OPSEC in the Blogosphere
To emphasize the critical nature of protecting sensitive information from enemy exploitation and provide information for implementation of an Army OPSEC Training Program consistent with recent guidance issued by the CSA.
Agenda

• Threat

• OPSEC

• Blogs and the Internet

• Summary
“Capability of a potential enemy to limit or negate mission accomplishment or to neutralize or reduce the effectiveness of a current of projected organization or material item.” Two types of threat information are required:
  • Intelligence collection threat
  • Combat capability threat

AR 530-1
# Categories of Threat

## Traditional Categories

<table>
<thead>
<tr>
<th>EXTERNAL</th>
<th>DOMESTIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Governments</td>
<td>Hackers Militia Groups</td>
</tr>
<tr>
<td>Foreign Intelligence Services (FIS)</td>
<td></td>
</tr>
</tbody>
</table>

## Non-Traditional Categories

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Al Qaeda</td>
<td>Drug Cartel</td>
</tr>
<tr>
<td>Warlords</td>
<td>Media</td>
</tr>
</tbody>
</table>

- Combinations
- Combinations of all of the above
- Long Term
- Short Term
## Paramilitary, Insurgent, Radical, Terrorist Threats Active in OIF/OEF Theaters

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small arms fire (SAF)</td>
<td>279</td>
<td>23.3%</td>
</tr>
<tr>
<td>Improvised explosive device (IED) attack</td>
<td>219</td>
<td>18.3%</td>
</tr>
<tr>
<td>Hostile-ambush</td>
<td>62</td>
<td>5.2%</td>
</tr>
<tr>
<td>Hostile-vehicle borne (VBIED)</td>
<td>55</td>
<td>4.6%</td>
</tr>
<tr>
<td>Hostile-helicopter shot down/downed</td>
<td>53</td>
<td>4.4%</td>
</tr>
<tr>
<td>Hostile-mortar attack</td>
<td>53</td>
<td>4.4%</td>
</tr>
<tr>
<td>Hostile-rocket propelled grenade (RPG) attack</td>
<td>50</td>
<td>4.2%</td>
</tr>
<tr>
<td>Hostile-vehicle accident</td>
<td>25</td>
<td>2.1%</td>
</tr>
<tr>
<td>Hostile-helicopter crash (missile attack)</td>
<td>22</td>
<td>1.8%</td>
</tr>
<tr>
<td>Hostile-sniper fire</td>
<td>17</td>
<td>1.4%</td>
</tr>
<tr>
<td>Hostile-rocket attack</td>
<td>14</td>
<td>1.2%</td>
</tr>
</tbody>
</table>

(Coalition Force (CF) Invasion through 5 OCT 04, includes all CF Casualties killed in action)


Adaptive, cunning, and learning Adversary ... unlike most previous experiences
Vulnerabilities
OPSEC Defined

• A process of identifying Essential Elements of Friendly Information (EEFI) and subsequently analyzing friendly actions attendant to military operations and other activities to:

  • Identify those actions that can be observed by adversary intelligence systems
  • **Determine indicators** Adversary intelligence systems might obtain that could be interpreted or pieced together to derive EEFI in time **to be useful to adversaries**
  • Select and execute measures that eliminate or reduce to an **acceptable** level the vulnerabilities of friendly action to adversary exploitation
Critical Information

What they are looking for:

1. Names/photographs of important people
2. Present and future U.S. capabilities
3. Meetings of top officials
4. News about U.S. diplomacy
5. U.S. positions
6. Important government places
7. Information about military facilities:
   - Location
   - Units
   - Weapons used
   - Fortifications & tunnels
   - Amount of lighting
   - Exterior size and shape
   - Number of soldiers & officers
   - Ammunition depot locations
   - Leave policies
   - Brigades and names of companies
   - Degree & speed of mobilization
What is a Blog?

A frequent, chronological publication of personal thoughts and Web links; a journal:

- a mixture of what is happening in a person's life and what is happening on the Web
- a kind of hybrid diary/guide site
- there are as many unique types of blogs as there are people

MyBlogLog.com

Chasing Daisy

Your 7-Day free trial of MyBlogLog Pro will expire on Friday, March 10, 2005. You have been given a trial of MyBlogLog Pro so you can see how cool it is: realtime, historical, and full daily stats. If you do not upgrade to MyBlogLog Pro you will be switched to our free version after seven days. Then you will miss out on a lot of great features. Summer, huh?

Today    Yesterday    Mar. 2    Mar. 1    Feb. 28    Feb. 27    Feb. 26
30 Day Total: 7 affiliate clicks | 6 page views | 4 readers

<table>
<thead>
<tr>
<th>Rank</th>
<th>Link Name</th>
<th>Link URI</th>
<th>Clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>I like your content</td>
<td><a href="http://www.imagetr.com/Tools/fig.php">http://www.imagetr.com/Tools/fig.php</a></td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>BBC's weekly trivia contest happened</td>
<td><a href="http://news.bbc.co.uk/1/hi/football/4360539.stm">http://news.bbc.co.uk/1/hi/football/4360539.stm</a></td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Lynne Wiener</td>
<td><a href="http://www.diaspora.com/explains.htm">http://www.diaspora.com/explains.htm</a></td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>A Nation</td>
<td><a href="http://news.bbc.co.uk/1/hi/football/4360539.stm">http://news.bbc.co.uk/1/hi/football/4360539.stm</a></td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>I could have been a contender</td>
<td><a href="http://buzzyworld.typepad.com/it_could_have">http://buzzyworld.typepad.com/it_could_have</a> Been_a_contender/</td>
<td>1</td>
</tr>
</tbody>
</table>
Military Blogging

UNCLASSIFIED // FOUO
Internet Cafes can be found on military bases, generally operated by MWR or private businesses when located outside the installation.
• Posting sensitive photographs to the internet (especially those showing the results of IED strikes, battle scenes, casualties, and destroyed or damaged equipment)

• Providing information which enhances the enemy’s targeting process

• Exploitation

• OPSEC is everyone’s responsibility
  • While they are therapeutic, they are also a snap-shot in time and the whole world is reading…
DOD Guidance and Legalities

- DOD Guidance states that an OPSEC review will be conducted prior to public release

- An OPSEC review is an evaluation of a document to ensure protection of sensitive or critical information.

- The following publications and memorandums address the issue
  - AR 530-1, Operations Security, 3 Mar 95
  - DoDD 5230.9, Clearance of DoD Information for Public Release, 21 Nov 03
  - Numerous SecDef, Secretary of the Army, CofS, and other official messages
As an active-duty service member, you have free speech rights, but these rights are limited. Here are some basic guidelines to what you can and can’t say and do as a member of the military. You have the right to …

- Read anything you want
- Write letters to newspapers
- Publish your own newspaper, as long as you don’t use military supplies or equipment to do so
DoD Website OPSEC Guidance

SECDEF’s Jan 03 OPSEC Message

14 Jan 2003
R 141553Z JAN 03 FM SECDEF WASHINGTON DC
TO ALDODACT
INFO RUEKJCS/SECDEF WASHINGTON DC//DASD SIO//SECURITY//
UNCLAS ALDODACT 02/03 ADDRESSEES PASS TO ALL SUBORDINATE COMMANDS

SUBJECT: WEB SITE OPSEC DISCREPANCIES

1. AN AL QAEDA TRAINING MANUAL RECOVERED IN AFGHANISTAN STATES: "USING PUBLIC SOURCES OPENLY AND WITHOUT RESORTING TO ILLEGAL MEANS, IT IS POSSIBLE TO GATHER AT LEAST 80% OF INFORMATION ABOUT THE ENEMY." 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.

2. THE FACT THAT FOR OFFICIAL USE ONLY (FOUO) AND OTHER SENSITIVE UNCLASSIFIED INFORMATION (E.G., ONOPS, OPLANS, SOP) CONTINUES TO BE FOUND ON PUBLIC WEB SITES INDICATES THAT TOO OFTEN DATA POSTED ARE INSUFFICIENTLY REVIEWED FOR SENSITIVITY AND/OR INADEQUATELY PROTECTED. OVER 1500 DISCREPANCIES WERE FOUND DURING THE PAST YEAR. THIS CONTINUING TREND MUST BE REVERSED.

3. THE DOD WEB SITE ADMINISTRATION POLICY (LINK AT WWW.DEFENSELINK.MIL/WEBMASTERS) REQUIRES THAT INFORMATION BE REVIEWED FOR DATA SENSITIVITY PRIOR TO WEB POSTING AND PROTECTED ACCORDINGLY. THIS REVIEW IS TO BE ACCOMPLISHED IN ACCORDANCE WITH DOD DIRECTIVE 5230.9, CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE, AND DOD INSTRUCTION 5230.29, SECURITY AND POLICY REVIEW OF DOD INFORMATION FOR PUBLIC RELEASE, AND MUST INCLUDE OPERATIONS SECURITY (OPSEC) CONSIDERATIONS AS DEFINED BY DOD DIRECTIVE 5205.2, DOD OPERATIONS SECURITY (OPSEC) PROGRAM.

4. USING THE OPSEC PROCESS IN A SYSTEMATIC WAY AND THINKING ABOUT WHAT MAY BE HELPFUL TO AN ENEMY PRIOR TO POSTING ANY INFORMATION TO THE WEB COULD ELIMINATE MANY VULNERABILITIES. THE INTERAGENCY OPSEC SUPPORT STAFF (IOSS) CAN PROVIDE PROFESSIONAL ASSISTANCE WITH THE OPSEC PROCESS (SEE WWW.IOSS.GOV). LIMITING DETAILS IS AN EASILY APPLIED COUNTERMEASURE THAT CAN INCREASE VULNERABILITIES WHILE STILL CONVEYING THE ESSENTIAL INFORMATION. SECURITY AND ACCESS PROTECTIONS MUST BE APPLIED ACCORDING TO THE SENSITIVITY OF DATA FOR BOTH WEB PAGES AND WEB-ENABLED APPLICATIONS. UNPUBLISHED ADDRESSES (URLS) AND UNLINKED WEB PAGES DO NOT PROVIDE SECURITY. SEE PART V, TABLE 1 OF THE WEB SITE ADMINISTRATION POLICY FOR FURTHER GUIDANCE.

5. HEADS OF COMPONENTS ARE RESPONSIBLE FOR MANAGEMENT OF INFORMATION PLACED ON COMPONENT WEBSITES. THEY MUST ENSURE THAT WEBSITE OWNERS TAKE RESPONSIBILITY FOR ALL CONTENT POSTED TO THEIR WEBSITES. WEBSITE OWNERS MUST REDOUBLE THEIR EFFORTS TO: A. VERIFY THAT TO ILLEGAL MEANS, IT IS POSSIBLE TO GATHER AT LEAST 80% OF INFORMATION ABOUT THE ENEMY. 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.

Terrorist manual - 80% of information about enemy gathered openly

1500 discrepancies during past year

Review information prior to posting – include OPSEC

Use OPSEC process – “Who is the intended audience?”

Commanders responsible for content & verification of need

Provide security training for those responsible for content
DA OPSEC Guidance – Feb 03

COMMANDERS AT ALL LEVELS MUST:

REVIEW THEIR WEBPAGES, ENSURE THEY ARE OPSEC COMPLIANT

APPLY THE OPSEC REVIEW PROCESS OUTLINED IN AR530-1

LIMIT DETAILS ABOUT SPECIFIC CAPABILITIES OR READINESS

ENSURE REVIEWING OFFICIALS AND WEBMASTERS ARE OPSEC TRAINED

ENSURE ALL ARMY WEB SITES ARE REGISTERED

VERIFY VALID MISSION NEED TO DISSEMINATE THE INFORMATION POSTED

AWRAC & 1st IO CMD SEARCH, IDENTIFY & REPORT WEBSITE OPSEC CONCERNS
CSA OPSEC Memo dated 4 Dec 03

- Protecting information is vital to Army success.

- “For Official Use Only” (FOUO) will be the standard marking for all unclassified products which, if released to the public, could cause harm to Army Operations or personnel including, but not limited to, force protection, movement and readiness data, and evolving tactics, techniques, and procedures. Where feasible, information that bears protection should be moved .... to the SIPRNET.”

- Do not assist the adversary by providing open source information.
Questions for the band:  Searched 8 forums

posted on 13-Jun-2005 3:24:45 PM I have a question for the whole band.

Gentlemen, I am with the 1st Brigade 101st ABN (AASLT) div stationed at Ft Campbell, KY. I was wondering what you have planned for the 20th of Sep 05. We are planning a family event for all the soldiers and their families prior to our return to Iraq. I understand that you are busy and may have other obligations but I thought I would ask. You have been very supportive of the soldiers in the past and it is very much appreciated. It would mean a lot to these soldiers and their families if you could make some sort of appearance. Many of us are returning for our second or third time and the strain on the families has been tough to say the least. Please let me know either way. Thank you for your time and consideration.

Name and Titled Deleted
101st ABN Div (AASLT), Bastogne"
"It is Monday again and we are still at K-2 airfield in Bayji. As a squadron, we are 'demonstrating a military presence.' That means the troops set up checkpoints and stop hundreds of cars, searching them and the people. They keep taking these 'detainees' or EPWs and I have partial responsibility for the 'jail', which is a building here on the airfield. But we are not set up for this. MPs are supposed to come and get them almost immediately but they take a while. Plus the Civil Affairs/Counter Intelligence teams that are supposed to talk to them don't know crap and the whole thing borders on a war crime. I am just trying to find blankets and light and medical care for the prisoners.
Serviceman Demoted

Guardsman punished for allegedly posting classified information

The Associated Press
Updated: 8:25 a.m. ET Aug. 2, 2005
PHOENIX - An Arizona National Guardsman serving in Iraq has been demoted for posting classified information on his Internet Web log, an Army official said Monday.

- Leonard Clark, 40, was demoted from specialist to private first class and fined $1,640, said Col. Bill Buckner, a spokesman for the Multi-National Corps-Iraq
- Soldiers in Iraq are allowed to maintain blogs or Web sites but cannot post information about Army operations or movements. They also are barred from posting information about the death of a soldier whose family hasn't yet been notified
This website explains that Jihadists have been authorized by God to break the control of the media from the Zionists.

- To stop communicating with one another by email entirely and instead use the site’s web-forum.
- To only use public computers that cannot be in any way linked to them.
- To use anonymous IP address websites in order to mask their identity while navigating.
- To not publish any of their identifying information in their online forum registration or in their forum posts.
Jihadist Use of Open Source

Image on the right was seen on a Jihadist website in May 2005. It is an image taken by a soldier and posted to a BLOG.

Image on the left is another example. It was also posted to a Jihadist website in May 2005. The Arabic caption reads: “G (RPG-7) 7 Nothing happened to it due to its use of reactive armor”.

US Equipment Vulnerabilities

Driver of Alpha 41 (the luckiest STRYKER Driver in Mosul)

This is the result of a medium sized-IED on our main scanning vehicle, The Buffalo. While no one was injured, it was still a sad day to see our most armored vehicle knocked out.

Thanks to the 10 panes of ballistic glass in each window, no one was hurt in this blast.
Summary

- DOD Guidance
  - Prior to posting information in the public domain, it should have an OPSEC review by the OPSEC officer IAW AR 530-1
    - Military Operations and Exercises information:
      - Unit readiness specificity
      - Tactics, Techniques, and Procedures
    - Personnel Information:
      - Identifying family members and military personnel-specific details
      - Disciplinary actions
    - Proprietary Information and Scientific:
      - Critical technology
      - Test & Evaluation and Research & Development of existing equipment
    - Intelligence Information:
      - Communications Intelligence
      - Sources and Methods
      - Protection of identities of undercover Intelligence Officers, Agents, Informants, etc
    - Other Information:
      - Outsourcing studies
      - Administrative dispute resolutions

Information you have access to, though UNCLASSIFIED, has value to an adversary
QUESTIONS?

Don't Blog on Me