REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05-14-2010	**FINAL**	

4. TITLE AND SUBTITLE

Balancing Social Media with Operations Security (OPSEC) in the 21st Century

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Adrian Bejar

Paper Advisor (if any): Professor Sweeney, JMO Instructor.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Naval War College
686 Cushing Road
Newport, RI 02841-1207

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES **A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.**

14. ABSTRACT

The use of social media and networking sites like Facebook, MySpace, and Twitter have revolutionized the way the world is communicating. The ability to share information at a moment's notice has truly impacted American lives forcing a dependence on sharing personal information. The Department of Defense (DOD) has embraced these new communication tools and set policy on allowing internet-based capabilities on all government networks. The new policy permits Web 2.0 social networking sites such as Facebook and Twitter to be used. The Department of the Navy (DON) has quickly adopted the policy and is utilizing social networks as methods to provide the public with a transparent view of the Navy's mission and daily operations. This new method of information sharing may seem harmless but there is an increased risk to Operations Security (OPSEC). The Operational Commander must safeguard his critical information and prevent any comprise of vital information. The lack of measures in place to support the use of social media and the ability for the user to quickly share information causes the Commander to contend with issues of control, security, and standardization making his ability to conduct OPSEC much more challenging.

15. SUBJECT TERMS

Operations Security, OPSEC, Internet, Social Media, Social Networking, Cyber, Public Affairs, COMSEC, Monitoring

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Department
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**		**28**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3414

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

BALANCING SOCIAL MEDIA WITH OPERATIONS SECURITY (OPSEC) IN THE 21st CENTURY

By
Adrian Bejar
Lieutenant Commander, United States Navy
Seminar #6

An essay submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Strategy and Policy Department.

The content of this essay reflect my own personal views and are not endorsed by the Naval War College or the Department of the Navy.

Signature: _____

03 May 2010

TABLE OF CONTENTS

List of Illustrations

ABSTRACT

The use of social media and networking sites like Facebook, MySpace, and Twitter have revolutionized the way the world is communicating. The ability to share information at a moment's notice has truly impacted American lives forcing a dependence on sharing personal information. The Department of Defense (DOD) has embraced these new communication tools and set policy on allowing internet-based capabilities on all government networks. The new policy permits Web 2.0 social networking sites such as Facebook and Twitter to be used. The Department of the Navy (DON) has quickly adopted the policy and is utilizing social networks as methods to provide the public with a transparent view of the Navy's mission and daily operations. This new method of information sharing may seem harmless but there is an increased risk to Operations Security (OPSEC). The Operational Commander must safeguard his critical information and prevent any comprise of vital information. The lack of measures in place to support the use of social media and the ability for the user to quickly share information causes the Commander to contend with issues of control, security, and standardization making his ability to conduct OPSEC much more challenging.

INTRODUCTION

The Information Age in the 21st Century has transformed the way we communicate and how we share information through the internet. Advanced information systems created a culture reliant on quick and autonomous sharing of information made possible with cell phones, computers, personal digital assistance devices, and wireless media. The continual expansion of media technology has introduced social networking to the general population with the ability to access split second information. Social media sites have connected and impacted people globally in ways never anticipated since the inception of digital media and the World Wide Web. Military personnel are equally influenced by social media and social networking. The next generations of recruits who are born into the digital age are instinctive to technology like social media and expect a highly technological military to embrace this innovation. On 19 February 2010, The Department of Defense (DOD) announced it was permitting internet-based capabilities on all government networks and allowing the use of social networking sites such as Facebook, MySpace, and Twitter.[1] With the increased concern of cyber security the new policy comes with tremendous risk and immediately challenges Operations Security (OPSEC).

This examination will consider the impact of social networking in the Department of the Navy (DON) and the scope of issues the Commander will contend with. The Department of Defense's decision to allow social networking provides various benefits but opens the Commander to many inherent risks to Operations Security. The Department of the Navy (DON) is unprepared to apply social media across the fleet. The fast transition to adopt internet-based capabilities has not allowed social media measures to be implemented, ultimately increasing OPSEC risk in the areas of social media policy, security, and control.

The result is unclear guidance, non-standardization, little oversight, and an opening to cyber exploitation. The paper will conclude that by standardizing the use of social networking through clear guidance, education and training, and enduring processes the Commander can prevent the inadvertent compromise of sensitive or classified U.S. Government information, activities, capabilities, or intentions to the public and our enemy.

BACKGROUND

Facebook, Twitter, and MySpace are social networking sites that have exploded in popularity globally and throughout the United States. At the start of 2010 there were over 113,000,000 million personnel registered on Facebook in the United States with approximately 55 percent being between the ages of 18-44.[2] The average age of a military service member is about 28 with the main demographic of the service being between the ages of 18-30 years.[3] With such a young composition, social networking is certainly not alien to the military. Blogging or Milblogging has been around for many years initially using the web to establish social platforms. Blogging especially increased during the start of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) allowing military service members to talk about their experiences.[4] Government networks at the time prevented blogging activity as a result blogging was not considered high risk. The new social networking internet applications surpass blogging making the ability to control critical information more difficult.

Social media and social networking should not be confused as the same thing. As Lon S. Cohen, a marketer, communicator, and freelance writer attempts to explain with a post on his blog, "even though these terms are used interchangeably, there is a big distinction between social media and social networking to the point which both can be separated by

websites representing one or both."[5] Cohen breaks down each word and defines them according to Dictionary.com:

- Social: 1. pertaining to, devoted to, or characterized by friendly companionship or relations: a social club.[6]
- Networking: 1. a supportive system of sharing information and services among individuals and groups having a common interest: Working mothers in the community use networking to help themselves manage successfully.[7]
- Media: 1. a pl. of medium. 2. (Usually used with a plural verb) the means of communication, as radio and television, newspapers, and magazines that reach or influence people widely: The media are covering the speech tonight.[8]

Cohen further defines social media as the strategy or means for broadcasting, while social networking is the act of connecting with people.[9] We have seen social media in many forms such as ARPANET, LinkedIn, YouTube, and to its maturity of today with Facebook, MySpace, and Twitter made possible using Web 2.0 technology. This paper will primarily focus on social networking and the OPSEC challenges Web 2.0 products confront the Commanders as the military embraces Facebook, Twitter, and MySpace. The challenge is how to apply policy smartly with OPSEC to mitigate risk and prevent potential violations.

Operations Security plays a major role in the daily routine of military operations. President Ronald Reagan identified a need for OPSEC and signed the National Security Decision Directive (NSDD) 298 establishing a National Operations Security Program to assist in OPSEC planning and prevent the inadvertent compromise of sensitive or classified U.S. Government information, activities, capabilities, or intentions.[10] The OPSEC program is a systematic five step process which includes the following: 1) Identification of Critical Information 2) Analysis of Threats 3) Analysis of Vulnerabilities 4) Assessment of Risk and 5) Application of Security Measures.[11] OPSEC is now more than ever a paramount concern for the Commander, given that the ability for each service member to easily share critical

information to the general population is likely. OPSEC must become routine and always part of your planning and daily operations. Operation Overlord, the Allied invasion of Normandy, is an example of properly executing OPSEC to successfully achieve an objective.[12] The military deception (MILDEC) plan as part of Operation Overlord combined with protecting Allied operational information was vital to its execution. However, when OPSEC is poorly conducted it usually results in an undesired operational outcome as the DOD discovered in the Vietnam Conflict. During Vietnam from 1966-1967, battle damage assessments (BDA) of high aircraft losses were assessed to be due to leaks of classified information, but after further investigation by the CIA and NSA Purple Dragon agency it was determined that the poor handling of sensitive unclassified information and the routine practices of Air Force operations lead to the high loss of aircraft.[13] This investigation eventually led to NSDD 298 and the start of the National OPSEC Program. OPSEC will be the Commanders primary concern as social media utilization becomes routine for daily operations.

The National Security Decision Directive 298 not only defined the five Step OPSEC process, but also established a lead agency for interagency training. The National Security Agency was tasked as the executive agent to spearhead the OPSEC program and mandated to establish the Interagency OPSEC Support Staff (IOSS) as a consultant to the U.S. Government.[14] The IOSS would be a staff consisting of representatives from the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Department of Energy, Department of Homeland Security, and Department of Defense, including the National Security Agency. The Department of Defense published DOD Directive 5205.02, titled as the DOD Operations Security (OPSEC) program manual and was recently updated as of

2008, to reemphasize NSDD 298 directives. The 2008 directive encompasses requirements for the release of information on websites and web-based applications. Directive continues to reference a dated 1998 Deputy Secretary of Defense Memorandum titled "DOD Web Site Administration Policies and Procedures."[15]

The Department of the Navy published and established OPSEC guidance for the fleet by releasing OPNAV Instruction 3421.1. The Navy's instruction was eventually a foundation for the Navy's tactics, techniques, and procedures (NTTP) 3-54M/MCWP 3-40.9 published in March of 2009. The NTTP assist the command OPSEC officer/planner at the Maritime Operations Center (MOC) at the operational and tactical level of war. Additionally, the Joint Publication 3-13.3 provides Joint Operations Security doctrine for the Joint Task Force Commander. There is no shortage of OPSEC instructions available to the Commander for reference, supplying the process to make wise OPSEC decisions during day-to-day activities and during operational planning. However, there is a lack of detailed guidance and measures for new internet-based capabilities in support of OPSEC. The updated Navy NTTP does include chapters on Web Page registration, Web risk assessment, and Red Team assessment, but it is very limited on information on how to approach social networking sites.[16]

In April of 2003, the Department of Defense revealed an Al Qaeda training manual claimed that 80 percent of their information was obtained from open source material.[17] The Secretary of Defense, Donald Rumsfeld, was concerned about possible vulnerabilities that could be found on our networks and issued a message entitled: Web Site OPSEC Discrepancies.[18] His concerns eventually shaped the Department of Defense's posture on unclassified systems, but stopped short of banning internet applications on DOD networks.

The new policy permitting internet-based capabilities allowing the instant exchange of information on publicly accessible websites is an increased risk to OPSEC. The possibility that a single user may piece small items of information into a product that contains sensitive or classified information is more evident today (Refer to Figure 1). Accepting this risk has become and remains a debate for senior leaders in the armed services.

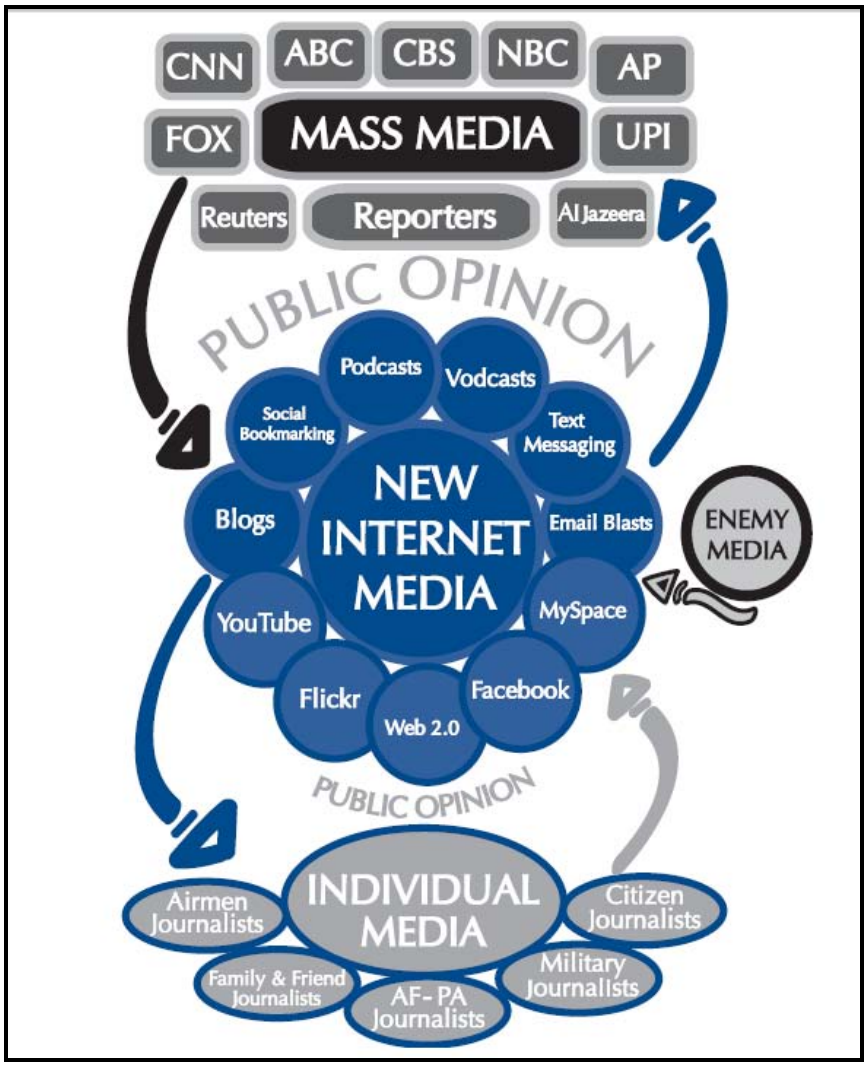

Figure 1. Media Chart. Air Force product reflecting new media products influenced by multiple factors, both from individual and mass media.[19]

Social Media Debate

On 26 February 2010, the Pentagon announced all users on unclassified .mil computers will be allowed to access social media.[20] This decision did not come lightly. The

Pentagon in the last several years had been struggling on how to grant service members, access without compromising information and maintain security to over 15,000 Defense Department computer networks. David Wennergren, the Pentagon's Deputy Chief Information Officer, justified lifting the ban by stating the Pentagon submitted to "the power of information sharing, the power of collaboration, to get the right information to the right person at the right time so you can make better decisions more quickly."[21] Thus, the DOD trusts the workforce to make smart decisions or choices on what they access and to closely monitor their use at the local level.

The ban reversed three years of inconsistent policy on social media. The Navy was open to using social networking sites, while the Marine Corp was opposed and in August of 2009 issued a directive banning access to all social media sites.[22] All services had implemented separate policy on social media and will continue until a standard DOD policy is provided. Many officials argue the cost and risk is too high, degrading our ability to safeguard our information as we provide our adversaries the perfect conduit to collect information, and the ideal "digital dumpster diving" environment for Open Source Intelligence (OSINT).[23]

The Department of Defense's sudden shift in policy is primarily two reasons, 1) the transition from the Bush administration to President Obama's administration and his policy on an open and transparent government and 2) the next generation of incoming sailor is born in a culture of social media honing skills that can benefit the DOD. The new administration has driven the Department of Defense into a new direction and the Secretary of Defense, Robert Gates, is carrying out the administration's policy diligently, requesting an open and transparent department and requiring each service component to comply.[24]

Social Networking Directives and Policy

President Obama signed his memorandum for Transparency and Open Government on January 21, 2009. In December 2009, Director Peter R. Orszag, Officer of Management and Budget, released a memorandum to all heads of executive departments and agencies in support of the President's policy. The memorandum outlined the way ahead to transparency, stressing the following key areas: How to Publish Government Information Online, Improve the Quality of Government Information, Create and Institutionalize a Culture of Open Government, and Create an Enabling Policy Framework for Open Government.[25] The federal government responded without delay, utilizing collaborative social media tools to engage the public. The Federal Chief Information Officer, Vivek Kundra, stated "Web 2.0 technologies are essential to tap into the vast amounts of knowledge…in communities across the country."[26]

In 2009 the Federal CIO Office led a working group to identify guidelines for a secure use of social media by Federal departments and agencies. The working group recognized four specific types of social media use within the Federal Government: Inward Sharing, Outward Sharing, Inbound Sharing, and Outbound Sharing.[27] Having a social networking footprint for sharing information to the public was categorized as Outbound Sharing, which also was determined to have a lack of guidance.[28] One directive recently published to correct this flaw is the Department of Defense Directive-Type Memorandum (DTM) 09-026 titled Responsible and Effective Use of the Internet-Based Capabilities. A broadly written memorandum, permitting the use of social media on DOD networks and implies the responsibility falls on the commander to monitor and ensure good OPSEC. Besides DTM 09-026 there is no supplemental guidance available to support the

implementation policy of new Web 2.0 tools. With Social Networking sites like Facebook, MySpace, and Twitter presently being used and implemented this gap needs to be filled rapidly to provide the Commander with the necessary tools to safeguard critical information.

Social Media Policy Gaps

Commands throughout the Navy are presently employing social media, in particular Facebook, to provide the transparency expected by the SECDEF and begin to inform the public of command missions and daily activity. Commands will be forced to use their personal expertise to manage Facebook or will be inclined to duplicate other command sites. However, an arbitrary template and limited expertise permit unintended vulnerabilities and consequences. The only guidance available to Navy commands is DTM-0926 and SECNAV Instruction 5270.47B, the Department of the Navy's Policy for Content of Publicly Accessible World Wide Web Sites. The Navy is undertaking the transition to social media and networking at such a great speed that policy and regulations are not keeping up. An update to SECNAV Instruction 5270.47B published in 2005, is necessary to reflect current DOD policy to provide basic language on website usage and impose a sense of standardization across social networking sites such as Facebook and Twitter.

Commanders should be able to understand their responsibilities and the resources available to answer critical questions. The role of the newly established United States Cyber Command (USCYBERCOM) and Fleet Cyber Command (FLTCYBERCOM), Tenth Fleet is currently being resolved but should play a vital role in making policy decisions. Guidance would have to identify the relationship between Network Warfare Command (NETWARCOM) who holds network operations (NETOPS) task and with FLTCYBERCOM who possesses OPSEC and Computer Network Operations (CNO)

responsibilities under Information Operations. A combined concept of operations with a priority on OSPEC will be ideal in the immediate future for the fleet to properly safeguard information.

A study conducted by the JANSON Communications Group, to evaluate the content of military Facebook pages from the user's point of view, revealed that standards did not exist for the fleet and Commanders were working off best practices being shared. JANSON's study evaluated 682 military Facebook pages revealing several disparities. Key findings to highlight are:

> "only 22% of pages studied had clear terms of use posted delineating what is acceptable behavior and comments on the page, 4% of the pages examined had no content or had not been updated for several months resulting in "zombie" pages though many more were excluded from the study data set, and many military Facebook pages were not clearly marked as "official" and can be confused with the larger number of unofficial and "clone" pages that look like government sponsored pages but may contained inaccurate and inappropriate content."[29]

JANSON's study illustrates the challenges the Navy has ahead as an organization to perfect their social media program. It is important that the Commanding Officer understands their role and authorities in monitoring social media usage or content.

Social Media Control Issues

Current directives place the responsibility on the Commander for monitoring content on their sites and providing the necessary oversight during usage. The ability for the commander to control or monitor the network is limited. The current policy is not clear on what those oversight limitations or restrictions are for monitoring social media. Historically, the Naval Security Group (NAVSECGRU) was the agent mandated in communication security (COMSEC) monitoring. This mission overtime became negligible as NAVESECGRU converted to NETWARCOM and priorities shifted.[30] Now,

USCYBERCOM and FLTCYBERCOM will have to revive dialogue and work with commands such as the Joint Communication Monitoring Agency (JCMA) to identify specific standards for monitoring social networking. The policy is vague and open to interpretation that Commanding Officer can be placed into complicated freedom of expression or privacy situations. This dilemma was evidenced recently by senior military leaders from Marine Corps Base Camp Pendleton, as a young Marine Sergeant's personal Facebook comments about the Presidents Administration sparked debate across the country.[31]

As USCYBERCOM establishes itself and becomes engaged it hopefully will readdress the importance of COMSEC. Until progress is made, the reality is JCMA, also tasked with monitoring DOD communications, is the only agency that can perform this now expanded role of monitoring social media sites.[32] JCMA is a small agency and like every organization manpower limitations do not support expansion. The sheer number of social networking sites alone would require large bandwidths of information for JCMA to analyze. There is a need to provide the Operational Commander with the means to carry out his or her own monitoring in support of OPSEC. If not provided, Operational Commanders will rely on other means, such as Judge Advocate Generals (JAG), to determine limitations or boundaries before crossing the line into privacy issues and violating the Freedom Intelligence Surveillance Act (FISA) of 1978.

If the Commander does not have a solid monitoring or oversight program, which should be supported by the OPSEC team, the ability to control content or information onto a site becomes a challenge and an increased OPSEC risk. As the saying goes "loose lips sink ships" or "the enemy is listening…he wants to know what you know" are quite relevant under these circumstances. Swap listening with networking and the phrase still applies. The

enemy throughout history has sought ways to discover critical information in order to compromise operations. This has been accomplished by intercepting unclassified communications, listening to sailors at the local bar, or as easy as reading unclassified email. Social networking sites like Facebook and Twitter are ideal settings for providing Open Source intelligence (OSINT). Without strict guidance or a form of standardization, the Department of Defense will be operating in disorder and the rules will be written on a daily occurrence. A very dangerous method of functioning that only leads to failure.

Without guidance or standardization we expose ourselves to failure and risk that is unacceptable, as the Israeli's recently experienced when they were forced to cancel a military operation after an Israeli soldier inadvertently exposed vital information about the raid on his Facebook page.[33] Networking sites, like Wikileaks, an organization that publishes anonymous information and leaks sensitive documents, are waiting for the military to be complacent in order to capitalize off leaked information. As demonstrated recently, Wikileaks released footage of an Iraqi video showing an Apache helicopters engaging the enemy and accusing soldiers of killing innocent civilians including two journalists.[34] The Secretary of Defense (SECDEF) and the Chairman of the Joint of Staff (CJCS) quickly responded and came to the Army's defense by making public comments on the incident.[35] The Public Affairs office is quickly realizing the second order of effects from social networking has many consequences since content not closely monitored can affect strategic communication messages or information operation themes. Incidents like these are unfortunately common and could easily be prevented. Our military personnel are not immune but actually become favorable targets to our adversary. It only takes one individual not respecting information or operation security to supply an open door for hackers.

Social Media Security Risk

Social networking sites, in particular Facebook, are commonly known to have weak security settings.[36] This vulnerability bypasses essential system security checks and in turn allowing hackers easy access to attempt spear phishing, social engineering, zero-day attacks, and denial of service. The United States is the leading country in Facebook usage, but with it comes a high rate of penetrations, approximately 30 percent.[37] As previously discussed, adversaries prefer these conditions. The ability to collect intelligence over the internet is cheaper and easy to exploit. In a typical scenario, an adversary can collect critical information by targeting a known individual through blogs or social media sites.[38] In turn these sites provide other links which the user participates in. In a matter of seconds our adversary is on Flickr photos browsing pictures and maintains updates through Twitter.[39] The user then tweets the status of their location, allowing our adversary to physically conduct surveillance closely on their target. At this point our adversary has no limitations collecting on their target.

According to Network Security Edge, an IT Intelligent Agent provider, they identified five social media security issues: "lack of a business policy or lack of enforcement of the policy, friending someone you don't know, not thinking twice about clicking on links, letting hijackers into accounts, and third-party application dangers."[40] Each issue lends itself to a vulnerability letting the hacker retrieve passwords or personal information. Additionally, hackers clone and spoof Facebook sites to steal passwords or collect information.[41] Plus, third party application allows for potential spreading of malware from "trusted" sources.[42] OPSEC must become a priority for operating and planning social media. The Navy must quickly recognize its shortfalls to mitigate risk in order to gain the benefits and advantages of

social media, as our senior navy leaders have accepted. ADM Roughead, Chief of Naval Operations, has stated "Social Media is another tool we can use to get a better look into the future and help us become a more effective Navy."[43] The DOD and service components are taking advantage of social media products to engage the public and support maritime security cooperation.

Social Media Advantages

There are obvious benefits in using social media and social networking to support and carry out the daily mission of the DOD. The State Department has embraced social media to support their mission of public diplomacy.[44] The State Department's ability to inform, influence, and engage a foreign population can now be achieved without leaving the office. Social media has become a means that has amplified the way the State Department is interfacing with foreign countries. Many other government agencies are using social media to educate, train, and inform the public. Social media Web 2.0 products such as Facebook and Twitter allow the Navy to connect and reach audiences not normally accustomed too, promoting public interaction. The next generations of sailors are regulars to the information age and have skills the Navy can draw on. Most recently, the Navy has used social media as a tool in public affairs in support of the Maritime Strategy.[45]

Maritime missions such as Humanitarian Assistance are using social networking to get the Navy message out in support of the overall strategic objective. The latest example would be Operation Unified Response during the devastating tragic earthquake in Haiti, social networking pages like Facebook were essential in informing the public of the daily progress being conducted (Refer to figure 2). This not only provided real time information but promoted the Navy in a positive way to the general population. Social networking

successes like Haiti are messages which in turn support recruiters in seeking out potential enlistees. Recruiting districts across the nation are using Social networking to attract people to the service. Social networking allows recruiters to build relationships with potential candidates without the intimidation of a recruiting office or the recruiter themselves. However, there is still an inherent risk to government transparency and open access to social networking making the system vulnerable to attack or collection.

Figure 2. JTF-HAITI Facebook Web Site. Web site was used as source of information after a US response, at the request of the Haitian government, during the devastating earthquake that struck Haiti on Jan 12, 2010.[46]

Even though there are many benefits to reap by using social media applications, we cannot get complacent by forgetting the key elements of OPSEC. The new policy creates a critical vulnerability that can be exploited. There is obviously an increased risk that materializes in which the potential of compromising sensitive information is imminent, the potential for our adversaries ability to conduct cyber attacks increases, and an expansion in

our efforts to self-monitor ourselves needs to be maintained. These critical vulnerabilities mentioned can easily be mitigated or corrected by focusing our efforts on producing clear guidance, hardening our network security, improving our processes, and providing the resources for oversight.

RECOMMENDATIONS

This paper has examined the various challenges that come with a new social media policy. OPSEC must be a priority for all Commanders and should be a term associated with social media at all times. The Department of Navy should consider phasing access to all Navy networks or echelons until measures are produced to provide overarching guidance. As part of that process the following recommendations are highly advised.

Standardization

Commanders are always concerned with OPSEC. To make well educated decisions the Commander must have clear guidance to achieve their objectives. Current doctrine does not clearly state the Navy's intention or processes to assist the Commander in making good choices in implementing internet-based capabilities. As identified in the Facebook Military Study, by JANSON Communications, there was lack of standardization from most sites was common.[47] From their findings, JANSON Communications suggested achievable recommendations that the Navy should consider in their next policy and directives. Key recommendations to highlight which support standardization throughout the navy are to "clearly identify command or agency sites as "official," provide a standard naming conventions for commands to use, provide guidance and define clearly what is acceptable and not appropriate use for a site, mandate a periodicity for maintaining sites and require updates, determine limitations and restrictions if site is being used as a Command intranet,

provide guidance on supporting resources and training, provide the Commander with the means of monitoring a site and the limitations in authority." [48]

Processes

All services, including the Navy, have been dealing with Milblogging in the past and many best practices have been used to mitigate blogging issues. Any existing blogging or web best practices should be integrated with newly developed social media policy. Additionally, sharing information and concepts with other services, for instance the Air Force, could enhance Navy Policy. Consideration should be given in adopting the Air Force Web Posting Response Assessment chart and revise it to reflect a Social Media context (Refer to figure 3). The assessment at least provides the Commander with a process to make his decisions and provide a better understanding for operators. As the Navy considers these processes, a working relationship between experts in Public Affairs, Network Operations, and Information Operations are essential to good OPSEC.

Monitoring and Oversight

The Commander's ability to monitor his networks is limited, a vital effort in OPSEC and ensuring sensitive information is not compromised or action can be taken quickly. However, he can achieve this objective in several ways. One, he can mandate that his OPSEC program include a Red Team that conducts self monitoring for his unit on a periodic basis. Second, reemphasize the process in requesting and offering COMSEC services. In OPNAV Instruction 2201.3B of 14 Apr 2009, the Chief of Naval Operations delineates responsibility to the following: "Only authorized personnel assigned to Navy Information Operations Command Norfolk, Navy Cyber Defense Operations Command, or other commands authorized by Commander, Navy Network Warfare Command (COMNAVNETWARCOM), as the Navy's designated service cryptologic element, will conduct activities such as red/blue

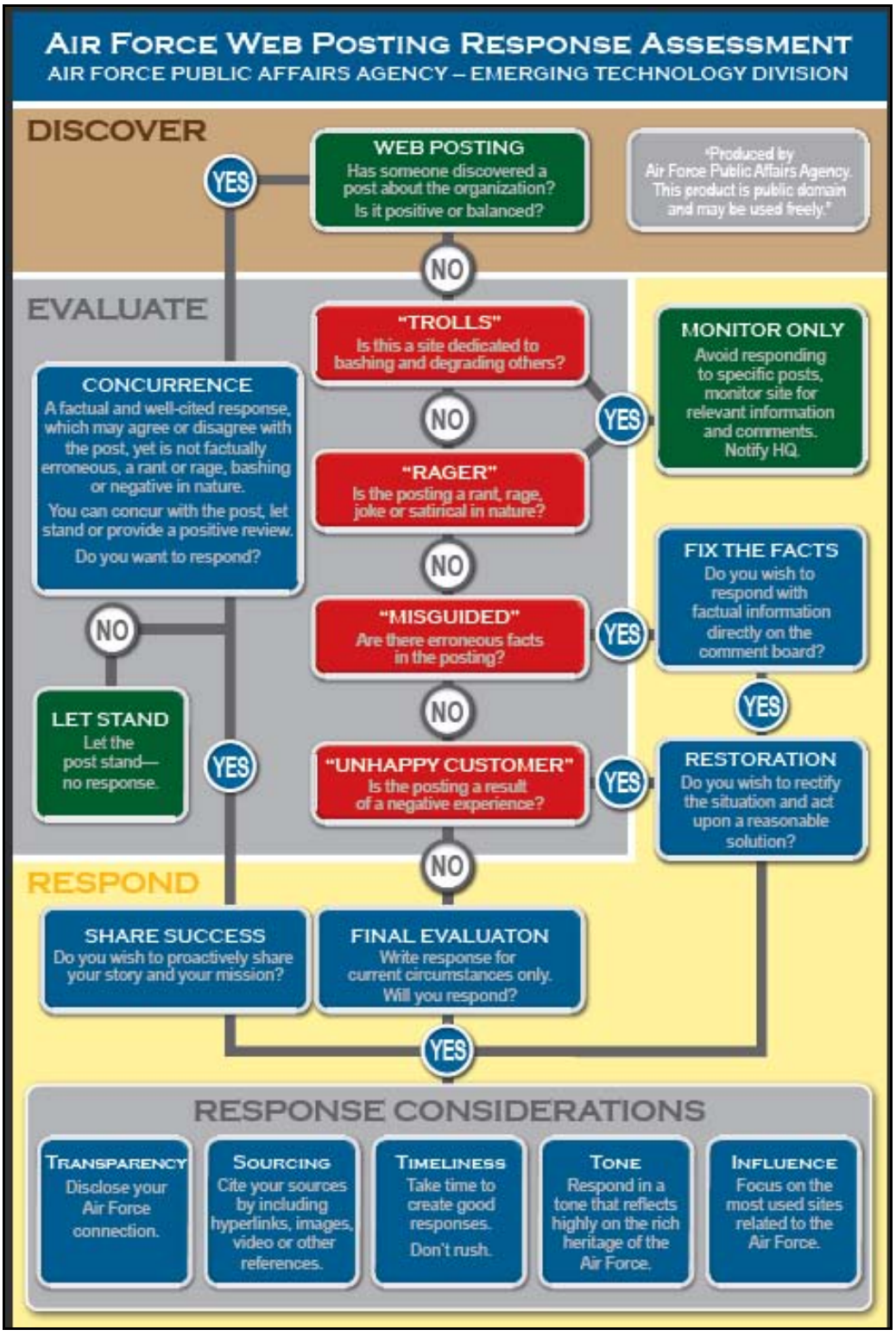

Figure 3. Air Force Web Posting Response Assessment. A product of the Air Force Public Affairs Agency Emerging Technology Division.[49]

team operations or other activities that would constitute COMSEC monitoring under the auspices of the current definition." Commanders should work with their local Navy Information Operation Command (NIOC) or FLTCYBERCOM to request COMSEC services for social networking. NIOC Norfolk currently supports web assessments for the fleet, but with the increase in social networking utilization their manpower would need to reflect the demand of the fleet. Along with web assessments, an OPSEC Red Team assessment should be required annually by all commands. NIOC OPSEC Teams need to expand their scope of responsibility to cover shore and include afloat commands. The bottom line is the Commander must have formal and consistent feedback to ensure his command and internet-based sites are properly secured.

CONCLUSION

The 21st Century Information Age has provided high end technology that has allowed to the United States military to access and share information in very sophisticated ways. The arrival of social networking has made its way into daily routines and everyday life of each sailor, airmen, soldier, and marine. The Department of Defense has made a decision to embrace this technology and use it to our advantage. By applying Operations Security smartly to our social media policy the Commander can successfully leverage this new capability to influence, engage, and inform the public as with our adversaries. With clear guidance, education, and training the worry of inadvertently releasing information through our social networking sites and providing vulnerabilities within our networks can be quickly mitigated.

NOTES

[1] William H. McMichael, "Pentagon Lifts Ban on Social Networking Web Sites," Federal Times, (08 March 2006), 7, http://www.proquest.com/ (accessed 23 March 2010).
[2] Facebakers, Facebook Statistics United States, http://www.facebakers.com/countries-with-facebook/US/ (accessed 09 April 2010).
[3] Defense Manpower Data Center, "Active Duty Demographic Profile," PowerPoint, September 2009, http://www.deomi.org/EOEEOResources/DemographicReports.cfm (accessed April 2010)
[4] Hugh Hewitt, "Rise of the MillBlogs," Weekly Standard, 28 April 2010, http://www.weeklystandard.com/Content/Public/Articles/000/000/003/840fvgmo.asp (accessed April 2010)
[5] Lon S. Cohen, " Is There A Difference Between Social Media And Social Networking?" *Blog*, entry posted 30 April 2009, http://lonscohen.com/blog/2009/04/difference-between-social-media-and-social-networking/ (accessed March 2010).
[6] *Dictionary.com*, http://dictionary.reference.com/browse/social, (accessed March 2010).
[7] Ibid.
[8] Ibid.
[9] Lon S. Cohen, " Is There A Difference Between Social Media And Social Networking?" *Blog*, entry posted 30 April 2009, http://lonscohen.com/blog/2009/04/difference-between-social-media-and-social-networking/ (accessed March 2010).
[10] *National Operations Security Program*, *National Security Decision Directive/NSDD-298*, 12 January 1988.
[11] Chairman, U.S. Joint Chiefs of Staff, *Operations Security*, Joint Publication (JP) 3-13.3 (Washington, DC: CJCS, 26 June 2006), II-2.
[12] OPSEC Division, "Operations Security Course," Powerpoint, July 2009, San Diego, Ca: Navy Information Operations Command San Diego, Training Department.
[13] National Security Agency/Central Security Service, *Purple Dragon: The Origin and Development of the United States OPSEC Program* (NSA Center for Cryptologic History, 1993), 4-5. Document is now declassified.
[14] *National Operations Security Program*, *National Security Decision Directive/NSDD-298*, 12 January 1988.
[15] William Lynn, Deputy Secretary of Defense, memorandum for distribution, DTM 09-026, "Responsible and Effective Use of Internet Based Capabilities," 25 February 2010.
[16] U.S. Navy, *Operations Security*, Navy Tactics Techniques and Procedures (NTTP) 3-54M, (Washington, DC: Department of the Navy, CNO, March 2009), 6-1.
[17] Secretary of Defense to All DoD Activity, message 090426Z AUG 06, 09 August 2006.
[18] Ibid.
[19] Air Force Public Affairs Agency, "New Media and The Air Force Version 2," November 2009, p6.
[20] William Lynn, Deputy Secretary of Defense, memorandum for distribution, DTM 09-026, "Responsible and Effective Use of Internet Based Capabilities," 25 February 2010.
[21] William H. McMichael, "Pentagon Lifts Ban on Social Networking Web Sites," Federal Times, (08 March 2006), 7, http://www.proquest.com/ (accessed 23 March 2010).
[22] Associated Press, "Marines Ban Social Networking, Citing Potential Security Risk," Foxnews, 4 August 2009, http://www.foxnews.com/story/0,2933,536647,00.html (accessed April 2010).
[23] Lt Col David A. Umphress, PhD, USAFR, "The Impact of the Internet on Collecting Open-Source Intelligence," Air & Space Power Journal, 1December 2005, http://www.airpower.au.af.mil/airchronicles/apj/apj05/win05/umphress.html (accessed April 2010).
[24] Phil Stewart, "Military allows Twitter, other social media," Reuters, 26 Feb 2010, http://www.reuters.com/article/idUSTRE61Q07G20100227 (accessed April 2010)
[25] Peter R. Orszag, Director OMB, to Heads of Executive Departments and Agencies, 08 December 2009.
[26] Federal CIO Council, "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," September 2009.
[27] Ibid.
[28] Ibid.
[29] JANSON Communications, "Military Facebook Study," March 2010, 15
[30] Chief of Naval Operations, " Communications Security Monitoring of Navy Security Telecommunications and Information Technology Systems," OPNAVINST 2201.3B, (Washington, DC: Department of the Navy, CNO, 14 Apr 09)

[31] San Diego Associated Press, "Camp Pendleton Marine Back on Facebook After Fueling Debate," CBS8.COM, 15 April 2010, http://www.cbs8.com/Global/story.asp?S=12318961 (accessed April 2010)
[32] Chief of Naval Operations, " Communications Security Monitoring of Navy Security Telecommunications and Information Technology Systems," OPNAVINST 2201.3B, (Washington, DC: Department of the Navy, CNO, 14 Apr 09).
[33] Yaakov Katz, "Facebook details cancel IDF Raid," The Jerusalem Post, 03 April 2010, http://www.jpost.com/Israel/Article.aspx?id=170156 (accessed April 2010)
[34] Fox News, "Gates Defends Soldiers in Iraq Shooting Video, Says Footage Lacks Context," Foxnews.com, 11 April 2010, http://www.foxnews.com/politics/2010/04/11/gates-defends-soldiers-iraq-shooting-video-says-footage-lacks-context/ (accessed April 2010)
[35] Ibid .
[36] Dan Raywood, "Facebook App Changes Could Lead to Security Issues," Secure Computing Magazine, 25 Jan 2010, http://www.securecomputing.net.au/News/165499,facebook-app-changes-could-lead-to-security-issues.aspx (accessed April 2010)
[37] Facebakers, Facebook Statistics United States, http://www.facebakers.com/countries-with-facebook/US/ (accessed 09 April 2010).
[38] David Carr, "Adversary Exploitation of Social Media," CIOZone.com, http://www.ciozone.com/index.php/Default-Category/Adversary-Exploitation-of-Social-Media.html (accessed April 2010)
[39] Ibid.
[40] Sue Marquette Poremba, "Five Social Media Security Issues," Network Security Edge, 07 April 2010, http://www.networksecurityedge.com/content/five-social-media-security-issues (accessed April 2010)
[41] Ibid.
[42] Ibid.
[43] Admiral Gary Roughead, Chief of Naval Operations, "CNO Releases Podcast on Summer Safety Campaign Wrap-Up, Social Media," Navy.mil, http://www.navy.mil/search/display.asp?story_id=48564 (accessed April 2010)
[44] DHS Privacy Office, "Government 2.0 Privacy and Best Practices: Report on the DHS Privacy Office Public Workshop," November 2009.
[45] Chief of Naval Operations, "CNO Guidance 2010: Executing the Maritime Strategy," Sep 2009, p14.
[46] Operations Unified Response JTF-Haiti official Facebook Web site, http://www.facebook.com/JTFHaiti (accessed April 2010)
[47] JANSON Communications, "Military Facebook Study," March 2010, 15
[48] Ibid.
[49] Air Force Public Affairs Agency, "New Media And The Air Force Version 2," November 2009, p33.

BIBLIOGRAPHY

Associated Press. "Marines Ban Social Networking, Citing Potential Security Risk." *Foxnews*, 4 August 2009. http://www.foxnews.com/story/0,2933,536647,00.html (accessed April 2010).

Carr, David. "Adversary Exploitation of Social Media." *CIOZone.com*. http://www.ciozone.com/index.php/Default-Category/Adversary-Exploitation-of-Social-Media.html (accessed April 2010).

Cohen, Lon S. " Is There A Difference Between Social Media And Social Networking?." Blog entry posted 30 April 2009. http://lonscohen.com/blog/2009/04/difference-between-social-media-and-social-networking/ (accessed March 2010).

David, Lt Col A. Umphress PhD, USAFR. "The Impact of the Internet on Collecting Open-Source Intelligence." *Air & Space Power Journal*, 1December 2005. http://www.airpower.au.af.mil/airchronicles/apj/apj05/win05/umphress.html (accessed April 2010).

Defense Manpower Data Center. "Active Duty Demographic Profile." PowerPoint, September 2009.

Dictionary.com. http://dictionary.reference.com/browse/social (accessed March 2010).

Facebakers. Facebook Statistics United States. http://www.facebakers.com/countries-with-facebook/US/ (accessed 09 April 2010).

Federal CIO Council. "*Guidelines for Secure Use of Social Media by Federal Departments and Agencies*." September 2009.

Fox News. "Gates Defends Soldiers in Iraq Shooting Video, Says Footage Lacks Context." *Foxnews.com*, 11 April 2010. http://www.foxnews.com/politics/2010/04/11/gates-defends-soldiers-iraq-shooting-video-says-footage-lacks-context/ (accessed April 2010).

Hewitt, Hugh. "Rise of the MillBlogs." *Weekly Standard*, 28 April 2010. http://www.weeklystandard.com/Content/Public/Articles/000/000/003/840fvgmo.asp, (accessed April 2010).

JANSON Communications. "*Military Facebook Study*." March 2010.

Katz, Yaakov. "Facebook details cancel IDF Raid." *The Jerusalem Post*, 03 April 2010. http://www.jpost.com/Israel/Article.aspx?id=170156 (accessed April 2010).

Kinniburgh, James and Denning, Dorothy. *Blogs and Military Information Strategy.* JSOU Report 06-5. Hurlburt Field, Florida: The JSOU Press, 2006.

McMichael, William H. "Pentagon Lifts Ban on Social Networking Web Sites." *Federal Times*, 08 March 2006. http://www.proquest.com/ (accessed 23 March 2010).

National Operations Security Program. National Security Decision Directive/NSDD-298, 12 January 1988. http://www.fas.org/irp/offdocs/nsdd298.htm (accessed April 2010).

Navy Information Operations Command San Diego. "Operations Security Course." PowerPoint. July 2009.

Orszag, Peter R. Director Office of Management and Budget, Executive Office of the President. To Heads of Executive Departments and Agencies. Memorandum, 08 December 2009.

Poremba, Sue Marquette. "Five Social Media Security Issues." *Network Security Edge*, 07 April 2010. http://www.networksecurityedge.com/content/five-social-media-security-issues (accessed April 2010).

Raywood, Dan. "Facebook App Changes Could Lead to Security Issues." *Secure Computing Magazine*, 25 Jan 2010. http://www.securecomputing.net.au/News/165499,facebook-app-changes-could-lead-to-security-issues.aspx (accessed April 2010).

Roughead, ADM Gary, Chief of Naval Operations. CNO Releases Podcast on Summer Safety Campaign Wrap-Up, Social Media.25 September 2009. Podcast. Official Website of the United States Navy.

San Diego Associated Press. "Camp Pendleton Marine Back on Facebook After Fueling Debate." *CBS8.COM*, 15 April 2010. http://www.cbs8.com/Global/story.asp?S=12318961 (accessed April 2010).

Stewart, Phil. "Military allows Twitter, other social media." *Reuters*, 26 Feb 2010. http://www.reuters.com/article/idUSTRE61Q07G20100227 (accessed April 2010).

U.S. Air Force. *Air Force Doctrine: New Media and the Air Force Version 2.*Air Force Public Affairs Agency, November 2009.

U.S. Department of Defense. *Responsible and Effective Use of Internet-based Capabilities*. Directive-Type Memorandum (DTM) 09-026. Washington, DC: DoD, 25 February 2010.

—. *DoD Operations Security (OPSEC) Program Manual*. Department of Defense Manual (DODM) 5205.02-M. Washington, DC: DoD, 3 November 2008.

U.S. Department of Homeland Security Privacy Office. *Government 2.0 Privacy and Best Practices: Report on the DHS Privacy Office Public Workshop*. Washington, DC: Nov 2009.

U.S. National Security Agency/Central Security Service. *Purple Dragon: The Origin and Development of the United States OPSEC Program.* NSA Center for Cryptologic History, 1993. Document is now declassified.

U.S. Navy. Office of the Chief of Naval Operations. "CNO Guidance 2010: Executing the Maritime Strategy." Washington, DC: Department of the Navy, CNO, Sep 2009.

—. *Operations Security*. Navy Tactics Techniques and Procedures (NTTP) 3-54M. Washington, DC: Department of the Navy, CNO, March 09.

—. " Communications Security Monitoring of Navy Security Telecommunications and Information Technology Systems." OPNAVINST 2201.3B. Washington, DC: Department of the Navy, CNO, 14 Apr 09.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Operations Security.* Final coordination. Joint Publication (JP) 3-13.3. Washington, DC: CJCS, 26 June 2006.

U.S. Secretary of Defense. To All Department of Defense, Activity, Message. 090426Z AUG 06. 09 August 2006.