

***TERRORISTS and SPIES are on the web...
...don't be an easy TARGET!***



Protect Operational Information

BE VIGILANT. REPORT SUSPICIOUS ACTIVITY.

Image credits:

Front cover:

U.S. Army photo by Sgt. Brandon Little, Task Force XII PAO, MND-B

Inside back cover:

U.S Army photo by Staff Sgt. Mike Pryor, 2nd BCT, 82nd Abn. Div. Public Affairs

Operations Security (OPSEC)

Terrorists select targets that offer the most opportunity for success. Information passed unknowingly by military personnel, and increasingly via cyberspace, is being used by terrorists in their planning efforts. OPSEC denies terrorists information about potential targets and reduces the availability of this information.

OPSEC focus areas for Antiterrorism include:

- Deny intelligence and information to terrorists
- Avoid rigid operational routines that produce observable patterns
- Know terrorist collection methods and techniques as well as the terrorist planning cycle and cyber attack methods
- Integrate OPSEC into organizational security programs and individual personal protection measures

Sample Cyberspace OPSEC procedures:

- Coordinate physical security measures to prevent unauthorized access to computer networks, equipment, facilities, and documents
- Password protect or restrict computer access to itineraries, travel plans, personnel rosters, building and base plans, billeting assignments, and very important person (VIP) guest lists
- Don't post personal, work, or family information to open social media websites
- Be careful who you allow into your social network; if you do not know a person who attempts to connect with you, investigate who they are and why they want to join your social network.
- Don't post sensitive work information or photographs on the internet; always assume a threat adversary is reading your material

Advances in technology increase risk

Advancements in technology pose new threats to security of critical information. In order to counter an adversary from employing these technologies, we must first know the technologies that exist and how they might be used within close proximity of our critical information.

Defense measures include:

- Educate Army computer users on restrictions for use of information technologies
- Work closely with information systems administrators to establish control measures
- Ensure personnel responsible for entry/exit inspections are properly trained

Commander at all levels must:

- Apply the OPSEC review process outlined in AR 530-1 (Operations Security)
- Review their Web Pages and ensure they are OPSEC compliant
- Ensure all Army web sites are registered
- Limit details about the organization's specific capabilities, readiness, and operational matters
- Verify there is a valid mission need to disseminate the information



Critical information is information that is vital to a specified mission. If a terrorist or spy obtains critical information, correctly analyzes it, and acts upon it, the compromise of the information may prevent or seriously degrade mission success. Critical information can be classified or unclassified. Classified information requires OPSEC measures for additional protection because it can be revealed through unclassified indicators. The use of essential elements of friendly information (EEFI) protects critical information because it prevents the release of sensitive or classified details.

Example of EEFI for threat countermeasures

- When do security guards or law enforcement change shifts?
- Are guards armed?
- Is there a security response team alarm – how quick is the response?
- Where is the security alarm / power system – is it protected?
- Are external CCTV cameras operated and are they actually monitored?
- How many security guards are there in a specific building (day and night)?
- Does the building practice fire drills and where are the assembly areas (do they change the assembly areas or keep them the same for every evacuation)?
- Are mail/packages accepted at night? How are packages processed – must they go through a centralized screening location?

“Our adversaries derive up to 80% of their intelligence from open-source information.” CRS Report for Congress, Sensitive But Unclassified Information and Other Controls: Policy and Options for Scientific and Technical Information, December 29, 2006

How can OPSEC help protect my organization against terrorism?

Terrorists require intelligence to accomplish their objectives. You can apply the OPSEC process to identify critical information that terrorists can use against you and control those indicators that give away that critical information.

Terrorists seek—and OPSEC is intended to deny—information about:

- What is important to Army units, personnel, and families
- How accessible it is
- If we are able to replace the item of interest
- How vulnerable it is (security weaknesses)
- What it is vulnerable to (threat tactics)
- What outcome can be achieved if attacked
- How easy it is to find or locate

OPSEC in the Blogosphere

A Blog (short for Web Log) is a frequent, chronological publication of personal thoughts and web links, including a mix of what's happening in a person's life. Blogs may include forms of personal diaries or guides for others.

Military blogs, by their nature, attract the attention of a variety of threats to include terrorists and spies. Tidbits of information gathered from blogs and other open source information make up pieces of a puzzle, which when combined, can complete a picture of what may become a terrorist's or spy's target.

Examples include:

- Posting sensitive photographs on the internet, such as battle scenes, casualties, destroyed or damaged equipment, and especially the effects of threat weapon systems such as improvised explosive devices
- Some photographs include geo-location and date/time information.
- Enemies can use this information for propaganda purposes, battle damage assessments, targeting, and refinement of TTPs
- Enemies can also use personal information to target individual soldiers and their families for attack, both overseas and at home

Vulnerabilities on websites:

- Installation or facility maps designating points of interest (such as barracks, work areas, headquarters, dining facilities)
- Security force schedules and rotation plans
- Security operating procedures
- Tactics, techniques, and procedures
- Capabilities and intent
- Indicators of unit morale
- Information which may undermine leadership
- Photographs particularly when they are accompanied by descriptive captions
- Personal information about patterns and routines
- Work email addresses

What we can do to reduce risk on the internet:

- Ensure any information you post has no significant value to the enemy
- Consider the audience when you are posting personal information on a blog or website, or sending an email
- Always assume a threat adversary is reading your material
- If you are threatened as a result of something you have posted or through an open forum such as blog – believe the threat and report it immediately
- Avoid posting work email addresses if possible; they can provide targets for phishing attacks
- Follow OPSEC policies and procedures
- Work with your OPSEC officer

Privacy tips for social networking

Social networking sites like Facebook, Google+, Twitter, Foursquare, LinkedIn, and others are a great way to keep family & friends updated on your life and to connect with colleagues, business associates, and communities that share your interests. Make sure you are comfortable with the information you share and use privacy settings to protect your information.

Protect personal information

STOP! THINK! THEN CONNECT. Think carefully about the kinds of information, comments, photos, and videos you share online.

Do not post job related information about: Personnel movements (itineraries, rosters, time tables, travel plans); current or future operations (movement of forces, capabilities & limitations, coalition & participating forces); intelligence, reconnaissance & surveillance (TTPs, capabilities and limitations, operational reporting); or communication in support of operations (work email addresses, logins and passwords, details of specific equipment, infrastructure and call signs).

KNOW YOUR AUDIENCE: Consider who may have access to your profile: family, friends, friends of friends, your school, college admissions officers, potential employers. Use available privacy settings to manage your audience.

Your privacy is only as protected as your least reliable friend allows it to be. When you choose to share information with friends, those friends can make their own decisions about forwarding your content. Think carefully before sharing.

Safe home computing

Home computers are typically not well secured and therefore are often easy to break into. Intruders want what you've stored (i.e., credit card numbers, bank account information, passwords) and anything else they find useful. Intruders also want your computer's resources, meaning your hard disk space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet. The more computers an intruder uses, the harder it is for law enforcement to find the originating source. If intruders can't be located, they can't be stopped, and they can't be prosecuted.

What should I do to secure my home computer?

- Install and use anti-virus programs
- Keep your system patched
- Use care when reading email with attachments
- Install and use a firewall program
- Install, use, and enable strong security measures on a home wireless router
- Make backups of important files
- Use strong passwords and change them frequently
- Use care when downloading and installing programs
- Understand the risk of downloading files and programs
- Install and use a file encryption program and access controls



BE VIGILANT. REPORT SUSPICIOUS ACTIVITY.

Resources

National Cyber-Alert System:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-0076>

National Crime Prevention Association:

<http://www.ncpc.org/>

Army Information Assurance Portal:

https://www.milsuite.mil/login/Login?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fwiki%2FPortal%3AArmy_Information_Assurance

Homeland Security Cyber Security Tips:

<http://www.dhs.gov/cybersecurity>

National Cyber Awareness System:

<http://www.us-cert.gov/alerts-and-tips/>

DoD Chief Information Officer:

<http://dodcio.defense.gov/Home/Topics/InformationAssurance.aspx>



Always Ready, Always Alert
Because someone is depending on you

