements outside the Air Force.

[118] Air Force Instruction 1-1, *Air Force Standards*, 12 November 2014, http://static.e-publishing.af.mil/production/1/af_cc/publication/afi1-1/afi1-1.pdf
[119] Air Force Instruction 35-101, *Public Affairs Responsibilities and Management*, 12 January 2016, 57, http://static.e-publishing.af.mil/production/1/saf_pa/publication/afi35-101/afi35-101.pdf.
[120] Air Force Instruction 1-1, *Air Force Standards,* 21.
[121] Air Force Instruction 1-1, *Air Force Standards,* 21.

AFI 35-104 - Media Operations[122]

Media instructions state the releasable products for official social media.[123] One of the core elements that the USAF controls are the release of personally identifiable information (PII). The following table abbreviates the USAF's guidelines on the release of PII.

Releasable	**Not Releasable**
Name. Releasable within guidelines described within this AFI and AFI 33-332, *The Air Force Privacy and Civil Liberties Program*.	Personal Address.
Duty Status. Active duty, retired, etc.	Age and Date of Birth.
Rank: Military grade and rank, civilian grade, military	Biographies and Photographs of Persons other than General Officers.
Gender.	Death. Civilian Employee or Military Person.
Military Awards and Decorations or Citations.	Discharges.
Duty Location. Current, past and future assignments are releasable, except sensitive and overseas assignments masked in unit records.	Duty Location. Current or future assignments, office and unit address and duty telephone number for personnel or units stationed overseas or for routinely deployable or sensitive units are not releasable.
	Family Members. Family member information, including number, age, gender, or names of family members.
	Marital Status

Source: Summarized from AFI 35-104 Media Operations

The USAF limits the type of PII released by privacy and civil liberties law. The release of information on operational deployments is at the discretion of MAJCOM leadership. In general, the arrival of units in theater, the home station, friendly force size, friendly casualty, past operations, personal interest stories, deployed units and locations are releasable. Information that would reveal intelligence sources, classified actions, future operations or information that could put people's lives at risk, or special operations are not releasable. The list of releasable and not releasable media is considerable. In

[122] Air Force Instruction 35-104, *Media Operations*, 13 July 2015, https://fas.org/irp/doddir/usaf/afi35-104.pdf.
[123] Air Force Instruction 35-104, *Media Operations*, 10.

addition to these guidelines are requirements for military leaders to establish plans for crisis communication.

AFI 35-102 Security and Policy Review[124]

This instruction establishes a reporting chain for publically disclosed information. It describes that clearance authority from MAJCOM, Field Operating Agencies, Wing Level Organizations for the release of official information. For example, within a wing-level organization, Public Affairs are responsible for releasing information targeted at the local and regional level. Also, local commanders, or their representative, may clear news or photos of national interest.

AFI 10-701 Operations Security[125]

This instruction describes the signature management, planning, process, education and assessment of operational security (OPSEC) in the USAF. Specifically, it defines OPSEC as "a process of identifying, analyzing and controlling critical information indicating friendly actions associated with military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems.
(2) Determine what specific indications could be collected, analyzed, and interpreted to derive critical information in time to be useful to adversaries.
(3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."[126]

All personnel conduct OPSEC training on enlistment and annually.

The AFI states guidelines for Web Content Vulnerability Analysis (WCVA). WCVA is a formal, structured process of evaluating information posted on organizational public and private websites.[127] The study complements each organization's requirement to have processes in place ensuring all information made available on publicly accessible websites are reviewed and approved before posting. It includes the requirement to have a

[124] Air Force Instructions 35-102, *Security and Policy Review Process*, 4 May 2016, https://fas.org/irp/doddir/usaf/afi35-102.pdf.
[125] Air Force Instruction 10-701.
[126] Air Force Instruction 10-701, *Operations Security*, 5.
[127] Air Force Instruction 10-701, *Operations Security*, 28.

legal review, automated keyword search, and management of information collected on OPSEC.[128] USAF policy indicates that operational security program managers, signature managers, and coordinators oversee the release of operational and personal information from the wing, Major Commands and Headquarters Air Force levels. The positions also conduct web content vulnerability analysis that includes keyword searches, web crawling, and legal reviews. Many wings will also invite information aggressor squadrons to conduct red team analysis of their released information.

USAF Social Media Guide[129]

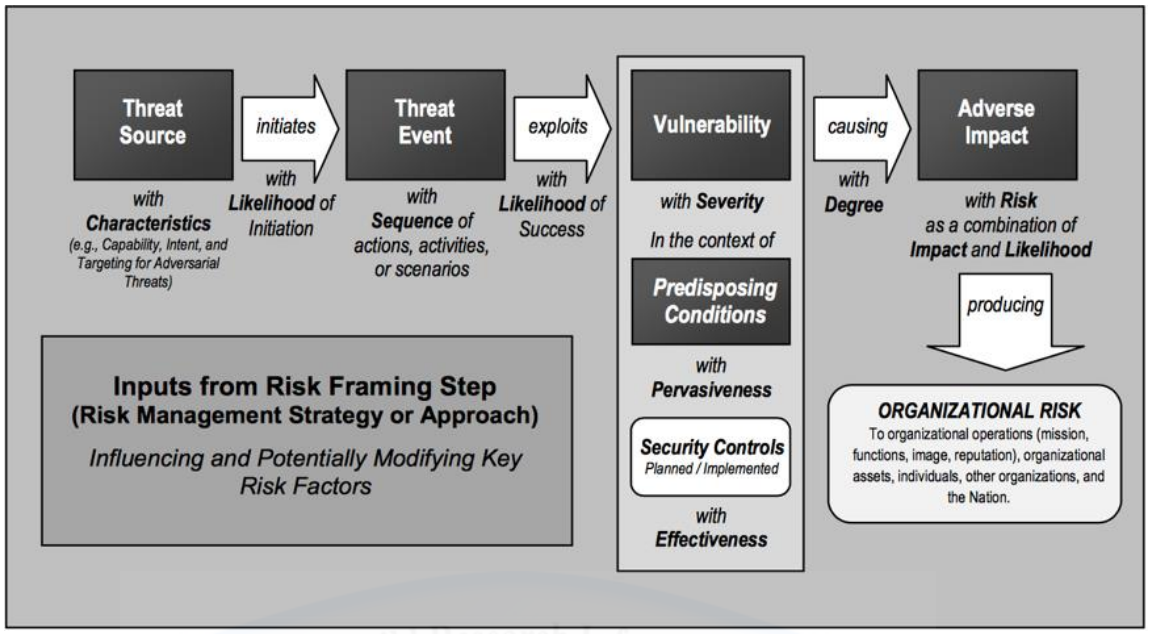
The USAF produces a social media guide that details how airmen, leaders, and families can successfully engage in social media. It provides easy to follow tips that assist airmen, commanders and their families in using social media in their personal and professional lives. It also provides educational training about how airman should tell their story online. The USAF provides examples of acceptable and unacceptable tweets, for instance, "Feels great after delivering 50 tons of food during our #C130 mission with @TeamRamstein!"[130]

USAF Education and Training

All information system users complete DOD Information Assuredness training before granting access to an information system. Users re-accomplish information assuredness training annually using the Advanced Distributed Learning System (ADLS) computer based training which reports compliance to the IAO. Specific training on social media is included to inform the wider community of information vulnerabilities.

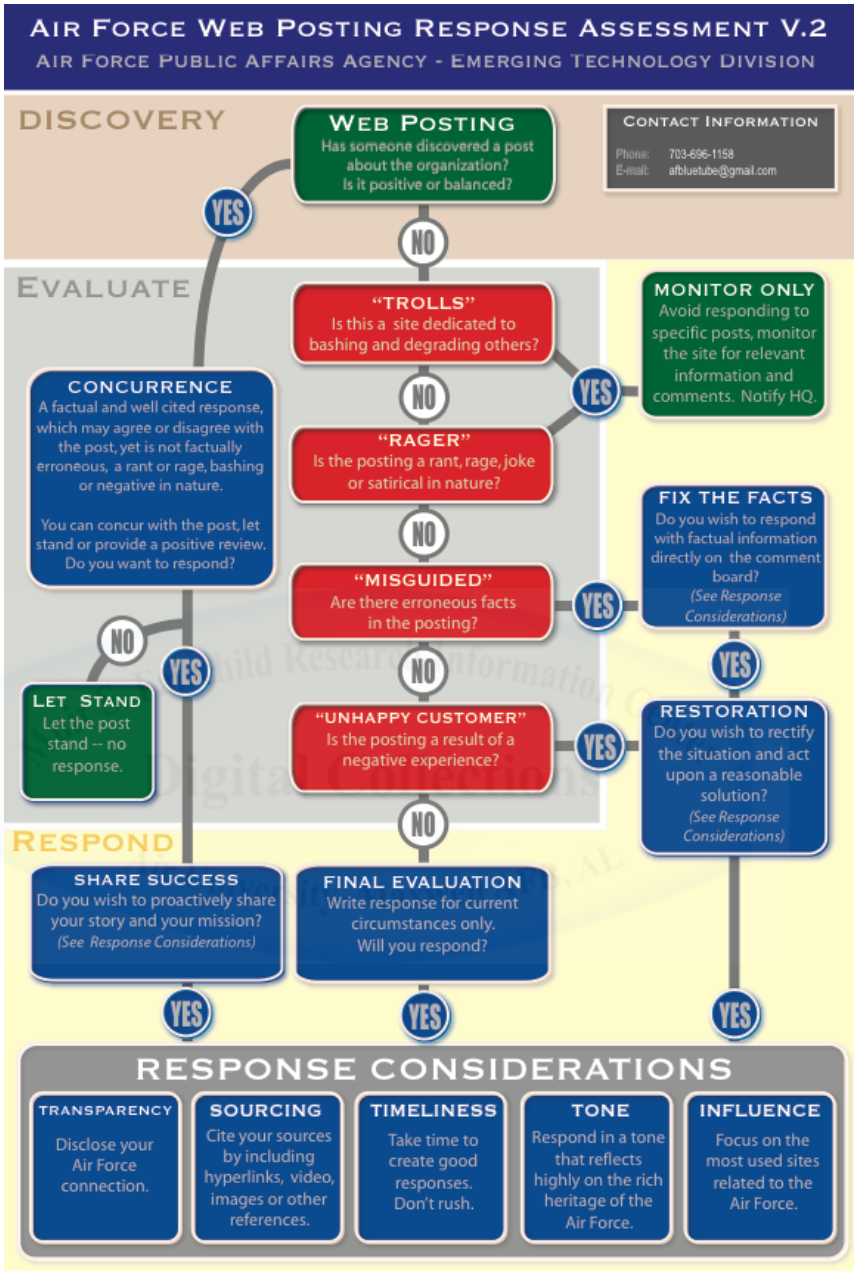
[128] Air Force Instruction 10-701, *Operations Security*, 28.
[129] USAF, "Social Media."
[130] USAF Social Media Pamphlet

Appendix C: Generic Risk Model



Source: National Institute of Standards and Technology: Guide for Conducting Risk Assessments

Appendix D: Air Force Web Posting Response Assessment V.2



Source:http://www.globalnerdy.com/wordpress/wpcontent/uploads/2008/12/air_force_web_posting_response_assessment-v2-1_5_09.pdf

Appendix E: Vulnerability Analysis of USAF Social Media

Commanders/PA's Posts	**Facebook**	**Twitter**
PII Release	**4**	
Address	0	0
Cell Number	0	0
Date of Birth	0	0
Discharge Information	0	0
Education	0	0
Family Members Names	4	0
Marital Status	0	0
SSN	0	0
Location Information Future	0	0
Information Leakage	**4**	
Classified Documents	0	0
Who, What Where and When - Individual Names, deployment location and deployment dates combined	0	0
Personnel KIA	0	0
Adversary KIA	0	0
Protective Measures	0	0
Battle Scenes	3	0
Force Deployment Future Operations	0	0
Future Exercises (Off-base)	0	0
Future position, location and time. Forces (overseas)	0	0
Intelligence Methods and Collection	0	0
Rules of Engagement	0	0

The precise location of forces (Off-base) in the future	4	0
POO for organized attack	0	0
Specific Tactics, Speeds, and Formations	0	0
Classified Discussions	0	0
Political Discussions	0	0
	0	0
Intellectual Property Release	0	0
Copyright Infringements	0	0
Commanders Critical Information	N/A	N/A
Content Management	**7**	**3**
Stale or Outdated Information	7	3
Total Followers	5,896,172	N/A

Source: Author original work - Compiled from Vulnerability Assessment

Appendix F: Threat Event Table 1-8

NO	Objective	Threat Source	Threat Event	SANS Institute	Vulnerability and Predisposing Conditions (Existing Controls)	Risk Overview	Organizationally Defined Consequence - Impact		Likelihood (after mitigation)	Residual Risk Level	Organizationally Defined Consequence - Impact		Potential Likelihood (no mitigation)	Potential Risk Level
1	Communicate to Organization	Community	Negative Responses to Post	Reputation/Brand as an Asset	Personnel Assigned to Monitor Site, Behavior Terms, USAF Flowchart, Crisis Management Training	Negative Comments	Personnel	Minor	Almost Certain	Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Low	Mission	Minor		Low
						Negative Reputation and Brand	Capability	Minor		Low	Capability	Minor		Low
							Reputation	Minor		Low	Reputation	Minor		Low
2	Cyber Harassment	Trolls	Inflammatory, extraneous, or off-topic messages in comments section	Reputation/Brand as an Asset	Personnel Assigned to Monitor Site, Behavior Terms, USAF Flowchart, Crisis Management Training	Inflammatory Comments	Personnel	Minor	Almost Certain	Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Low	Mission	Minor		Low
						Additional Monitoring, Interrupted	Capability	Minor		Low	Capability	Minor		Low
						Messaging, Site Disruption	Reputation	Minor		Low	Reputation	Minor		Low
3	Signpost Messages to Organization and Public	Issue Motivated Groups	Persistent Messaging	Reputation/Brand as an Asset	Personnel Assigned to Monitor Site, Behavior Terms, USAF Flowchart, Crisis Management Training	Signposting/Message Board	Personnel	Minor	Almost Certain	Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Low	Mission	Minor		Low
						Additional Monitoring, Interrupted	Capability	Minor		Low	Capability	Minor		Low
						Messaging, Site Disruption	Reputation	Minor		Low	Reputation	Minor		Low
4	Harassment Psychological Operations	Terrorist Lone Wolf	Messaging	Reputation/Brand as an Asset - Comments Field	Personnel Assigned to Monitor Site, Behavior Terms, USAF Flowchart, Crisis Management Training	Harassing messages to airmen and families within comments field	Personnel	Minor	Occasional	Very Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Moderate		Low	Mission	Moderate		Medium
						Harassment, Family Distress, Failure to achieve an organizational objective	Capability	Minor		Very Low	Capability	Minor		Low
						Short Term National Media Attention	Reputation	Moderate		Low	Reputation	Moderate		Medium
5	Harassment Embarrassment to Organization	Activists Issue Motivated Groups Foreign Terrorist Groups	Conducts externally-based session in hijacking social media account	Reputation/Brand as an Asset Hacktivism	Crisis Management in Public Affairs Policy & Password Management Annual Training Two Factor Identification	Hijacking Organizations Accounts	Personnel	Minor	Improbable	Very Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Very Low	Mission	Minor		Low
						Messaging on Wall/Interruptions	Capability	Minor		Very Low	Capability	Minor		Low
						Short term national media attention	Reputation	Major		Low	Reputation	Major		High
6	Financial Gain Protect Intellectual Property	Legal Firms	Gather information using open source discovery of organizational information	Content Management - Copyright/IP & Censorship	PA Training on Intellectual Property and Copyright, Media Policy AFI 35-104	Copyright/Trademark Infringement	Personnel	Minor	Improbable	Very Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Very Low	Mission	Minor		Low
						Litigation, financial loss and	Capability	Minor		Very Low	Capability	Minor		Low
						short term national media attention	Reputation	Moderate		Very Low	Reputation	Moderate		Medium
7	Identity Theft for Financial Gain	Criminal Organization	Perform open source/Reconnaissance/Craft Spear Phising Attacks/Modified Malware/Scams etc.	Cyber Crime	PII Policy on Release of Personal Information	Identity Theft	Personnel	Minor	Almost Certain	Low	Personnel	Minor	Almost Certain	Low
						Leading to	Mission	Minor		Low	Mission	Minor		Low
						Personal Financial Loss/Reputation	Capability	Minor		Low	Capability	Minor		Low
						Damage	Reputation	Minor		Low	Reputation	Minor		Low
8	Target Single Airmen	Terrorist Lone Wolf Issue Motivated Groups	Aggregated PII Using OSINT	Location Awareness Investigative Tool Reconnaissance	PII Regulations, Location Training, OPSEC Training, Family Brochures, Social Media training	Aggregated PII (or accidental Release of PII)	Personnel	Critical	Rare	Low	Personnel	Critical	Occasional	High
						Leading to	Mission	Moderate		Very Low	Mission	Moderate		Low
						Serious Injury/Loss of Life	Capability	Moderate		Very Low	Capability	Moderate		Low
							Reputation	Major		Very Low	Reputation	Major		Medium

Source: Author original work - generated from RAAF/USAF Risk Management Tables & Vulnerability Assessment

Appendix G: Threat Event Table 9-14

9	Target Group of Airmen or Families	Terrorist Lone Wolf Issue Motivated Groups	Gather PII Using OSINT	Location Awareness Investigative Tool Reconnaissance	PII Regulations, Location Training, OPSEC Training, Family Brochures, Social Media training	Aggregated PII (or accidental Release of Group Information) Leading to Multiple Fatalities/Many Serious Injuri	Personnel	Catastrophic	Rare	Low	Personnel	atastrophi	Occasional	High
							Mission	Major		Very Low	Mission	Major		Medium
							Capability	Major		Very Low	Capability	Major		Medium
							Reputation	Critical		Low	Reputation	Critical		High
10	Target Mission	State Sponsored Actors (APT)	form Reconnaissance Surveillance of Targeted Organization through OSINT	Location Awareness Data Mining OSINT	Air Gap between Classified Systems, OPSEC Training, AFI 10-701	Release of Docments labelled Classified or Sensitive Leading to Failure to achieve a mission that is essential to a strategic objective	Personnel	Minor	Rare	Very Low	Personnel	Minor	Occasional	Very Low
							Mission	Catastrophic		Low	Mission	atastrophi		High
							Capability	Critical		Low	Capability	Critical		High
							Reputation	Critical		Low	Reputation	Critical		High
11	Strategic Advantage	State Sponsored Actors (APT)	Compromise Classified Material		Social Media Host on Non-Classified System Air Gap System OPSEC, PAO, Classification Training	Non-Malicious accidental release of Classified information Leading to State based strategic advantage loss	Personnel	Minor	Improbable	Very Low	Personnel	Minor	Almost Certain	Low
							Mission	Major		Low	Mission	Major		High
							Capability	Major		Low	Capability	Major		High
							Reputation	Major		Low	Reputation	Major		High
12	News Story	Media	Gather information using open source discovery of organizational information	Reputation/Brand as an Asset	PA Control of Information Posted	Poor judgement regarding release of information Leading to Uncontrolled news release	Personnel	Minor	Occasional	Very Low	Personnel	Minor	Probable	Low
							Mission	Minor		Very Low	Mission	Minor		Low
							Capability	Minor		Very Low	Capability	Minor		Low
							Reputation	Moderate		Low	Reputation	Moderate		Medium
13	Targeted Network Breach	Hackers-Non State Actors	Exploit vulnerabilities on internal organizational information systems	Data Loss	2-Factor Identification Air Gap Classified Information Remote Access Requirements Password Training	Target Personnel for Passwords Leading to Breach of Classified System	Personnel	Minor	Improbable	Very Low	Personnel	Minor	Almost Certain	Low
							Mission	Major		Low	Mission	Major		High
							Capability	Major		Low	Capability	Major		High
							Reputation	Moderate		Very Low	Reputation	Moderate		Medium
14	Gain Mission or Capability Information	Foreign Terrorist Organization or Nation State	Aggregate Mission and Capability information across organizational and individual social media sites	Data Loss	AFI 10-701 Operational Security, Commanders may restrict social media use for operations and missions, Web Content Vulnerability Analysis, Aggressor Squadrons penetration testing.	Aggregate unclassified information Leading to Failure to achieve an important operational objective with significant unit/tactical implications OR temporary loss (severe degradation) to defense capability	Personnel	Moderate	Occasional	Low	Personnel	Moderate	Probable	Medium
							Mission	Major		Medium	Mission	Major		High
							Capability	Major		Medium	Capability	Major		High
							Reputation	Moderate		Low	Reputation	Moderate		Medium

Source: Author original work - generated from RAAF/USAF Risk Management Tables & Vulnerability Assessment

Bibliography

ABC Australia. "Donald Trump, Malcom Turnbull Meeting Looks like an Attempt to Mend Fractures." News. *ABC News*, 05May2017. http://www.abc.net.au/news/2017-05-05/donald-trump-malcolm-turnbull-meeting-usyd-analysis/8501058.

Air Force "Guidance Memorandum to AFI 90-802 Risk Management." Department of the Air Force, March 8, 2016. http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf.

Air Force Instruction 1-1, *Air Force Standards*, 12 November 2014, http://static.e-publishing.af.mil/production/1/af_cc/publication/afi1-1/afi1-1.pdf.

Air Force Instruction 10-701, *Operations Security*, 8 June 2011. http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf.

Air Force Instruction 35-101, *Public Affairs Responsibilities and Management*, 12 January 2016, http://static.e-publishing.af.mil/production/1/saf_pa/publication/afi35-101/afi35-101.pdf.

Air Force Instructions 35-102, *Security and Policy Review Process*, 4 May 2016, https://fas.org/irp/doddir/usaf/afi35-102.pdf.

Air Force Instruction 35-104, *Media Operations*, 13 July 2015, https://fas.org/irp/doddir/usaf/afi35-104.pdf.

Anonymous. "Anonymous Explains It's Objectives." YouTube, 07Feb2012. https://www.youtube.com/watch?v=WSNbImxjK3E.

Arquilla, John, David F. Ronfeldt, and United States, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand, 2001.

Australian Government Department of Defence. *Defence Issues Paper 2014*. Australia: Commonwealth of Australia, 2014. http://www.defence.gov.au/whitepaper/docs/defenceissuespaper2014.pdf.

Bejar, Adrian. "Balancing Social Media with Operations Security in the 21st Century." Naval War College, 03May2010.

Benson, David. "Why the Internet Is Not Increasing Terrorism." *Security Studies* 23, no. May 2014 (May 2014): 293–328.

Blank, Rebecca. "Information Security: Guide for Conducting Risk Assessments." National Institute of Standards and Technology, September 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Bleier, Evan, and Christopher Brennan. "A Hundred American Soldiers Named on ISIS 'Kill List' - but Servicemen Say They Are 'Unfazed by Extremists' Threats." *Daily Mail*, March 23, 2015. http://www.dailymail.co.uk/news/article-3007128/Soldiers-names-addresses-photos-published-ISIS-s-kill-list-say-unfazed-threat.html.

Brian, Barrett. "Time To Lock Up Your Twitter Account With Two-Factor." *Wired Magazine*, June 9, 2016. https://www.wired.com/2016/06/twitter-hack/.

Brown, Justin. "What the Centcom Twitter Hack Means to You." *Government Technology*, 23Jan2015. http://www.govtech.com/security/What-the-CentCom-Twitter-Hack-Means-to-You.html.

Cilluffo, Frank. “Emerging Cyber Threats to the United States.” GW Center for Cyber and Homeland Security, February 25, 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HHSC_Testimony_Feb%2025-2016_Final.pdf.

Clapper, James. *Worldwide Threat Assessment of the US Intelligence Community*. Senate Armed Services Committee, February 9, 2016. https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st Ecco pbk. ed. New York: Ecco, 2012.

Commonwealth of Australia. “2016 Defence White Paper.” Department of Defence, 2016. http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

Cronin, Audrey Kurth. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. 1. paperback print. Princeton: Princeton Univ. Press, 2011.

“Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Ise of Internet-Based Capabilities.” Deputy Secretary of Defense, February 25, 2010. https://fas.org/irp/doddir/dod/dtm-09-026.pdf.

Drapeau, Mark, and Linton Wells. “Social Software and National Security: An Initial Net Assessment.” Centre for Technology and National Security Policy. National Defense University, April 2009. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA497525.

Goldfein, Dave. Letter. “‘America’s Air Force: Always There’ Letter of Intent.” Letter, January 27, 2017.

Hall, Jimmy. “Leveraging Social Networking in the United States Army.” Army War College, 2011. http://www.dtic.mil/dtic/tr/fulltext/u2/a559960.pdf.

“Israeli Military ‘Unfriends’ Soldier after Facebook Leak.” *BBC News*, March 4, 2010, Online edition. http://news.bbc.co.uk/2/hi/8549099.stm.

Lark, John, Valentin Nikonov, International Organization for Standardization, International Trade Centre UNCTAD/GATT, and United Nations Industrial Development Organization. *ISO31000: Risk Management: A Practical Guide for SMEs*. International Organization for Standardization, 2015.

Libicki, Martin C. *Cyberspace in Peace and War*. Annapolis, Maryland: Naval Institute Press, 2016.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press, 2015.

Lt Gen Bender, William. “Air Force Policy Directive 17-1 Information Dominance Governance and Management.” USAF, 12April2016. https://fas.org/irp/doddir/usaf/afpd17-1.pdf.

Managing Director. “Open Government Directive.” *Federal Communications Commission*, December 8, 2009. https://www.fcc.gov/general/open-government-directive.

Meehan, Patrick. “Jihadist Use of Social Media - How to Prevent Terrorism and Preserve Innovation.” Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives presented at the Hearing before the Subcommittee on Counterterrorism and

Intelligence of the Committee on Homeland Security House of Representatives, Washington, D.C, December 6, 2011. https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm.

Mei, Sin. "Why Facebook and Twitter Are Stripping Out Your Context." *Sentiance*, October 11, 2013. https://www.sentiance.com/2013/10/11/facebook-twitter-stripping-context/.

Molok, Nurul nuha Abdul, Shanton Chang, and Atif Ahmad. "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats." Edith Cowan University, November 30, 2010. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism.

Patterson, George. *Review of Social Media and Defence*. Commonwealth of Australia, 2011. http://www.defence.gov.au/pathwaytochange/docs/socialmedia/Review%20of%20Social%20Media%20and%20Defence%20Full%20report.pdf.

Royal Australian Air Force. "Social Networking: A Guide to Effective Social Media Use." Commonwealth of Australia. *Social Networking*, 2014. https://www.airforce.gov.au/docs/Social%20Media%20Booklet.pdf.

Royal Australian Air Force. "Air Force Safety Manual." Commonwealth of Australia, January 20, 2016.

Ryan, AM, Mick, and Marcus Thompson, AM. "Social Media in the Military: Opportunity, Perils and a Safe Middle Path." Grounded Curiosity. Accessed April 6, 2017. http://groundedcuriosity.com/social-media-in-the-military-opportunities-perils-and-a-safe-middle-path/#sthash.rd2ODm2U.dpbs.

Secretary of the Air Force Public Affairs. "AF Presents Fiscal Year 2017 Budget." U.S. Air Force. *U.S. Air Force*, February 9, 2016. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/652961/af-presents-fiscal-year-2017-budget.aspx.

Shirky, Clay. "How Social Media Can Make History." Ted Talk, June 2009. https://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history#t-192111.

Shullich, Robert. "Risk Assessment of Social Media." SANS Institute InfoSec Reading Room, December 5, 2011. https://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford; New York: Oxford University Press, 2014.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar*, n.d.

"Strategy for Operations in the Information Environment." Department of Defense, June 2019. https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

Trudell, Kayshel. Special Operations Wing Public Affairs Office Interview. Telephone, March 28, 2017.

USAF. "U.S. Air Force Social Media." Air Force Public Affairs Agency, Addition 2013. http://www.af.mil/Portals/1/documents/SocialMediaGuide2013.pdf.

Weimann, Gabriel. *Terrorism in Cyberspace: The next Generation*. Washington, D.C.: New York: Columbia University Press: Woodrow Wilson Center Press, 2015.