USAWC STRATEGY RESEARCH PROJECT

OPSEC IN THE INFORMATION AGE

by

Lieutenant Colonel Robert G. Michnowicz
United States Army Reserve

Colonel Steven M. Lemons
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
OPSEC in the Information Age	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Robert Michnowicz	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**22**	

ABSTRACT

AUTHOR: Lieutenant Colonel Robert G. Michnowicz

TITLE: OPSEC in the Information Age

FORMAT: Strategy Research Project

DATE: 8 March 2006 WORD COUNT: 5789 PAGES: 19

KEY TERMS: Information Operations, Operations Security, Terrorism

CLASSIFICATION: Unclassified

Current Operations Security (OPSEC) policy and regulations appear outdated and in need of revision to successfully deny US adversaries the ability to gain information. Many of the issues that concerned the Army leadership in the American Revolution, both World Wars and Vietnam continues to remain problematic. Entering into late 2005, computer technology and communication advances require a renewed effort by the United States government to curtail vulnerability in the critical areas of unclassified open source communication networks. The internal effort to deny adversaries any advantage could have implications regarding methods of communication with families, freedom of information and media relations as the United States maintains troops overseas and continues the Global War on Terror.

As a starting point to understanding the importance of safeguarding information, a review of the background and history of security problems throughout the Army's history begins the study. This is followed by an examination of governmental and Army staff efforts to increase security awareness within the Departments of Defense and Army through policy, direction and command emphasis. Finally, the study looks at increased training, new organizations and Public Affairs issues that all influence how the United States Army addresses Operations Security in the Information Age.

OPSEC IN THE INFORMATION AGE

Current Operations Security (OPSEC) policy and regulations appear outdated and in need of revision in order to successfully deny US adversaries the ability to gain information. Many of the same issues that concerned the Army leadership in the American Revolution, both World Wars and Vietnam continues to remain problems that affect wartime operations. As the nation enters into late 2005, computer technology and communication advances require a renewed internal effort by the United States government to curtail vulnerability in the critical areas of unclassified open source communication networks. The internal effort to deny adversaries any advantage could have implications regarding all methods of communication with families, freedom of information and media relations as the United States maintains troops overseas and continues the Global War on Terror.

As a starting point to understanding the importance of safeguarding information, a review of the background and history of security problems throughout the Army's history begins the study. This is followed by an examination of governmental and Army staff efforts to increase security awareness within the Departments of Defense and Army through policy, direction and command emphasis. Finally a look at how increased training, newly created organizations and Public Affairs issues all influence how the United States Army addresses Operations Security in the beginning of the Information Age will be addressed.

The United States Army has long maintained a connection with the problems of Operational Security and will continue to do so in the future. As a matter of clarity highlighting the notion that words matter, the meaning of Operations Security (OPSEC) begins with a definition.

> OPSEC is defined as 1. A systematic process by which a government, organization, or individual can identify, control and protect generally unclassified information about an operation/activity and, thus deny or mitigate an adversary's/competitor's ability to compromise or interrupt said operational activity. 2. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to (a) identify those actions that can be observed by adversary intelligence systems, (b) determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries,…[1]

OPSEC History and Background

Always an operational issue, the effort to safeguard friendly information from adversaries has been a problem throughout the United States Army's history. Summed up best by General

George Washington, “Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion.”[2] General Washington was not speaking of communication nodes or computer networks, but his message is clear and still valid today. As a known OPSEC practitioner, he knew that a thinking adversary could connect the bits of information gained from observation and listening skills and derive intelligence from information. The attempt to prevent any information leaks that transform into something that when viewed as a whole could affect the army’s future operations or intentions remained foremost in his mind. General Washington’s abilities to keep information secure helped set the stage to extract his army and keep its fighting power intact while being pursued by the British Army during the American Revolution. His abilities to slip away and continue to gain information on British and Hessian forces facilitated his victories at Trenton and Princeton, while keeping the enemy guessing of his intentions.

During the First World War, Operations Security was governed by a series of notes and directives issued by the American Expeditionary Force (AEF) Chief press officer, American Military Attaché in London, Secretary of State or the (AEF) Chief of Intelligence.[3] Covering the period from 25 June 1917 through 18 November 1918, the policies were amended on thirteen occasions. The significant additions that most resemble today’s guidelines were issued on April 2nd, 1918. In the memo from the Chief of G-2(D), a list of topics covered the primary security and censorship issues of the time. Guidelines were issued on identification of troops by state, unit number or component, place locations, ship movements, army plans (real or possible), effects of enemy fire, casualties including individual dead or wounded names.[4] “In brief whatever will be printed which tends to injure the position of the United States in the congress of nations or the position of American soldiers in Europe.”[5]

Regarding the position of soldiers in Europe, the consequences of poor OPSEC and the direct result can be gleaned from an event that took place on November 10th, 1918. During an operation for the 356th Infantry, two of its’ organic battalions, 1st and 3rd, were able to use proper security measures and surprise to effectively cross a river at night with minimal casualties. The regiment’s actions to safeguard the plan included issuance of orders to few officers and muffling of oars and boards on the boats. Both practices highlighted security concerns and secrecy. However, the 2nd battalion arrived at its designated crossing point at 2100 and was unable to cross until 0100 a.m. While waiting, the battalion was detected and received German artillery fire upon its positions. The resulting effects killed or wounded 232 of 600 soldiers including the battalion commander and most of his officers.[6] Although the example is tactical in nature, one must conclude that two battalions succeeded in their security practices while one was

compromised. Proper OPSEC procedures had a profound effect on the 356th Infantry's mission accomplishment. The mission was accomplished and the objective taken, but the resulting casualties in one unit were deemed very high by most standards, 38%.

Security measures also encompassed more than the battlefield actions within the unit. In particular, comments on casualties and effects of enemy fire transcend time in that they are still problems today. In 1918, the issue or publication of names killed or wounded prior to family notification was illustrated clearly as a concern. The thirst for public information and operational security measures required significant coordination between the Intelligence officer, Press officer and the Department of State representatives. As the United States entered the Second World War, similar issues remained relevant and guidance expanded into actions taken by soldiers in the event of capture.

During the Second World War, security reminders produced through the Office of War Information used posters and catch phrases to illustrate security concerns. "Loose lips might sink ships" and "Somebody talked", the heart rendering poster showing a sad puppy, Gold Star banner indicating a serviceman killed in action and naval tunic over the back of a living room chair became synonymous with the public security effort. All designed to ensure the military and general populations were aware of the potential enemy collection effort that affected successful pursuit of the United States war effort. An additional poster, maintained "The enemy is listening: He wants to know what you know, Keep it to yourself."[7] Focused primarily on spoken words, conversations and written mail, the awareness program was designed to prevent an adversary from obtaining any information that could provide advantage. Additionally, the government issued rules of conduct to soldiers departing for overseas duty.[8] Within the rules were instructions on writing home, talk and capture. The rules highlighted ten prohibited subjects. They include discussion of casualties, effects of enemy operations, plans or forecasts for future operations and movements of troops, aircraft or ships.[9] The soldiers had to be constantly reminded to beware of enemy efforts designed to piece together information into something that would impact on operations.

A significant OPSEC breach in the Second World War was the compromise of the radar direction system "Eureka."[10] This system, used for special operations insertions by the Office of Strategic Services (OSS) to pinpoint drop zones for equipment and personnel, appears to have been compromised as early as 1942, without the Allies knowledge. Using captured German documents, it appears that not only did the Germans ascertain the purpose of the devices, but they employed captured equipment in deception and decoy operations. The Allies use of limited frequencies and limited use of security devices such as a Morse code key greatly facilitated

German efforts to gain complete information. As the war continued into 1943-44, the "Eureka" compromise resulted in misdirected air drops of equipment, and capture or elimination of OSS teams attempting to link with resistance fighters. After capture by the German forces, it became apparent to surviving team members that German Intelligence possessed significant knowledge of the key locations and instructors within OSS bases in England and Italy. The Germans were also exceptionally informed about OSS operational procedures. One captured radio operator from OSS team Tacoma was quoted "they knew more than I did about the outfit."[11] The losses in equipment and personnel became significant throughout the war and the Germans exploited the captured radio equipment and proceeded to capture a growing number of Allied special operations personnel.[12] The enemy successfully gained information and used it to their advantage. It was painstakingly clear that the lack of security consciousness impacted the operational efforts of the Allied war effort. Increased focus on OPSEC policy or training could have helped some of the effort to derail the German intelligence effort.

It wasn't until the late 1960's in Southeast Asia, that the OPSEC methodology known today had its origins.[13] Faced with the enemy gaining advanced knowledge of operations, a team was established to ascertain how the enemy gained information. As an additional focus the team was also tasked to find out how to combat the problem. The team found out that although on a small scale security and intelligence counter measures existed, they were insufficient to counter the enemy's efforts to gain information.[14] Once the team analyzed current practices and security methods the concepts of a large scale Operations Security program were initiated. The team then made recommendations to commanders who implemented the counter security policies. The acronym OPSEC became synonymous with a concerted national effort that affected government agencies, the military, research and development and industry. Although timely and important, it wasn't until 1988, twenty years later, that the formal National Operations Security Program was established with specific guidelines and requirements assigned to federal agencies.[15]

National Security Directive 298 and Department of Defense OPSEC Policy

The requirements established through National Security Decision Directive (NSDD) 298 initiated several steps to making the OPSEC directive the definitive executive guidance to all agencies within the federal government. The directive outlined the objectives, process, application, and policy. More importantly, it also established the proactive measure to establish a lead agency for interagency training. The National Security Agency (NSA) received a tasking to establish the Interagency OPSEC Support Staff (IOSS). The director of the NSA became the

Executive Agent for interagency OPSEC training and the establishment of the IOSS.[16] Additionally, each Executive department and agency assigned or supporting national security missions with classified or sensitive activities was directed to establish a formal OPSEC program.[17] Significantly, NSDD 298 identified and formalized the five step OPSEC process. These steps include; identification of critical information to be protected, analysis of the threat, analysis of vulnerabilities, assessment of the risks, and application of counter measures. As a policy, the NSDD 298 was primarily designed to address shortfalls in security measures for information available to the general public through open sources.[18] The NSDD clearly established the beginnings of policies and processes that govern OPSEC guidelines used today.

Current Operations Security (OPSEC) policy and regulations date from the 1980's and 90's and include as a base document NSDD 298. Used in conjunction with NSDD 298, the 1999 Department of Defense Directive 5205.2 was reissued to update existing policies and re-emphasize the importance of the Department of Defense (DoD) OPSEC program. Significant additions to the requirements of NSDD 298 included a listing of responsibilities under the supervision of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and the Chairman of the Joint Chiefs of Staff.[19] The additions reflect additional levels of supervision including mention of combatant commanders responsibilities not illustrated previously. 5205.2 did continue to refer to the five step OPSEC process as the analytical, risk based process that incorporates five distinct elements. No change to the five sub elements was indicated.[20]

Despite the additions, continuance of the OPSEC process and the reissue of the DoD directive, in 2003, the Al Qaeda training manual claimed that as much as 80% of their required information about US forces could be obtained from open source material.[21] Focused upon computer networks primarily, the translation of the Al Qaeda training manual with the statement about open source information gathering successes indicated a continued problem with the information security system as it exists today. Upon discovery of the problem, the Secretary of Defense issued a directive. Dated in January of 2003, Secretary Rumsfeld issued a message entitled: Web Site OPSEC Discrepancies. Within his DoD wide message was the statement on the susceptibility of the government informational network. "At more than 700 gigabytes, the DoD web-based data makes a vast, readily available source of information on DoD plans, programs, and activities. One must conclude our enemies access DoD web sites on a regular basis."[22] One of the five OPSEC steps is determination of vulnerability. The United States governmental networks systems are vulnerable using open source data. Secretary Rumsfeld

issued guidance and reminders to departmental heads of their responsibilities to manage information within their respective components. In his DoD memo, the Secretary directed that component heads apply the OPSEC review process and use that process to clear information for public dissemination, limit details, and ensure appropriate personnel received training in security measures. He also maintained that website owners are responsible for content and verification of need.[23] According to Army Regulation AR 530-1, the OPSEC review process "is an evaluation of a document to ensure protection of sensitive or critical information. The document may be a memorandum, letter, message, briefing, contract, news release, technical document, proposal, plan, order, response to Freedom of Information Act or Privacy Act requests or other visual or electronic media."[24] A Commander's direction or request may initiate the review process but Standard Operating Procedures will state which documents automatically go for review. The Army's answer to OPSEC is to make it a Commander's responsibility to plan and implement policy to preserve secrecy in all phases of operations, exercises, tests or activities.[25]

Army Staff Memorandums on OPSEC

Based on Secretary Rumsfelds directive the United States Army hierarchy sought to address its OPSEC issues through command emphasis and direct action designed to underscore the importance of the issue. Throughout 2003, the Army staff sought to give guidance and implement techniques to address OPSEC and website deficiencies identified during spot checks of Army websites. In a February 2003 message, Commanders at all levels were directed to review web pages, ensure OPSEC compliance and take steps to reduce vulnerabilities.[26] Included within the guidance were instructions to the commanders on benefits of conducting the unit website review process and first and foremost, a reminder to limit detailed information posted on unit sites.[27] Commanders were further advised to utilize the published Army OPSEC checklist to review content on public accessible websites.[28]

In the June 2003 OPSEC directive from Department of the Army, unit commanders were instructed to conduct a mandatory Army wide OPSEC Review. Three main directives applied to all levels of Army organizations and leadership. Commanders and Directors were tasked to review OPSEC programs, ensure trained personnel were assigned as OPSEC officers and integrate OPSEC into training events.[29] Additionally, unit commanders were directed to forward an assessment of their unit's OPSEC status to the Department of the Army. Instructions were also provided to assist the OPSEC effort by accessing the Army Knowledge Online website folder for pertinent guidance and policy. Through this directive, specific command emphasis

was provided to all levels of Army leadership on the protection of information and application of procedures to combat adversary collection efforts.[30]

In December 2003, the Chief of Staff of the Army, General Schoomaker, issued his initial Memo on the importance of OPSEC awareness. Within his message, he highlighted many of the facility, troop movement, and weapon effect issues that had confronted the AEF in the First World War and the Office of War Information during the Second World War. General Schoomaker further stated "that the Protection of friendly information is vital to success in accomplishing the Army's mission." Additionally, he emphasized the importance of caution regarding photographs of units and equipment.[31] In the two years between the 2003 Secretary of Defense and Army Chief of Staff Memos and 2005, problems remained with Operational Security measures. Soldiers continued to post information on units or casualties, battlefield effects and unit locations. Pictures of vehicle vulnerabilities with annotations were available on the internet.[32] All these violations continued, despite the Army staff efforts to mandate commander's participation and increase visibility of counter OPSEC tools using the internet and DA message dissemination process.

In February 2005, the Vice Chief of the United States Army issued a Department of the Army message regarding distribution of sensitive photos found on unclassified information computer networks. The Vice Chief's message highlighted our adversary's intent to use the American reliance on computer network based information against us. In the first paragraph, "The enemy is actively searching the unclassified networks for information, especially sensitive photos, in order to obtain targeting data, weapons system vulnerabilities, and Tactics, Techniques and Procedures (TTP's) for use against the coalition. A more aggressive attitude toward protecting friendly information is vital to mission success. The enemy is a pro at exploiting our OPSEC vulnerabilities."[33] The Vice Chief's memo served to remind all that the enemy is highly adaptable and able to use computer networks to their advantage, whether to publish their own information or glean information from the coalition as required. In essence, our own carelessness about OPSEC issues is helping the enemy. As a result, Army leaders were once again encouraged to discuss OPSEC with their troops and emphasize the critical importance of maintaining security in official and non official correspondence using all forms of media.

In August 2005, six months after the Vice Chief's message, the Chief of Staff of the Army issued additional Operations Security guidance in a follow up Department of the Army message. His strongly worded note highlighted that OPSEC is a chain of command responsibility and that we must do a better job across the Army. Emphasizing leader involvement, the Chief

highlighted that the OPSEC problem is not a new issue, has been addressed previously, and must be dealt with in order to reduce risk and any degradation to our operations.[34] The significant difference between the Secretary of Defense's message and the Chief's memo is that while the DoD message gave guidance, the Chief's message provided clear assistance in the form of tools that all can access and utilize to address the problem. These tools included staff coordination with the OPSEC interagency training teams and the Army G-2, a mobile training team for those deployed, and a new OPSEC training module. The Army G-6 was tasked with analyzing and reporting on computer/network OPSEC violations on a quarterly basis. Army Regulation AR 530-1 was scheduled to receive changes and updates that include sections on internet postings and usage.[35] Through the Chief of Staff's message process, the Army leadership implemented the steps necessary to apply the five step OPSEC process and increase information, knowledge, and training to reduce opportunities for the enemy to take advantage of lapses in operations security.

In December 2005, the Sergeant Major of the Army sent out an OPSEC focused message posted on the Army Knowledge Online home page. Clearly, the OPSEC issue has received visibility at the highest levels of government and the military. The message is clear, unless the United States Army can manage its internal information properly, adversaries can effectively glean intent, capabilities, and vulnerabilities by using the same technology Americans use in open source networks. The "Information Age" brings with it increased capabilities in digital photography, telecommunications and the Internet with world wide access. The recent increase in message traffic from Department of the Army levels indicate that a renewed emphasis on knowledge, training and implementation of OPSEC programs as an internal start point is beginning. The Army leadership also directed the creation of several organizations designed to implement OPSEC training and assessments in conjunction with the Interagency OPSEC Support Staff already designated to assist multi-agency training by NSDD 298.

OPSEC Training using Interagency OPSEC Support Staff

The Capstone OPSEC training efforts began with the IOSS as the designated authority for all interagency training.[36] The information and training efforts begin at the macro level with the yearly National OPSEC conference. Given each year over the past several years since 2003, the National OPSEC conference highlights specific topics of general interest to the Interagency Community. A cursory look at the available course offerings include a variety of subjects that affect the defense, law enforcement, research/development and the industrial espionage communities. Examples of the wide ranging list of subjects given within the conference and

exhibition website indicate an Application of Advanced OPSEC Security, Al Qaeda training programs in the United States, Application of OPSEC to Criminal investigations and OPSEC in and out of uniform: Personal Security in the Digital era.[37] There are also portions of the seminars that focus on OPSEC planning. These include military operations, survey planning, security of computer networks and OPSEC within undercover operations.[38] Two courses that utilize National Security policy as the baseline framework encompass OPSEC fundamentals and OPSEC in the International Security Environment.[39] There is not any indication of near term shortages of training materials, instructors or workshops. There appears to a growing interdependent system of OPSEC bureaucracy covering all aspects of communications and information protection operating under the auspices of the IOSS. The difficult part in the long term is the coordination of the many interdependent entities tasked with providing OPSEC protection.

The IOSS also provides the overall coverage for OPSEC focused mobile training teams (MTT). A comprehensive listing of the mobile training team dates and topics available is also web based to facilitate access. Created in a user friendly manner, the (MTT) descriptions include course titles, dates, prerequisites, course length, and delivery mode. Focused on fundamentals, vulnerabilities and analysis, the MTT's can provide training using video conferencing and/or platform instruction.[40] The ten listed courses cover the basics of Operational Security management, process and analysis techniques.[41] They are meant to compliment Department of Defense and subordinate governmental agency efforts for managers and executives primarily. The IOSS mobile training team effort crosses agency boundaries while providing information and training to sub elements that in turn must train their own personnel in OPSEC procedures. Understanding that OPSEC training and education entails more than briefings on what soldiers are allowed to write home about, the Army's effort to compliment and augment the IOSS training efforts included formation of the OPSEC Support Element and Army Web Risk Assessment Cell. As an operational issue crossing into public affairs, intelligence and information operations, the Army G-3 remains the proponent and responsible executor for the Army staff on OPSEC issues.

Army OPSEC Organizations

One of the initiatives forwarded by the Army G-3 action plan on OPSEC was the establishment of the Army Operations Security Support Element (OSE), one of two new internal Army agencies focusing on OPSEC issues. Functioning under the command and control of the 1st Information Operations Command, the OSE has received the mandate to be the lead

organization in the Army's fight against OPSEC violations.[42] The OSE mission has six primary roles as defined within AR 530-1. The OSE was created and organized to function in an advisory capacity to the Army G-3. The OSE is the lead element regarding OPSEC issues with a key purpose in all areas of OPSEC doctrine, training, tactics, techniques and procedures. As the lead element for Army OPSEC, the OSE is also designed to represent its parent service in all joint, inter-service and DoD interactions. Lastly, the OSE has a role to provide mobile training teams for deploying forces, OPSEC training, and support to Headquarters, Department of the Army for all OPSEC matters including acting as the Red Team.[43]

The OSE training effort includes a web based program that provides a one stop shop for OPSEC requirements. Using links from the 1st Information Operations Command that provide direct access to the OPSEC web page, the OSE has provided users with policy, guidance and conference briefings. There are also links to the training course dates and locations available to coordinate training events. The importance of a central location for all pertinent information is significant. Not only focusing on traditional problems with OPSEC, the OSE also facilitates coverage of the newer mediums of computers, information operations, and network vulnerabilities as well. Within the links subdivision are sections that cover OPSEC for Direct and Senior Leaders, OPSEC officers and trainers, and OPSEC basic information. The additional sections provide links to the three main players affecting OPSEC policy and training. These include the regulations listed for Army OPSEC under AR 530-1, Public Affairs governed by AR 360-1 and Web Master's governed by AR 25-1.[44] Included within the OSE mandate are provisions to work and coordinate operations within DoD, Joint Staff, the Army Public Affairs and Information Operations communities. The G-3 mandate sought to provide the best portrayal of the Army's message to the public without compromising essential friendly information. Part of the OSE mandate is an assessment of OPSEC as it relates to the internet and World Wide Web. As evidenced during the vulnerability assessments, the website review resulted in 517 findings in approximately 50% of registered sites.[45] There is clearly a need to address computer OPSEC issues. Knowledge and mandatory reporting requirements do not seem to be enough. In a website review of Operation Iraqi Freedom efforts, it was found that patient files from MEDCOM, ammunition status from Joint Munitions Command, and procurement data from the Army Comptroller all were vulnerable to exploitation or movement into an open web site.[46] All told, some 1600 discrepancies were found over a year long period.[47] Using this number as an indicator of the scope of the problem, Army leadership also determined that more help for the OSE was in order. Focusing upon the gains in computer

technology and the subsequent reliance upon information networks, the Army also created an Army Web Risk Assessment Cell (AWRAC).

The AWRAC, the second of the two new organizations established by the Army staff, is a recent addition to the security effort. The organization is designed to review content and conduct assessments of all the Army's publicly viewed websites to ensure compliance with DoD and other Federal policies.[48] As the CSA's primary computer network monitor, the AWRAC reports to the Army G-6 in support of the CSA's guidance to analyze and report on computer/network OPSEC violations. The AWRAC also plays a proactive part in determining that inappropriate, sensitive and personal information is removed from publicly accessible web sites.

In addition to the creation of the OSE and AWRAC, the Army G-3 plan to address OPSEC issues has several added focus areas. Already encompassing the creation of the OSE, AWRAC and the revision of Army Regulation AR 530-1, the G-3 plan included initiatives that re-engineer Army web site access to the general public and implementation of a wartime OPSEC training program. The effort to implement a "wartime" training program included training to units before departure to Operation Iraqi Freedom and Operation Enduring Freedom, upon arrival in theater and to Family Support Groups.[49] The concentrated effort is web based, command emphasized and mandated by policy and regulation. All the pieces for a successful implementation of OPSEC procedures are in place. There has been a revision of AR 530-1 and policy addressing computer networks, all within the past several years. Despite the considerable effort put forward by the White House, DoD, IOSS and the Army there still remain issues with what constitutes free speech, censorship and what is considered sensitive information. There remains debate on how that information is best protected and how to ensure all personnel are aware of the threat. The military has made significant progress in taking an issue with roots dating back to the American Revolution and updating its' policy and guidelines accordingly.

In strictly OPSEC terms, the implications for the military indicate that a change in mindset is required. OPSEC training is evolving from that once a year mandatory class, into an integrated training piece of all training events. The security problems with communication and the written word are timeless, and these remain a concern for all levels of command. Examples abound from United States Army history. There is still a long way to go. The problems with rapid dissemination of photos and information on the internet are unique to the 21 st century when compared to the past. It is possible that the groundwork has been laid through policy, new oversight organizations, and direct guidance to commanders. These techniques may

address future problems, but the issue must remain an important aspect of any commander's focused efforts. It is also possible and probable that with the improvements in communications technology and dissemination, that this is only the tip of the iceberg. By its new context and usage within the information age, OPSEC now entails public affairs and information operations. The answer in times past was a censorship of sorts. Often self imposed, the censors applied clear guidance from the intelligence staffs in order to safeguard information leaking to the enemy. As the United States Army moves through the 21st century, censorship of the press and military is not only impractical but a public relations nightmare waiting to happen.

OPSEC and Public Affairs

The OPSEC connection with public affairs brings to light the central argument between the public's right to know and sensitive critical information.[50] One of the tools available to bridge the gap between the two ideas is the 1st Information Operations (IO) Command. Discussed previously as the proponent for the Army's efforts on OPSEC using web based technology and mobile training teams, the 1st IO has discussed the OPSEC, Public Affairs, Web Master, relationship as a triangle of three separate but connected activities. OPSEC's focus is the need to protect information, Public Affairs focus is the need to project information and the Web Master's focus is the connection of information.[51] All three are concerned with information flow and content, but in different aspects. Guidance given by the Chief of Public Affairs indicates that while review of disseminated information is required by public affairs channels, that review does not constitute approval by OPSEC authorities.[52] It is also required that Public Affairs personnel review all information slated to be accessible by the public. The policies and procedures for clearance are indicated within Public Affairs regulation AR 360-1. This effort to provide a public relations take on information dissemination, adds an additional layer of complexity to an already difficult coordination of effort.

The coordination of all three organizations is such a necessity that the Army G-3 will have to direct action to gain momentum in the OPSEC fight. The formation of the OSE as the lead agency represents one important step. If the OSE has true oversight and the authority commensurate with responsibilities over OPSEC issues, then the Army will have set the pieces in place to safeguard and facilitate the information flow. Keeping in mind the ever-increasing thirst for information required by various users, including the public and media, the scope of the problem remains extensive and enigmatic.

On a daily basis, there remains the campaign to safeguard information from the individual soldier level through all levels of the civilian work force. Through use of the unit leaders at each

level of command, the Army leadership has managed to elevate the problem from one of peripheral concern into the limelight. The significance of this cannot be overstated. OPSEC focus is not quite the Cold War Mission Essential Task List (METL) focus many troop leaders were familiar with from unit level activities in the not so distant past. It is nevertheless, just as important an issue and may be just as instrumental in saving soldiers lives. Given the tools provided through guidance, computer based training efforts and the effort to coordinate public affairs, information operations, and security, the Army must highlight the fight for OPSEC on a continual basis. It is that important and worthy of the strategic focus required by leaders at the highest levels of the government. Strategically, the OPSEC effort also represents the tie in to information operations and ultimately public affairs. All require more than passing degree of knowledge and application. This is the one area with so much wide ranging impact that it must be done right the first time. Public opinion, world opinion, family support groups, the print and television media are all participants in the OPSEC issue. Adversaries already glean 80% of their information requirements based upon our mistakes or indiscretions.

The OPSEC dilemma that has plagued the United States Army throughout its' history continues to manifest itself in daily events. United States public opinion and in turn world opinion are key influences on support for the current war. They are also prime conduits for security leaks. The need for public information must satisfy the thirst for knowledge while keeping secure any information about potentially classified operations or material. The key issue revolves around the effort to lower or eliminate the percentage of information the enemy can gather, evaluate and apply to further their goals. That remains the critical task for Army leadership. Success in that endeavor will have effect on mission success in the ongoing Global War on Terror. It may save lives and spare army families unintentional hardship. The Army leadership seems to understand the magnitude of the task. Through "official" messages and letters, the organization has seen a re-emphasized command influence and oversight effort. Policy and direction have been evaluated and re-issued with additional relevant information on computer usage added. New organizations like the 1 st IO Command, OSE and AWRAC have been created and received the mandate to address OPSEC issues army wide. One location has been created to facilitate a single computer centric focal point for training, policy and guidance using the Army Knowledge Online (AKO). Through the use of messages on AKO soldiers receive constant awareness of the OPSEC issues. In short, the Army appears to have synchronized its effort to combat OPSEC in the Information Age. Time will tell whether the implementation of that effort and focus on OPSEC issues is just a passing fancy or dedicated

change in the way the Army does business. Nevertheless, the priority for information security must remain high for our nation to continue the Global War on Terror to a successful conclusion.

Endnotes

[1] U.S. Interagency OPSEC Support Staff, *OPSEC Glossary of Terms* available from http://www.ioss.gov/docs/definitions.html; Internet, accessed 18 October 2005, 10.

[2] U.S. Department of Energy, *An Operational Security (OPSEC) Primer*, Washington D.C.: Department of Energy, available from http://www.defendamerica.mil/articles/a021202b.html; Internet; accessed 7 December 2005, 1.

[3] U.S. Department of the Army, *Reports of the Commander in Chief, Staff Sections and Services, AcofS-G-2, GHQ, AEF,* vol 13 (Washington D.C.: Center of Military History, 1991, First Published 1948, CMH Pub 23-19), 81-90.

[4] Ibid., 87.

[5] Ibid., 90.

[6] The Infantry Journal Incorporated, "Surprise," *Infantry in Battle,* 2nd ed. (Washington D.C., The Infantry Journal Incorporated, 1939; reprint, Washington D.C.: Center of Military History, 1997),110-112.

[7] U.S. Department of Energy, *An Operational Security (OPSEC) Primer*, 1.

[8] "Loose Lips Sink Ships," EyeWitness to History (1997) available from http://www.eyewitnesstohistory.com; Internet; accessed 11 December 2005, 1.

[9] Ibid., 1-2.

[10]Chris Burton, "The Eureka-Rebecca Compromises: Another Look at Special Operations Security During World War II," *Air Power History*. Washington: Winter 2005. Vol. 52, Iss. 4 [database on line]; available from ProQuest; accessed 14 January 2006, 2.

[11] Ibid., 8.

[12] Ibid., 11.

[13] U.S. Department of Energy, *An Operational Security (OPSEC) Primer*, 1.

[14] Ibid., 2.

[15] The White House, *National Operations Security Program* , National Security Decision Directive Number 298, (Washington D.C.: The White House, 22 January 1988), 2.

[16] Ibid., 3.

[17] Ibid., 2.

[18] Ibid., 1.

[19] U.S. Department of Defense, *DoD Operations Security (OPSEC) Program* Department of Defense Directive 5205.2, (Washington D.C.: U.S. Department of Defense, 29 November 1999), 3-4.

[20] Ibid., 9.

[21] U.S. Secretary of Defense Donald Rumsfeld, "Web Site OPSEC Discrepancies," Memorandum for All DoD Activities, Washington D.C., 14 January 03, available from http://www.ioss.gov/docs/rumsfeld_14jan03.html; Internet, accessed 18 October 05, 1.

[22] Ibid.

[23] Ibid., 2.

[24] U.S. Department of the Army, *Operations and Signal Security, Operations Security (OPSEC)* Army Regulation 530-1(Washington D.C.: U.S. Department of the Army, 27 September 2005), para. 4-1.

[25] Ibid., para 2-1.

[26] U.S. Department of the Army, DAMO-AOC-CAT, "Armywide Website OPSEC Review," Memorandum for All Army Activities, Washington D.C., 28 February 2003, para 2.

[27] Ibid., para 6.

[28] Ibid., para 6 (h).

[29] U.S Department of the Army, DAMO-AOC-CAT, "Army Operations Security (OPSEC) Directive," Memorandum for All Army Activities, Washington D.C., 23 June 2003, para 2.

[30] Ibid., para 6.

[31] U.S. Chief of Staff of the Army General Peter Schoomaker, "Reemphasis of Operations Security (OPSEC)," Memorandum for Principal Officials of Headquarters, Department of the Army, Washington D.C., 4 December 2003, para 1.

[32] U.S. Vice Chief of Staff of the Army General Richard Cody, "Sensitive Photos," Memorandum for All Army Leaders 05 (LTC) or Equivalent and Above, Washington D.C., 14 February 2005, para 1.

[33] Ibid.

[34] U.S. Chief of Staff of the Army General Peter Schoomaker, "Sensitive Photographs," Memorandum for All Army Leaders, Washington D.C., 23 August 2005, para 1.

[35] Ibid., para 3.

[36] The White House, *National Operations Security Program* , National Security Decision Directive Number 298, 3.

[37] U.S. Interagency OPSEC Support Staff, *National OPSEC Conference and Exhibition Abstracts* available from http://www.ioss.gov/conf/abstracts_conf.html; Internet, accessed 18 October 2005, 4-5.

[38] Ibid., 6.

[39] Ibid., 4.

[40] U.S. Interagency OPSEC Support Staff, *Training – Course Listing* available from http://www.ioss.gov/training/course_listing.html; Internet, accessed 18 October 2005.

[41] Ibid.

[42] U.S. Department of the Army, *Operations and Signal Security, Operations Security (OPSEC)* Army Regulation 530-1, para 2-20.

[43] Ibid.

[44] Army G-3, "Army OPSEC Action Plan, " briefing slides, Army G-3, Supported by 1st IO Command, 2004 OPSEC Conference, available from https://opsec.1iocmd.army.mil/io_portal /filemanager_CF/data/public/vad%20 page/OPSEC/Resources; Internet; accessed 18 December 05. Slide 7.

[45] Ibid., slide 17.

[46] Ibid.

[47] Herbert White, "Walking the Tightrope," briefing slides, 1st IO Command, March 2005 available from https://opsec.1iocmd.army.mil/io_portal /filemanager_CF/data/public/vad%20 page/OPSEC/Resources; Internet; accessed 18 December 05. slide 10.

[48] U.S. Department of the Army, *Operations and Signal Security, Operations Security (OPSEC)* Army Regulation 530-1, para 2-21.

[49] Army G-3, "Army OPSEC Action Plan, " slide 25.

[50] Herbert White, "Walking the Tightrope," slide 1.

[51] Ibid., slide 13.

[52] Ibid., slide 12.