

OPSEC is Everyone's Responsibility: CHANGING A MINDSET

SECOND LIEUTENANT JAMES A. CAPOBIANCO

"In the Global War on Terrorism, we face an insidious and adaptive adversary capable of gathering open source information on our operations and intentions. Do not provide him assistance through uncontrolled release of information that may compromise our own force protection. We are an Army at war and our Soldiers deserve the best operations security (OPSEC) we can provide."

— General Peter J. Schoomaker,
Chief of Staff of the Army

THE IMPORTANCE OF OPERATIONS SECURITY

According to a memorandum from the office of the Secretary of Defense, Soldiers in Afghanistan found an Al Qaeda training manual; this manual purports that by "using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy." The U.S. is an open nation; our founding principles of liberty and freedom compel such openness. In fact, the Department of Defense alone maintains more than 700 gigabytes of web-based data. Based upon captured documents, the realities of American society, and other intelligence indicators, we must assume that our enemies use our openness as a fertile bed for intelligence gathering. Specifically, it is a sure bet that adversaries are routinely accessing and monitoring Internet sites and other open-source media to gain an advantage against our superiorly equipped and trained forces.

The modern American concept of war has tended to neglect the existence and real threat of espionage conducted against the United States and its allies. Soldiers have adjusted well to increased operations tempo

and deployments. They are meeting unforeseen challenges with innovation and courage. Yet, some Soldiers are failing to recognize the potential damage they are causing by failing to protect critical information on past, present, and future operations.

Central in our struggle to accomplish our mission is our ability to establish and maintain OPSEC. Failure to enforce basic OPSEC rules and regulations results in the transmission of potentially damaging information into the hands of our adversaries. In order to enforce OPSEC, all Soldiers must learn what type of information needs to be protected and how to protect it.

WHAT IS OPSEC?

OPSEC is a continuous process that must occur during times of peace and war. Current OPSEC guidelines prohibit the posting, discussion, or description of tactics, techniques, and procedures (TTPs) that pertain to small unit operations and how Soldiers operate in the current environment. Additionally, information which contains lessons learned or system capabilities/vulnerabilities must not be placed in a public or non-secure environment. (See your local intelligence office for your unit's complete OPSEC regulations.)

Knowing what is and what is not critical information is the basis for establishing and maintaining good OPSEC. Specifically, Soldiers must know what information is considered critical information or essential elements of friendly information (EEFI). In general, critical information is considered to be "specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable

consequences for friendly mission accomplishment" (Joint Pub 1-02). EEFIs are associated with "key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness" (Joint Pub 1-02).

HOW TO PROTECT OPSEC

Equally imperative to successful OPSEC is being aware of how critical information and EEFIs are compromised. Virtually every means of communication can be compromised. However, the easiest and most prevalent means is through open sources. Open-source materials include, but are not limited to: webpages, news channels, newspapers, technical manuals, field manuals, and government white papers.

The most common ways our enemies obtain information are through monitoring and intercepting:

- ✓ Websites,
- ✓ Cell phones,
- ✓ Pagers,
- ✓ PDAs,
- ✓ Telephones, and
- ✓ Trash.

Information leaked through these sources is easily preventable. The easiest way to counter enemy attempts is to simply not transmit pertinent information via these mediums and to be cognizant of what type of information is placed in the trash and how that trash is ultimately disposed. Additionally, it is crucial that information controls be placed on government-sponsored webpages. Information posted and linked to these sites must be reviewed to ensure that no critical information or EEFIs are included. If such information is to be posted, it must — at a minimum — be accompanied by password protection.

Protecting OPSEC is everyone's responsibility. Every Soldier possesses some knowledge that is coveted by our enemies. Soldiers must be mindful of the content of their public discussions, phone conversations, and e-mail. In order to guarantee the protection of vital information, Soldiers must assume that someone else may either be listening to their conversations, or reading their written correspondence. While at work, Soldiers must use an approved means of secure communication whenever transmitting sensitive information.



else may have access to it. If you did not need to enter a password to gain access to a website, then neither does the enemy.

Also of growing concern are article submissions to open-source magazines and newspapers. *Infantry Magazine* routinely receives articles which contain a great deal of useful information on how to conduct patrols, avoid ambushes — in general, how to be successful on the modern battlefield. Unfortunately, some of this information is “too good” for publishing and can only appear on our secure, password-protected website. We certainly do not wish to discourage the

COMMON OPSEC VIOLATIONS

American Soldiers routinely discuss their deployment schedules with friends and family through unclassified mediums. Soldiers are returning from theater and posting their tactical experiences in chat forums, on message boards, and in other open-source media. The majority of these individuals are merely trying to share their hard-gained knowledge with their peers. These attempts are understandable and even encouraged; yet they must be conducted in appropriate settings. Without proper control measures, sensitive information flows directly to the enemy. The result of a well-intended, open-source dispersal of information is the potential disruption and dissolution of American military security and success.

For example, lessons learned regarding logistical planning and execution may provide a terrorist with enough knowledge to successfully infiltrate and sabotage a critical supply center or route used by coalition forces. Discussing how to conduct a patrol or raid will give the enemy a foundation from which he can build a formidable defense and countermeasures. Listing limitations and vulnerabilities of a piece of equipment is one of the most damaging OPSEC violations. While your intentions may be to suggest improvements and present a means of overcoming the limitation, in essence, you are telling the adversary what your equipment can and cannot do. If the enemy knows a piece of equipment works inconsistently in inclement weather or erratically in restrictive terrain, then he can plan accordingly and strip American forces of their technological superiority and turn it into a potential hindrance. This is of particularly grave concern when the equipment is a prototype or is undergoing research and development (R&D) for final fielding. Any information pertaining to R&D allows present and future enemies to monitor, anticipate, and exploit our technological advancements and initiatives.

With the increasing prominence of the Internet, many Soldiers are using it as a means to share information whose indiscriminate dissemination may ultimately prove detrimental to the safety and success of our troops. Before sharing information, think about who

submission of pertinent and timely articles, nor do we wish to ebb the exchange of experiences and ideas, but we do recommend you proofread your text for potential OPSEC violations. Historical reviews of tactics and missions are almost always acceptable in their entirety, but information pertaining to current operations must be closely assessed before it can be openly distributed.

Violations in OPSEC give our adversaries one piece of the puzzle at a time. Enemy information gathering is predicated upon patience and persistence. Over time, the enemy is able to gather enough information to make an informed decision on how we conduct our missions and as to what our future intentions are.

CONCLUSION

Operations security is a practice that must be adhered to at all times. It is a policy that is as equally imperative in peace as it is in war. Despite its importance, Soldiers have become lax in their adherence to proper OPSEC procedures. Information pertaining to deployment schedules, missions, tactics, and recent lessons learned is just some of the information being shared through numerous open source mediums. The indiscriminate sharing of information will damage ongoing and future military operations; it is only a matter of when and to what degree. Soldiers must learn what information needs to be protected and how to protect it.

The war on terror is being waged incessantly at home and abroad; given the will and tenacity of the American Soldier, it will result in victory. However, we must not provide our enemy with detailed information on how we operate — to do so compromises the security and safety of our troops. What may seem to be of no intelligence value to you may prove to be the coups de grace in the planning and implementation of a future terrorist attack. Remember, OPSEC is everyone's responsibility!

Second Lieutenant James A. Capobianco is a graduate of the Fort Benning Officer Candidate School. He has a master's degree in international studies. At the time this article was written, he was serving as a research assistant with *Infantry Magazine*.
