Social Media and Operations Security

...weighing the balance between security and open communication
### Social Media and Operations Security: Weighing the Balance between Security and Open Communication

**Title and Subtitle:**
Social Media and Operations Security: Weighing the Balance between Security and Open Communication

**Performing Organization:**
Army Office of the Chief of Public Affairs, Online and Social Media Division, 1500 Pentagon, Washington, Dc, 20301

**Distribution/Availability Statement:**
Approved for public release; distribution unlimited

**Security Classification:**
- Report: Unclassified
- Abstract: Unclassified
- This Page: Unclassified
Overview

• What is OPSEC
• Balancing OPSEC with public affairs
• Operations Security and what it means to your organization (military or not)
• How social media and open communication can make our Army (and your organization) stronger
• Rules of Engagement
What is OPSEC?

- OPSEC = Operations Security
  - Protection of classified, sensitive, or need-to-know information
  - Proprietary information, insider information, trade secrets, etc.
- All organizations have their own form of Operations Security – information that must be protected
What is OPSEC?

What are they looking for:

– Names/photographs of important people
– Present and future US capabilities
– Meetings of top officials
– Information about military facilities as stated in AR 530-1
  • Location of formations & units
  • Weapons used
  • Fortifications and tunnels
  • Amount of lighting
  • Exterior size and shape of buildings
  • Number of soldiers/officers
  • Ammunition depot locations
– Leave policies
– Degree & speed of mobilization

*98% of the Intel Al Qaeda collects is “open source”*
Balancing OPSEC w/ Public Affairs

- The U.S. Army, and all government organizations, have communications concerns other organizations do not

- Release of inappropriate information can result in lost lives

- Examples:
  - Policies and ROE that govern the use of weapons and electronic or acoustic warfare systems
  - Overall bed/treatment capacity (bases, stations, etc.)
  - New weapons that are available or are being employed
  - Vulnerabilities of defensive dispositions
  - Vulnerabilities to attack
  - Vulnerabilities / capabilities of units, weapons systems
  - Doctrine for using various weapons
  - Shortages in medical specialties/personnel
  - Unit locations (grid coordinates, cities, etc.)
  - Date/time of flights
What it means to your organization

The objective of OPSEC is to make oneself or organization a “hard target”

- Make it more difficult for an adversary to indentify and exploit vulnerabilities
- Don’t post or publish personal or organizational critical information in public venues, including social media
OPSEC at home or on base

• Set profiles to “private” or “friends-only” to limit the threat of public information being used against you
  – Enemies can gather information about you or your family members
    • Rises in home robberies because people have been revealing when they go on leave or vacation
  – Enemies can gather information about bases and capabilities by reading your profile
    • Pictures of quarters, armored vehicles, weapons in your photo albums
    • Photos of formations
    • “Checking in” via FourSquare or Tweeting at morning formation
  – Be careful of using location-based services that make your location public
    • Example: Repeatedly revealing your location enables strangers to track your movements. And if you are linked with a spouse or child, they can be tracked, too.
    • Think about:
      – Posting geo-tagged photos on sites such as Facebook
      – Facebook Places
      – Yelp
      – FourSquare
      – Twitter
OPSEC in the field

What if you’re captured by enemy forces?

– Is your information publicly accessible?
  • Being “linked” to significant others/family/friends makes it easier for enemies to gather information about you
  • In detention or torture situations, what they find can be used against you
  • Can the enemy get photos of your spouse, child or pet off your page to use against you?

– Do you have ‘power of attorney’?
  • If you are captured, they have authority to access your accounts to prevent malicious access or
  • Prepare a list of your social media sites with usernames and passwords and leave it with them
  • If captured, does your spouse/friend have access to disable your online profiles?
OPSEC in the field

– Are your passwords safe and up-to-date?
– What if your account was hacked or you were tortured into providing password?
  • If enemies hack your accounts, they can potentially use it in a malicious or demoralizing manner
  • They could send messages that would appear to be from you to thwart rescue efforts or put others in harms way
Social media can make your organization stronger

*Social media is another tool to get your info out*
*Allows your audience dialogue with you and others*
Social media can make your organization stronger.
Educate vs. Regulate

• Mitigate the risk of using social media by educating the Soldiers and family members

• Think about what you post and what people can figure out about you

• It all goes back to OPSEC and UCMJ
Resources

- **Department of Defense**
  - [DoD Directive 8500.01E](#), “Information Assurance (IA),” October 24, 2002
  - [DoD Directive 5230.09](#), “Clearance of DoD Information for Public Release”
  - [DoD Directive-Type Memorandum 09-026](#), “Responsible and Effective Use of Internet-based Capabilities,” February 25, 2010
  - [DoD Social Media Hub](#) – contains safety guides and informational websites for practicing OPSEC

- **U.S. Army**
  - [Memo](#) – “Responsible Use of Internet-based Capabilities,” March 30, 2010
  - [AR 25-1](#), “Army Knowledge Management and Information Technology Management,” December 4, 2008
  - [AR 360-1](#), “The Army Public Affairs Program,” September 15, 2000
Rule of Thumb

If you aren’t comfortable placing the same information on a sign in your front yard, don’t put it online
Questions?

Contact Information:

ocpa.osmd@us.army.mil
(703) 614-0371