Social Media and the DOD

Benefits, Risks, and Mitigation

Lt Col Dieter A. Waldvogel, USAF, PhD

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

Description of the Issue

Social media and social networking sites (SNS) are used commonly and synonymously in information technology (IT) literature. SNS, including Web 2.0 Internet-based capabilities, are umbrella terms used to define the various activities integrating web technology, social interaction, and user-generated content. Social media refers to the various activities integrating web technology, social interaction, and user-generated content. Social media includes blogs, wikis, social networks, photo libraries, virtual worlds, location-based services, and video sharing sites.[1] Today's most commonly used SNSs include Facebook, Twitter, Google Apps, YouTube, LinkedIn, and Snapchat. On 25 February 2010, US Deputy Secretary of Defense William J. Lynn III issued the first directive-type memorandum (DTM) on the "Responsible and Effective Use of Internet Capabilities,"[2] and within months, service members had access to SNSs on their computers at work.[3]

The benefits and opportunities offered by these Internet-based capabilities are many. Among others, the opportunity for troops stationed abroad to have instant access to their loved ones at home, a public marketing and recruiting tool for military services and DOD organizations, and a tool for personnel to gain real-time situational awareness and the ability within DOD networks to share lessons learned in real time across pertinent communities. According to Air Force instruction (AFI) 35-101, *Public Affairs Policies and Procedures,* [4] 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 (OPSEC). *The United States Army's Social Media Handbook*[5] "allows every Soldier to be a part of the US Army's story, and it allows America to connect with its Army."

This medium, however, also comes with big risks and vulnerabilities—both technical and behavioral. SNSs pose serious threats to the Department of Defense Information Networks (DODIN) and military operations as cyber criminals and adversaries are finding SNSs to be a major attack vector and entry point to infiltrate our networks and exfiltrate its data.[6]

Technical threats. SNSs are vulnerable to web application attacks such as buffer overflows, cross-site scripting (XSS), code injections, and so forth. XSS attacks are a type of code injection in the form of a browser-side script. Many SNSs allow users to publish content in plain text, HTML, or active content such as JavaScript and Flash. If these posts contain malicious content, the web browser can be forced to perform a variety of unintended actions such as downloading malware, surfing to a malicious website, and even denial of service.[7] Code-injection attacks allow cyber criminals and adversaries to inject malicious codes (i.e., instructions) into a system that are then executed by an application. If performed successfully, code injections can result in sensitive data exfiltration and even destruction of the affected system. Also, SNS phishing attacks can escape e-mail content filters since these messages do not flow through network e-mail servers. Finally, SNSs are not subject to federal or DOD information assurance standards, controls, or enforcement, and therefore may not consistently provide confidentiality.[8]

Behavioral/OPSEC threats. Information security (INFOSEC):

> . . . refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.[9]

OPSEC, is one of the main components of INFOSEC, which, in turn, is "the pinnacle of social media security concerns."[10] OPSEC includes processes and actions taken to protect unclassified information that can be used against us by adversaries.

SNSs are valuable resources for cyber criminals and adversaries and can create serious OPSEC vulnerabilities for the Air Force and the DOD as a whole. SNSs provide adversaries with a nonregulated mass dissemination channel which allows them to conduct real information operations and gather intelligence.[11] According to a 2010 survey by *Computerworld* magazine,[12] more than half of SNS users in the United States post sensitive information that makes them vulnerable to cybercrime. It is estimated that SNS users receive 71 percent of spam and 46 percent of phishing attacks through social media.[13] Of particular interest to the DOD is the fact that adversaries are using SNSs to choose targets and to detect imminent attacks.

There have been some incidents involving service members and civilians tweeting about their location and ongoing operations. On 2 May 2011, a resident of Abbottabad, Pakistan was tweeting about helicopters hovering over his apartment in the middle of the night. He later discovered that this incident was a Navy sea-air-land (SEAL) team member's raid on his neighbor, Osama Bin Laden. Although inadvertently, this top-secret mission by US Special Forces was almost jeopardized by tweets from someone witnessing the operation.[14]

In January 2010, in what became known as the Robin Sage experiment,[15] an American security consultant ran a social-engineering experiment targeting the US intelligence and defense communities with a fictitious cyber character. The fictitious persona posted photos of an attractive young woman with profiles created to appeal to government and cleared defense contractors. During the 28-day operation, more than 550 people, including very senior government officials, interacted with the fictitious female through several SNSs. The profile also attracted several senior defense contractors within Lockheed Martin, Northrop Grumman, and Booz Allen Hamilton. In one instance, the fictitious female managed to get sensitive information and photos with geo-locational information from a US Army Ranger in Afghanistan.

Current DOD social media policies. Current DOD policy, as well as the *Uniform Code of Military Justice*, require personnel to follow certain rules when publishing information on public websites.[16] These rules, however, are not intended to limit free speech. Instead, rules are there to ensure DOD members do not compromise sensitive information or OPSEC. For example, disparaging senior government officials, revealing operational details, or divulging classified information are offenses punishable under the *UCMJ*. Thus, the issue the DOD is grappling with is how to allow full access to SNSs while at the same time minimize the risks. In 2010, the DOD released a policy memorandum on the use and access to Internet-based capabilities including SNSs—DTM 09–026. This policy was later superseded by DOD Instruction 8550.01, DOD Internet Services and Internet-based Capabilities in 2012. According to this latest DOD chief information officer guidance:

> DoD Internet services and IbC [Internet-based Capabilities] used to collect, disseminate, store, or otherwise process DoD information shall be configured and operated in a manner that maximizes the protection (e.g., confidentiality, integrity, and availability) of the information, commensurate with the risk and magnitude of harm that could result from the loss, compromise, or corruption of the information.[17]

Even though the DOD social media policy does not require organizations to have a presence in SNSs, it has an entire hub dedicated to social media.[18] The Army alone has hundreds of registered FaceBook pages. Thousands more comprise the collection of Army, Navy, Air Force, and Marine pages, mostly Facebook, Twitter and Flickr pages that are listed on the online registry.

AFI 1-1, Air Force Culture, updated on November 2014, is the only recent policy that briefly addresses behavioral best practices on SNSs within the Air Force. According to AFI 1-1, every Airman is personally responsible for what they say and post on SNSs. So where does that leave commanders? AFI 1-1 addresses both OPSEC concerns and the responsibility of each Airman to protect sensitive information from public disclosure, but it does not set policy for protecting networks against the technical threats posed by SNSs.

Problem Statement

Today, the only official Air Force regulation that briefly addresses the OPSEC concerns posed by SNSs is buried on page 21 of AFI 1-1. The "Air Force Social Media Guide" offers Airmen and their families some guidance on the appropriate use of SNSs, but neither of these publications addresses the technical risks and possible mitigations associated with this medium.[19] The Air Force does not have a coherent policy, regulation, or instruction specifically governing the use of SNSs. Current Air Force web policies and instructions are currently under revision to address operational and procedural changes involving public and private web content and may soon offer better guidance and policy addressing the use of SNSs. Without concrete and up-to-date official guidance, however, and considering all the risks discussed herein, how can Air Force commanders balance appropriate security measures to protect information and sensitive operations while taking advantage of the Internet-based capabilities SNSs can to offer our personnel?

Recommendations

1. The Air Force must ensure that the Nonclassified Internet Protocol Router Network (NIPRNET) is configured to maximize technical security. To better protect DOD networks from Internet technical threats, the National Security Agency's Systems and Analysis Center[20] offers recommendations and best practices for the use of social media. Their recommendations for technical best practices include:

   a. Ensure operating systems and web browsers are up-to-date with the latest patches. Maintain a blacklist of blocked sites for the network.

   b. Update virus scanners with the latest definitions and patches, and scan often.

   c. Do not browse the Internet from privileged accounts such as root or administrator.

   d. Enable data execution prevention in the operating system to prevent buffer overflow attacks.

   e. Install an application firewall or host intrusion prevention system and enable whitelisting.

   f. Apply software restrictions policies (SRP) on machines running Microsoft Windows platforms (most Air Force workstations run Windows platforms). SRP keeps a white-list of allowed executables, preventing the installation of malicious downloads.

2. SNSs offer vast amounts of information that adversaries can use to gather intelligence or to exploit DOD operations and personnel. The latest DOD Internet Services and Internet-based Capabilities Instruction, DOD Instruction 8550.01, states that "DoD employees shall be educated and trained to conduct both organizational and individual communication effectively to deny adversaries the opportunity to take advantage of information that may be inappropriately disseminated."[21] Although most technical threats posed by SNSs can be mitigated through the proper use of security measures already in place in most Air Force networks that is perimeter defenses, firewalls, and so forth, information and operations security hinges mainly on the OPSEC and INFOSEC mindset of each and every Airman, and their willingness to divulge—whether intentionally or unintentionally—sensitive information in public forums. Based on the evolving global nature of SNSs and the increasing vulnerabilities brought about by a lack of OPSEC and INFOSEC awareness, it is increasingly evident that the Air Force must step up its OPSEC and INFOSEC training as it

relates to SNSs. This training must be continuously emphasized throughout an Airman's career. Social media INFOSEC/OPSEC awareness training must become a mandatory annual or biannual training. This training must include OPSEC lessons learned, as well as SNS behavioral best practices and possible repercussions for posting inappropriate content online. The Air Force must train its Airmen to refrain from posting personally identifiable information or any information that could reveal sensitive military operations or compromise security. A good training resource for commanders is the Joint OPSEC Support Element at Joint Base San Antonio–Lackland, Texas, which offers OPSEC training materials and resources, some of which now focus on social media.

3. The Air Force must draft policy that specifically addresses the risks and vulnerabilities that come with the use of SNSs. This policy should spell out general guidance for SNS technical and behavioral best practices, social media INFOSEC/OPSEC training standards, and possible consequences or disciplinary actions for violating OPSEC principles on social media. Also, this policy should be broad and flexible enough to be able to adapt to the evolving nature of SNSs. In *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce*,[22] the authors offer some excellent recommendations that address SNS threats and mitigations.
4. Finally, every commander must ensure that any official website or SNS presence be vetted through the proper Air Force public affairs (PA) office and that it meets Air Force web policies. However, this may prove to be a challenge at units that do not have a PA representative.

If used in concert, technical best practices, along with an increased emphasis on OPSEC and INFOSEC awareness training, can help minimize the risks of exposing privileged, sensitive, or even classified information, to adversaries and cybercriminals.

Conclusion

Despite all the vulnerabilities and technical risks associated with SNS, it is unrealistic to attempt to block access to the ever-growing number of SNSs and expect our networks to be safe from attacks and exploits. Instead, the DOD and the Air Force should focus on regulating, not restricting, social media use. DOD and Air Force SNS policies should be broad and flexible enough to be able to adapt to the evolving nature of SNSs. There are proven technical mitigations and best practices that, when properly followed, can offer a strong defense against adversaries. A proper social media OPSEC/INFOSEC awareness training campaign, coupled with robust security features within the DODIN, can go a long way in protecting USAF personnel, networks, and missions while allowing service members access to sites that promote real-time information and collaboration opportunities. The DOD's challenge is to come up with a permanent social media policy that is broad and flexible enough to fill all the security gaps that have emerged, and will continue to emerge as SNS evolve. This task won't be easy but, as Corrin stated,[23] SMSs have become too powerful as an information and strategic messaging platform to be dismissed or ignored. ✪

Notes

[1] National Archives Records Management Information Page, Bulletin 2014-02, *Guidance on Managing Social Media Records*, Archives.com, 4 March 2017, https://www.archives.gov/records-mgmt/bulletins/2014/2014-02.html.

[2] DOD Directive-Type Memorandum 09-026, *Responsible and Effective Use of Internet Capabilities*, 25 February 2010, http://www.dodlive.mil/files/2010/02/DTM-09-026.pdf.

[3] Tom Budzynam, "Social Media Shapes Markets, the Military and Life," American Forces Press Service, 31 August 2010, http://archive.defense.gov/news/newsarticle.aspx?id=60665.

[4] Air Force instruction 35-101, *Public Affairs Policies and Procedures*, 12 January 2016, 20.

[5] US Army, *The United States Army Social Media Handbook* (Washington: Office of the Chief of Public Affairs, 2016), 3, https://www.army.mil/e2/rv5_downloads/socialmedia/army_social_media_handbook.pdf.

[6] Robert Shullich, *Risk Assessment of Social Media*, Global Information Assurance certification paper, Escal Institute of Advanced Technologies (SANS), 5 December 2011, https://www.giac.org/paper/gsec/4307/risk-assessment-social-media/106672.

[7] National Security Agency Information Assurance Directorate, Pamphlet MIT–005FS–2013, "Best Practices for Keeping your Home Network Secure," May 2014, http://dodcio.defense.gov/Portals/0/Documents/Cyber/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure_Web_update.pdf.

[8] DOD Instruction (DODI) 8550.01 (2012), "DOD Internet Services and Internet-based Capabilities," 11 September 2012, http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf.

[9] SANS Institute, "Information Security Resources," 7 March 2017, http://www.sans.org/information-security/?portal=75a38dd7be0670333f6c90d44771 436b.

[10] Amber Corrin, "DOD's New Policy "Likes" Social Media, but with Caveats," FCW.com, 14 August 2012, https://fcw.com/articles/2012/08/15/feat-inside-dod-social-media-policy%20.aspx.

[11] Lt Col Bertrand Boyer, "Countering Hybrid Threats in Cyberspace," *The Cyber Defense Review*, 15 February 2017, http://www.cyberdefensereview.org/2017/02/15/countering-hybrid-threats-in-cyberspace/.

[12] Sharon Gaudin, "Half of Social Networkers Post Risky Information, Study Finds," *Computerworld*, 4 May 2010, http://www.computerworld.com/article/2517936/social-business/half-of-social-networkers-post-risky-information--study-finds.html.

[13] Shullich, *Risk Assessment.*

[14] Ibid.

[15] Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl, "Advanced Social Engineering Attacks," *Journal of Information Security and Applications* 22 (2015): 113–22.

[16] Office of Government Ethics Legal Advisory 15-03, "Social Media Education and Training;" Claudette Roulo, "Social Media Polices Protect DOD Employees, Official Says," American Forces Press Service, 22 April 2013, http://archive.defense.gov/news/newsarticle.aspx?id=119840.

[17] DODI 8550.01, DOD Internet Services.

[18] DOD chief information officer, "DOD Social Media Hub," 7 March 2017, http://dodcio.defense.gov/Social-Media.

[19] Air Force Public Affairs Agency, "Air Force Social Media Guide," 4th ed., 2013, http://www.af.mil/Portals/1/documents/SocialMediaGuide2013.pdf.

[20] NSA Information Assurance Directorate, Pamphlet MIT–005FS–2013, "Best Practices for Keeping Your Home Network Secure," May 2014.

[21] DOD Instruction 8550.01, DOD Internet Services.

[22] Panayotis A. Yannakogeorgos and John P. Geis II, *The Human Side of Cyber Conflict: Organizing, Training, and Equipping the Air Force Cyber Workforce* (Maxwell AFB, AL: Air University Press, 2016).

[23] Corrin, "DOD's New Policy," 2.

Lt Col Dieter A. Waldvogel

Colonel Waldvogel (BA, Texas Tech University; MA, Embry Riddle Aeronautical University; and PhD, University of Texas–Austin) is a cyberspace operations officer, a senior Latin America regional affairs strategist, and currently a professor of foreign languages at the US Air Force Academy (USAFA), Colorado. Colonel Waldvogel is the director of assessments in the Department of Foreign Languages and International Programs at the Academy. As a cyberspace operations officer, the colonel served in leadership positions with the 789th Communications Squadron, Air Force Space Command Headquarters Directorate of Logistics and Communication, 379th Air Expeditionary Wing Mission Support Group, and the National Security Agency/Information Assurance Directorate.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

http://www.airpower.au.af.mil

The *ASPJ* staff would like to correct the following errors in the Spring 2017 edition:

1. On page 30 of the article "Air Mines: Countering the Drone Threat to Aircraft" an editing error resulted in a sentence reading ". . . stealth aircraft, such as the very large B-52. . .". The sentence should be corrected to read ". . . stealth aircraft like the B-2 bomber that has a very large dimension of. . .".
2. Due to an error at the contract printers, some hard-copy journal editions had pages 17–32 inverted.