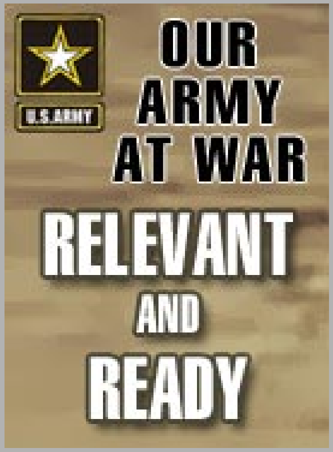
U.S. Army 1st Information Operations Command

1st BN - Vulnerability Assessment Division (VAD)

OPSEC in the Blogosphere



Purpose

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

OPSEC Definition of Threat

“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	NON TRADITIONAL
EXTERNAL	Foreign Governments Foreign Intelligence Services (FIS)	Al Qaeda Warlords
DOMESTIC	Hackers Militia Groups	Drug Cartel Media

- Combinations
- Combinations of all of the above
- Long Term
- Short Term

UNCLASSIFIED // FOUO

Paramilitary, Insurgent, Radical, Terrorist Threats Active in OIF/OEF Theaters

1. Small arms fire (SAF)	279	23.3%
2. Improvised explosive device (IED) attack	219	18.3%
3. Hostile-ambush	62	5.2%
4. Hostile-vehicle borne (VBIED)	55	4.6%
5A. Hostile-helicopter shot down/downed	53	4.4%
5B. Hostile-mortar attack	53	4.4%
6. Hostile-rocket propelled grenade (RPG) attack	50	4.2%
7. Hostile-vehicle accident	25	2.1%
8. Hostile-helicopter crash (missile attack)	22	1.8%
9. Hostile- sniper fire	17	1.4%
10. Hostile-rocket attack	14	1.2%

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

Source: http://www.centcom.mil/CENTCOMNews & http://casualties.org/oif/stats.aspx, 5 OCT 04

U

Adaptive, cunning, and learning Adversary ... unlike most previous experiences

Vulnerabilities

PING!
ARE YOU QUITE SURE YOU REALLY ABSOLUTELY 100% WANT TO SEND THIS EMAIL?
OK
NOPE
CANCEL

BLOGGER - Microsoft Internet Explorer provided by Compaq

http://www.blogger.com/

WHAT'S UP

USA Today Iraqis enjoy new freedom of expression: "We suffered for years under Saddam Hussein, not being able to speak out,' says Omar Fadhil, 24, a dentist. 'Now, you can make your voice heard around the world." You said it Omar. That's pretty much our whole thing.
- Biz [4/20/2004] #

We're Back Y'all Thanks to everyone who showed up at our little Blogger shindig at Club De Ville in Austin, TX. That was fun, here's some photos.
- Biz [3/25/2004] #

Mess with Texas Some of us Blogger folks are going to SXSW and to kick things up a notch we're serving up free drinks and t-shirts Monday evening from 6:30-8:00 on March 15th over at Club De Ville in Austin, TX. We provide beer and schwag to our users because we care.
- Biz [3/5/2004] #

Blog Me Tender Valentines Day is almost here so we'd be remiss if we didn't show you How To Network With Blogger. (It's the thing to do.) And stay tuned for part two of our v-day tutorial extravaganza. That's right, it's a

FRESH BLOGS

The 10 most recently published blogs:

GARMIN

The Rino 110/120

Handheld GPS, combined with two-way radio/receiver. Allows you to send your position to another Rino user within a 2 mile radius.

Whole Earth Provision Company

OPSEC Defined

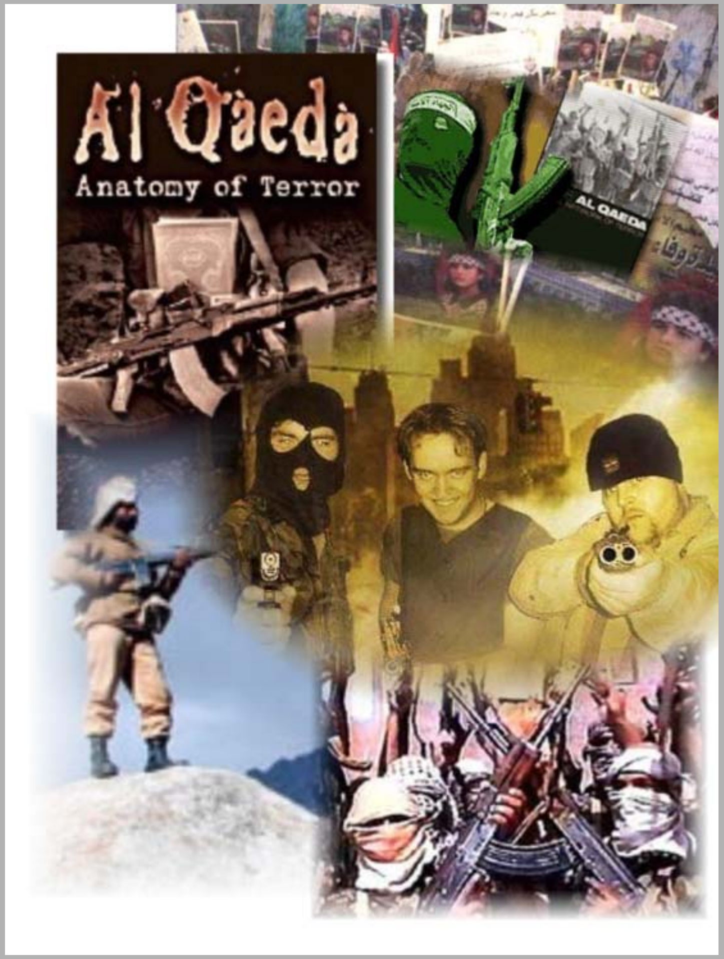
- A process of identifying Essential Elements of Friendly Information (EEFI) and subsequently analyzing friendly actions attendant to military operations and other activities to:

  - **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:

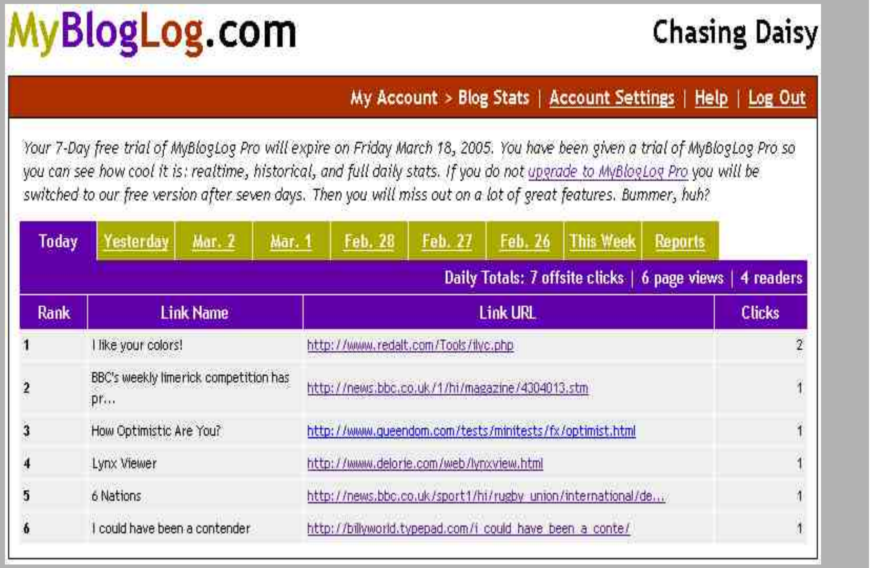
1. Names/photographs of important people
2. Present and future U.S. capabilities
3. Meetings of top officials
4. News about U.S. diplomacy
5. U.S. positions
6. Important government places
7. Information about military facilities:
    - Location
    - Units
    - Weapons used
    - Fortifications & tunnels
    - 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 18, 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. Bummer, huh?

Today | Yesterday | Mar. 2 | Mar. 1 | Feb. 28 | Feb. 27 | Feb. 26 | This Week | Reports

Daily Totals: 7 offsite clicks | 6 page views | 4 readers

Rank	Link Name	Link URL	Clicks
1	I like your colors!	http://www.redalt.com/Tools/ilyc.php	2
2	BBC's weekly limerick competition has pr...	http://news.bbc.co.uk/1/hi/magazine/4304013.stm	1
3	How Optimistic Are You?	http://www.queendom.com/tests/minitests/fx/optimist.html	1
4	Lynx Viewer	http://www.delorie.com/web/lynxview.html	1
5	6 Nations	http://news.bbc.co.uk/sport1/hi/rugby_union/international/de...	1
6	I could have been a contender	http://billyworld.typepad.com/i_could_have_been_a_conte/	1

Military Blogging

ArmyTimes
14 March 2005
www.armytimes.com

NEW SERGEANTS
20,000 IDENTIFIED FOR FASTER STRIPES 20

Recruiting falls short *Active Army misses February goal* 10

War protest *Sixth-graders unload on private in Korea* 18

Senior NCO moves Thousands eyed for promotion, schooling 21

ABRAMS REPORT CARD
SAFETY UPGRADES EYED FOR TANKS IN IRAQ 8

FORT BRAGGISTAN
WHY CAROLINA POST BECAME AFGHANISTAN FOR TWO WEEKS 30

SOLE SEARCHING
TIPS FOR BUYING RUNNING SHOES 35

INSIDE

LIVE FROM IRAQ

BAND OF BLOGGERS

Soldiers are online & uncensored.
Is OpSec at risk as war diaries catch on? 14

PLUS 10 tips on starting your own blog 16

THE MUDVILLE GAZETTE
Argghhh!!!
THE HOME OF TWO OF JONAH'S MILITARY GUYS +1 ©
BLACK FIVE
SGT. HOOK
THIS WE'LL DEFEND
Blogosphere Truth Squad
We can fact-check your ass without even getting dressed!
http://mamamontezz.mu.nu/

Internet Cafe

Internet Cafes can be found on military bases, generally operated by MWR or private businesses when located outside the installation

Blog OPSEC Concerns & Issues

- 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

1st Amendment Issues

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

Terror Alert Notice

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

Terrorist manual - 80% of information about enemy gathered openly

TO ILLEGAL MEANS, IT ... D DATA MAKES A VAST, READILY VAILABLE SOURCE OF INFORMATION ON DOD PLANS, PROGRAMS, AND ACTIVITIES. ONE MUST CONCLUDE OUR ENEMIES ACCESS DOD WEB SITES ON A REGULAR BASIS.

1500 discrepancies during past year

2. THE FAC ... D 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. O ... D.

Review information prior to posting – include OPSEC

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 ... ORMATION FOR PUBLIC RELEASE, AND ... ERATIONS SECURITY (OPSEC) PROGRAM.

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

Commanders responsible for content & verification of need

4. USING THE OPSEC PROCESS IN A SYSTEMA ... 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 DECREASE VULNERABILITIES WHILE STILL CONVEYING THE ESSENTIAL INFOR ... DATA FOR BOTH WEB PAGES AND WEB-ENABLED ... SECURITY. SEE PART V, TABLE 1 OF THE WEB SITE ADMINISTRATION POLICY FOR FURTHER GUIDANCE.

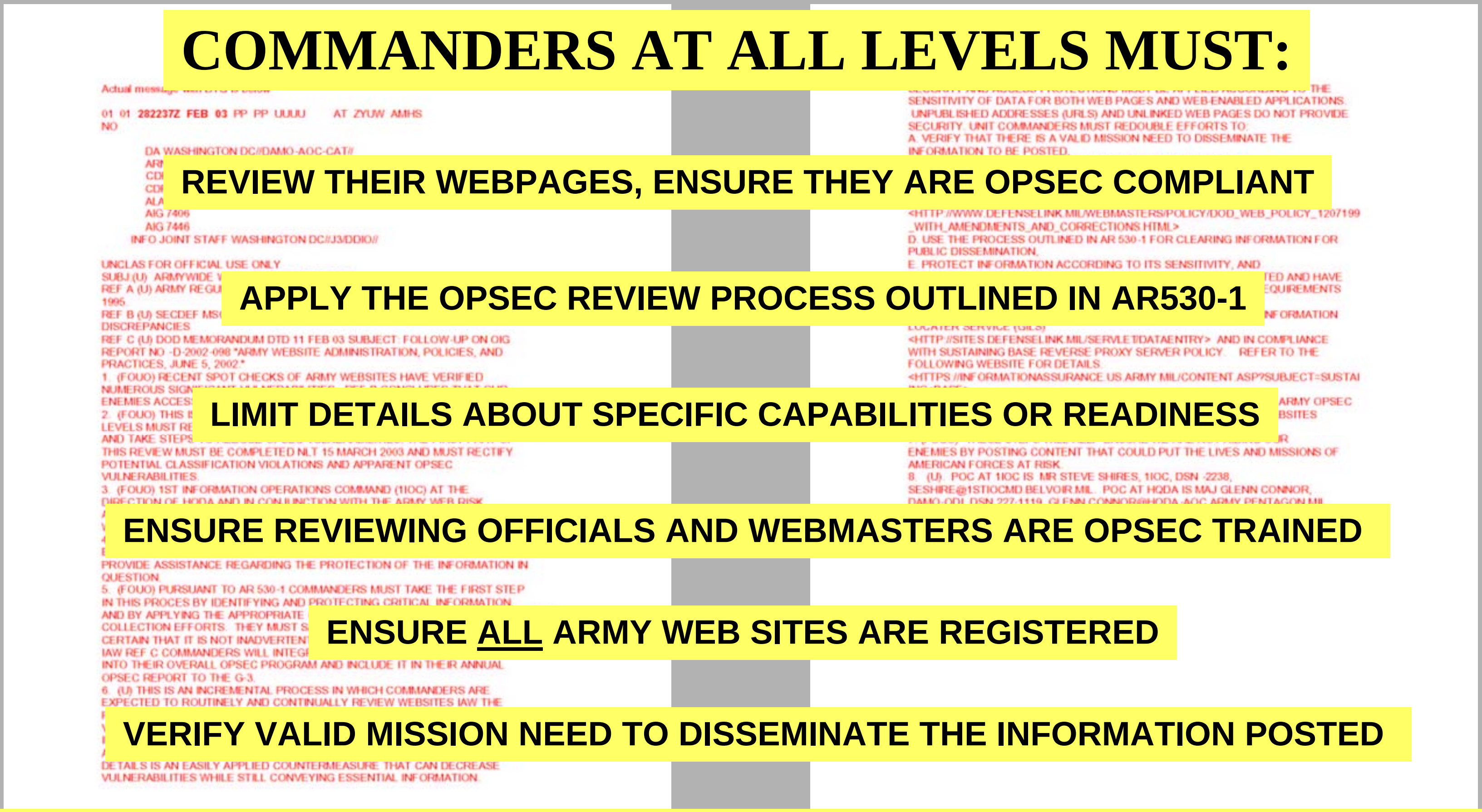
Provide security training for those responsible for content

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

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



Actual message with DTG is below

01 01 282237Z FEB 03 PP PP UUUU AT ZYUW AMHS
NO

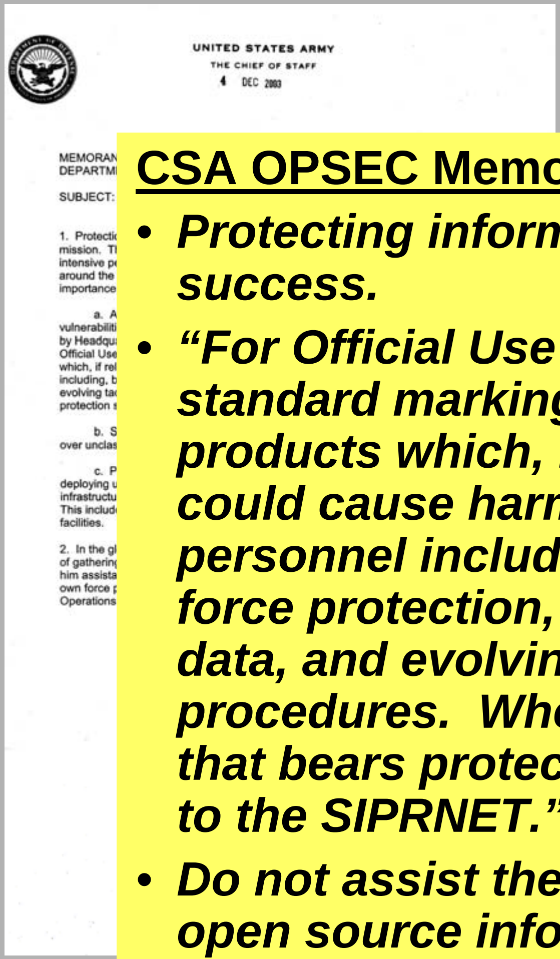
DA WASHINGTON DC//DAMO-AOC-CAT//
ARI
CD
CD
ALA
AIG 7406
AIG 7446
INFO JOINT STAFF WASHINGTON DC//J3/DDIO//

UNCLAS FOR OFFICIAL USE ONLY
SUBJ:(U) ARMYWIDE W
REF A (U) ARMY REGU
1995
REF B (U) SECDEF MS
DISCREPANCIES
REF C (U) DOD MEMORANDUM DTD 11 FEB 03 SUBJECT: FOLLOW-UP ON OIG REPORT NO -D-2002-098 "ARMY WEBSITE ADMINISTRATION, POLICIES, AND PRACTICES, JUNE 5, 2002."
1. (FOUO) RECENT SPOT CHECKS OF ARMY WEBSITES HAVE VERIFIED NUMEROUS SIGN
ENEMIES ACCES
2. (FOUO) THIS I
LEVELS MUST RE
AND TAKE STEPS
THIS REVIEW MUST BE COMPLETED NLT 15 MARCH 2003 AND MUST RECTIFY POTENTIAL CLASSIFICATION VIOLATIONS AND APPARENT OPSEC VULNERABILITIES.
3. (FOUO) 1ST INFORMATION OPERATIONS COMMAND (1IOC) AT THE DIRECTION OF HQDA AND IN CONJUNCTION WITH THE ARMY WEB RISK
PROVIDE ASSISTANCE REGARDING THE PROTECTION OF THE INFORMATION IN QUESTION.
5. (FOUO) PURSUANT TO AR 530-1 COMMANDERS MUST TAKE THE FIRST STEP IN THIS PROCES BY IDENTIFYING AND PROTECTING CRITICAL INFORMATION AND BY APPLYING THE APPROPRIATE
COLLECTION EFFORTS. THEY MUST S
CERTAIN THAT IT IS NOT INADVERTEN
IAW REF C COMMANDERS WILL INTEG
INTO THEIR OVERALL OPSEC PROGRAM AND INCLUDE IT IN THEIR ANNUAL OPSEC REPORT TO THE G-3.
6. (U) THIS IS AN INCREMENTAL PROCESS IN WHICH COMMANDERS ARE EXPECTED TO ROUTINELY AND CONTINUALLY REVIEW WEBSITES IAW THE
DETAILS IS AN EASILY APPLIED COUNTERMEASURE THAT CAN DECREASE VULNERABILITIES WHILE STILL CONVEYING ESSENTIAL INFORMATION.

SENSITIVITY OF DATA FOR BOTH WEB PAGES AND WEB-ENABLED APPLICATIONS. UNPUBLISHED ADDRESSES (URLS) AND UNLINKED WEB PAGES DO NOT PROVIDE SECURITY. UNIT COMMANDERS MUST REDOUBLE EFFORTS TO:
A. VERIFY THAT THERE IS A VALID MISSION NEED TO DISSEMINATE THE INFORMATION TO BE POSTED.
<HTTP://WWW.DEFENSELINK.MIL/WEBMASTERS/POLICY/DOD_WEB_POLICY_1207199_WITH_AMENDMENTS_AND_CORRECTIONS.HTML>
D. USE THE PROCESS OUTLINED IN AR 530-1 FOR CLEARING INFORMATION FOR PUBLIC DISSEMINATION.
E. PROTECT INFORMATION ACCORDING TO ITS SENSITIVITY, AND
TED AND HAVE
EQUIREMENTS
NFORMATION
LOCATER SERVICE (GILS)
<HTTP://SITES.DEFENSELINK.MIL/SERVLET/DATAENTRY> AND IN COMPLIANCE WITH SUSTAINING BASE REVERSE PROXY SERVER POLICY. REFER TO THE FOLLOWING WEBSITE FOR DETAILS.
<HTTPS://INFORMATIONASSURANCE.US.ARMY.MIL/CONTENT.ASP?SUBJECT=SUSTAI
ARMY OPSEC
BSITES
R
ENEMIES BY POSTING CONTENT THAT COULD PUT THE LIVES AND MISSIONS OF AMERICAN FORCES AT RISK.
8. (U) POC AT 1IOC IS MR STEVE SHIRES, 1IOC, DSN -2238, SESHIRE@1STIOCMD.BELVOIR.MIL. POC AT HQDA IS MAJ GLENN CONNOR,

AWRAC & 1st IO CMD SEARCH, IDENTIFY & REPORT WEBSITE OPSEC CONCERNS

CSA OPSEC Guidance – Dec 03



UNITED STATES ARMY
THE CHIEF OF STAFF
4 DEC 2003

MEMORAN
DEPARTM

SUBJECT:

1. Protecti
mission. Tl
intensive pe
around the
importance

a. A
vulnerabiliti
by Headqu
Official Use
which, if rel
including, b
evolving tac
protection s

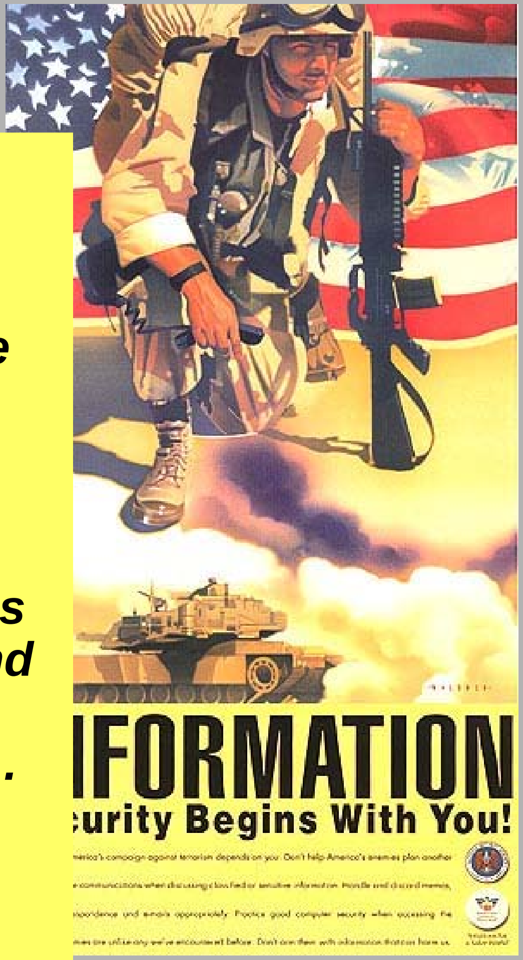
b. S
over unclas

c. P
deploying u
infrastructu
This includ
facilities.

2. In the gl
of gatherin
him assista
own force p
Operations

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.***



Real-Time Blog

Not Logged In? Who’s Online Now. You are here: 3 Doors Down Message Board
Search Results SubjectAuthorLast PostBoard
Do you have a question for Gregg……xxxx..13-Jun-2005 #:24:45 PM

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"

Real-Time Blog

Does this blog provide too much information?

"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

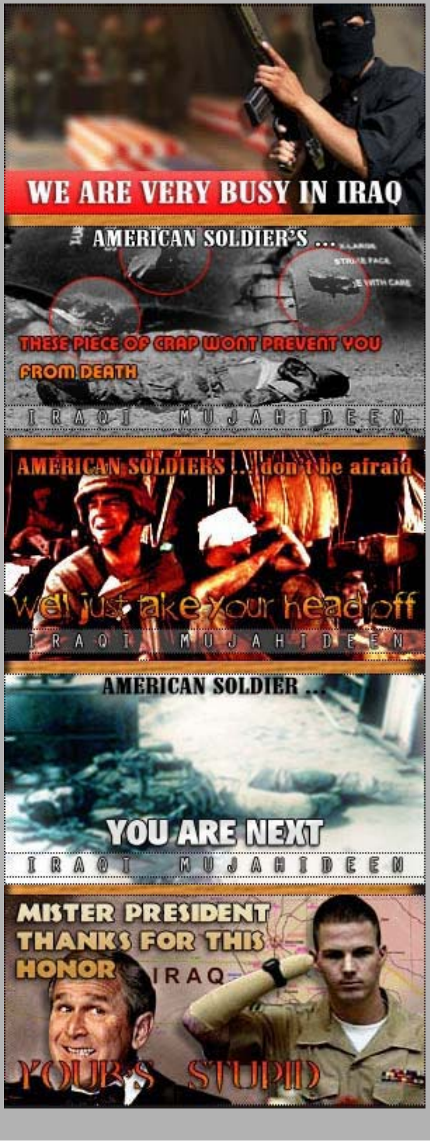
The Associated Press
Updated: 8:25 a.m. ET Aug. 2, 2005
PHOENIX - An Arizona National Guardsman serving in Iraq has been demoted for posting classified information on his Internet Web log, an Army official said Monday.

- **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**

"Jihadi Information Battalion"

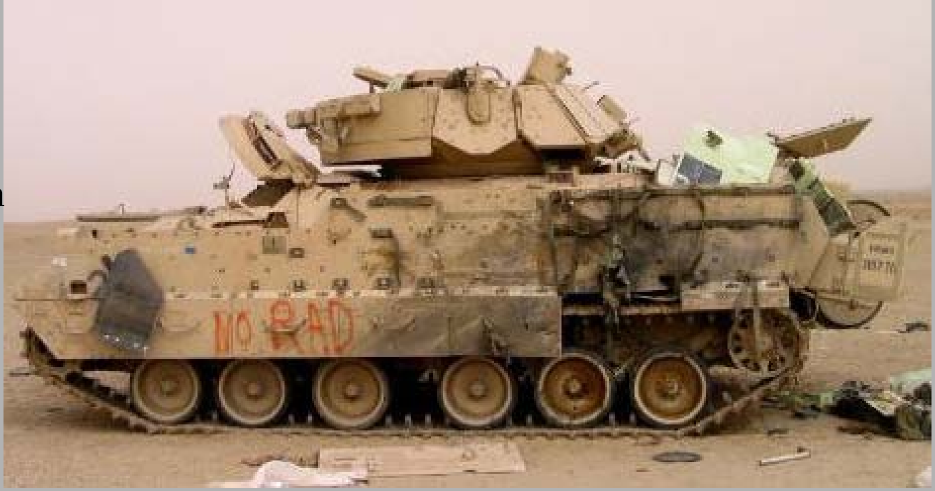
This website explains that Jihadists have been authorized by God to break the control of the media from the Zionists.

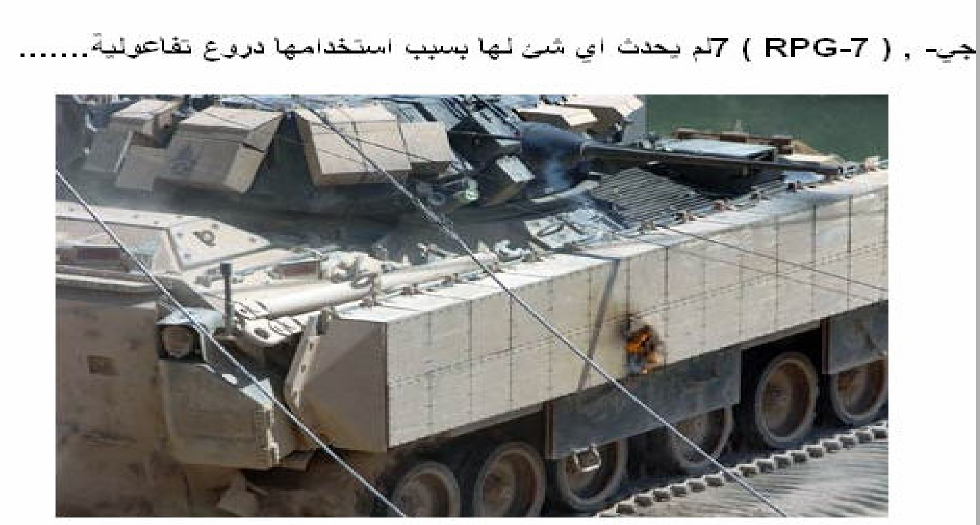
- To stop communicating with one another by email entirely and instead use the site's web-forum.
- To only use public computers that cannot be in any way linked to them.
- To use anonymous IP address websites in order to mask their identity while navigating.
- To not publish any of their identifying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

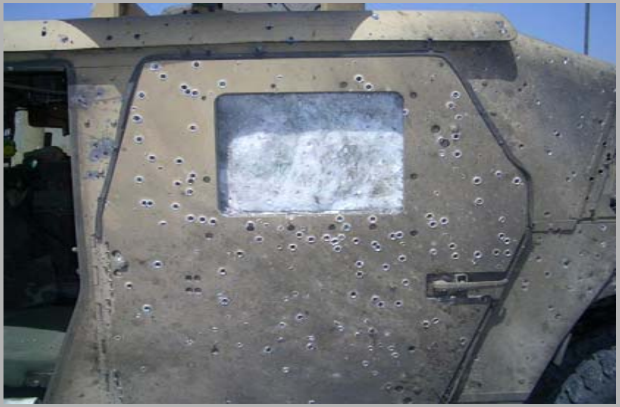




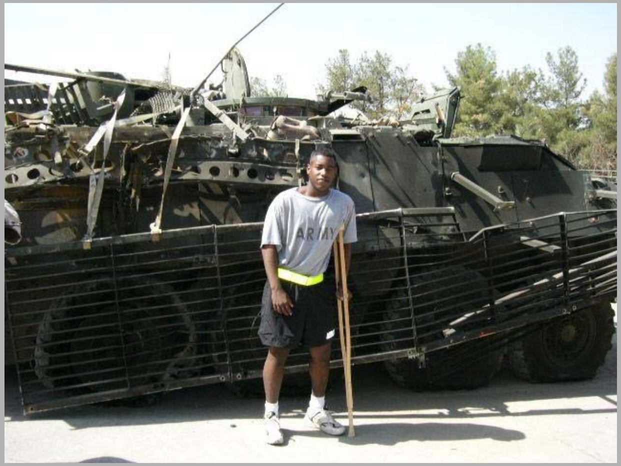
جي- , (RPG-7) 7لم يحدث اي شئ لها بسبب استخدامها دروع تفاعولية.......

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".

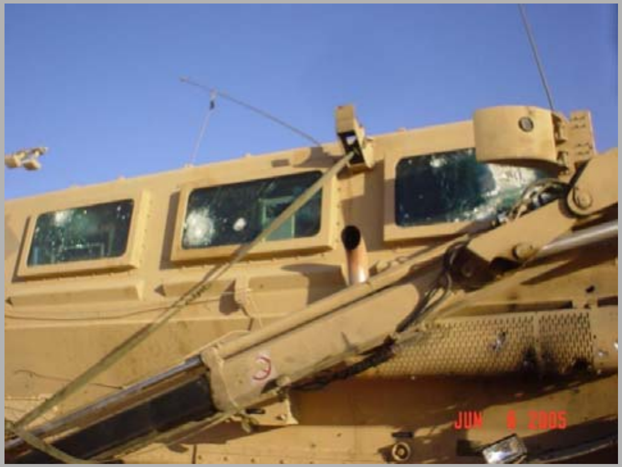
US Equipment Vulnerabilities



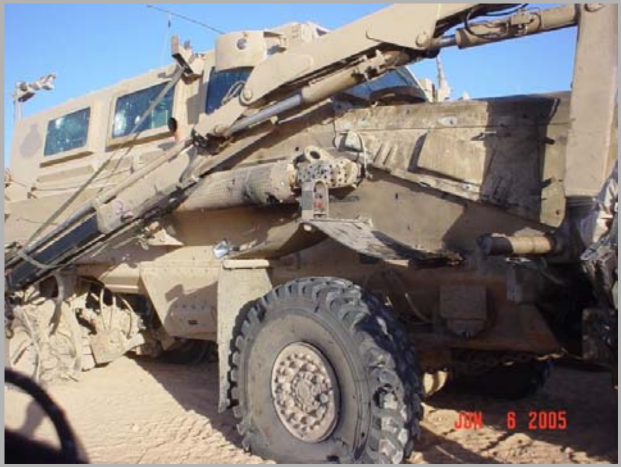
HMMWV



Driver of Alpha 41 (the luckiest STRYKER Driver in Mosul



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



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

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