Redactions were part of the original presentation.

PE 40

Road Map

- Key Evidence
- Formal Education and Training
- Work as an Intelligence Analyst
- Knowledge of WikiLeaks

Road Map

- Gharani Video (BE22PAX)
- CIDNE-I & CIDNE-A SIGACTS
- ACIC Report
- Apache Video
- Password Cracking
- JTF-GTMO Assessments
- OGA Documents
- Department of State Cables
- Farah Investigation File
- USF-I GAL

Road Map

- Causing Intelligence to be Published
- Aiding the Enemy

305th MI Battalion

Information Security
AR 380-5

Classification Designations

AR 380-5, page 10, para 2-10

Confidential - Cause *Damage*

Secret - Cause *Serious Damage*

Top Secret - Cause *Exceptionally Grave Damage*

To National Security.

Classification Process

page 9, para 2-7

In making a decision to originally classify an item of information, an original classification authority will:

a. Determine that the information has not already been classified

b. Determine that the information is eligible for classification

c. Determine that classification of the information is a realistic course of action and that information can be protected from unauthorized disclosure when classified.

d. Decide that unauthorized disclosure could reasonably be expected to cause damage to national security.

Classification Criteria

page 9, para 2-8

- Military Plans, Weapons Systems, or Operations
- Foreign Government Information
- Intelligence Activities, sources or methods
- Foreign Relations Or Activities Of The US
- Scientific, Technological, Or Economic Matters Relating To National Security
- US Government Programs For Safeguarding Nuclear Materials Or Facilities
- Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security

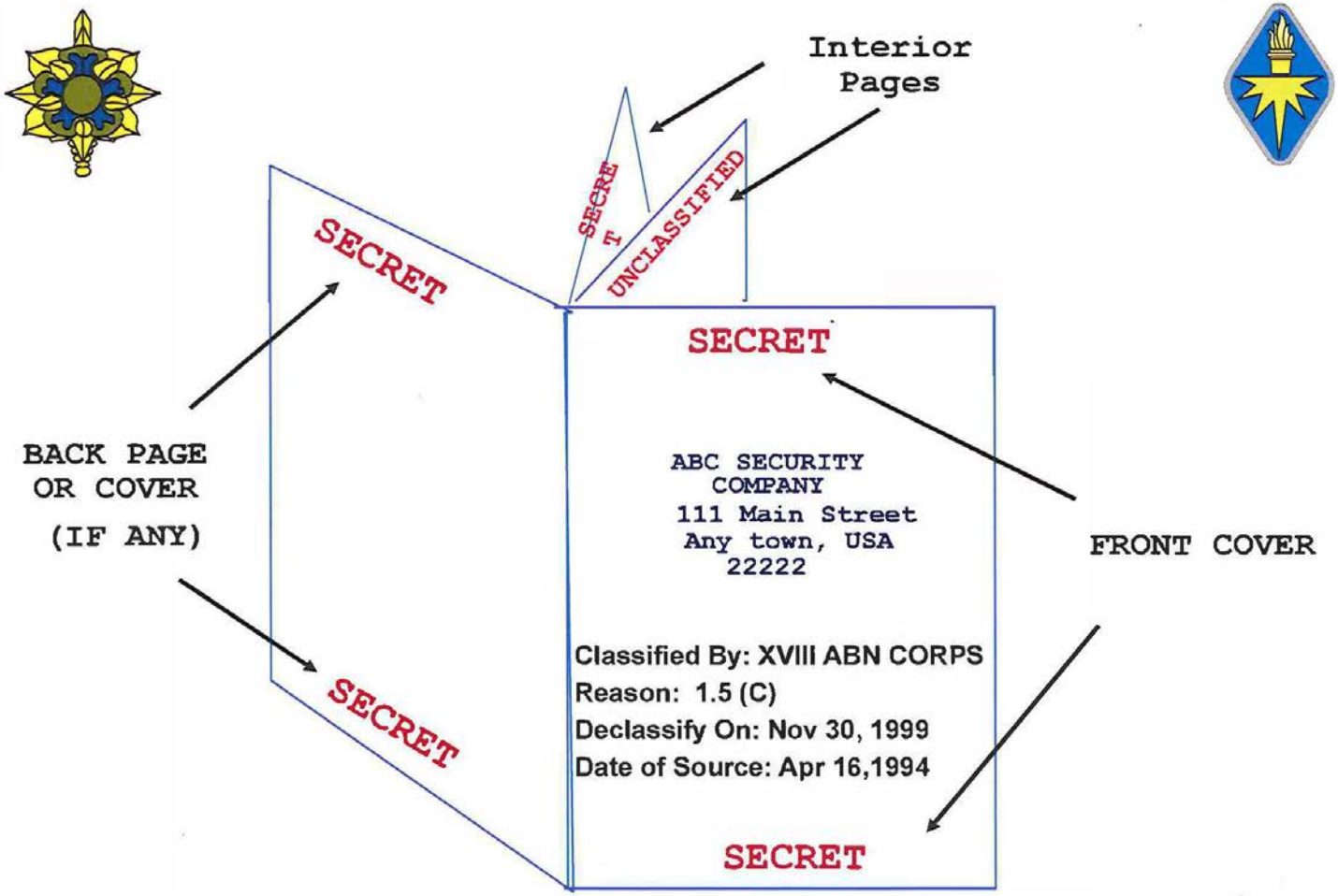
Prohibitions and Limitations

page 9-11, para 2-8, 2-15

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a Person, Agency or Organization
- Restrain competition

US classification can only be applied to information that is owned by, produced by or for, or is under the control of the US government.

ManningB_00007364



PE 52

Declassification Programs

page 14, para 3-1

Department of the Army files and records will not be declassified without prior review to determine if continued classification is warranted and authorized.

(1) Original classification authority action

(2) Automatic (Per Executive order)

(3) Mandatory

(4) Systematic

Individual Responsibility

page 3, para 1-9

- All personnel have an official responsibility to safeguard classified information.

- All personnel will report any violations or anything that could lead to the unauthorized disclosure of classified and sensitive information.

Storage Standards

page 78, para 7-3

Classified information must be secured under adequate conditions to limit access by unauthorized personnel.

- **General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for:**
  - **Containers**
  - **Vault Doors**
  - **Alarm Systems**
  - **Associated security devices suitable for storage and protection of classified material.**

Control Measures

page 67, para 6-9, 6-10

- DA personnel are responsible for ensuring that unauthorized persons do not gain access to classified information.

- Classified information will be protected at all times either by storage, having it under personal observation and physical control of an authorized individual.

Control Measures

page 33, para 4-34

Classified labels will be placed on all classified Automated Data Processing media

SF 708

SF 707

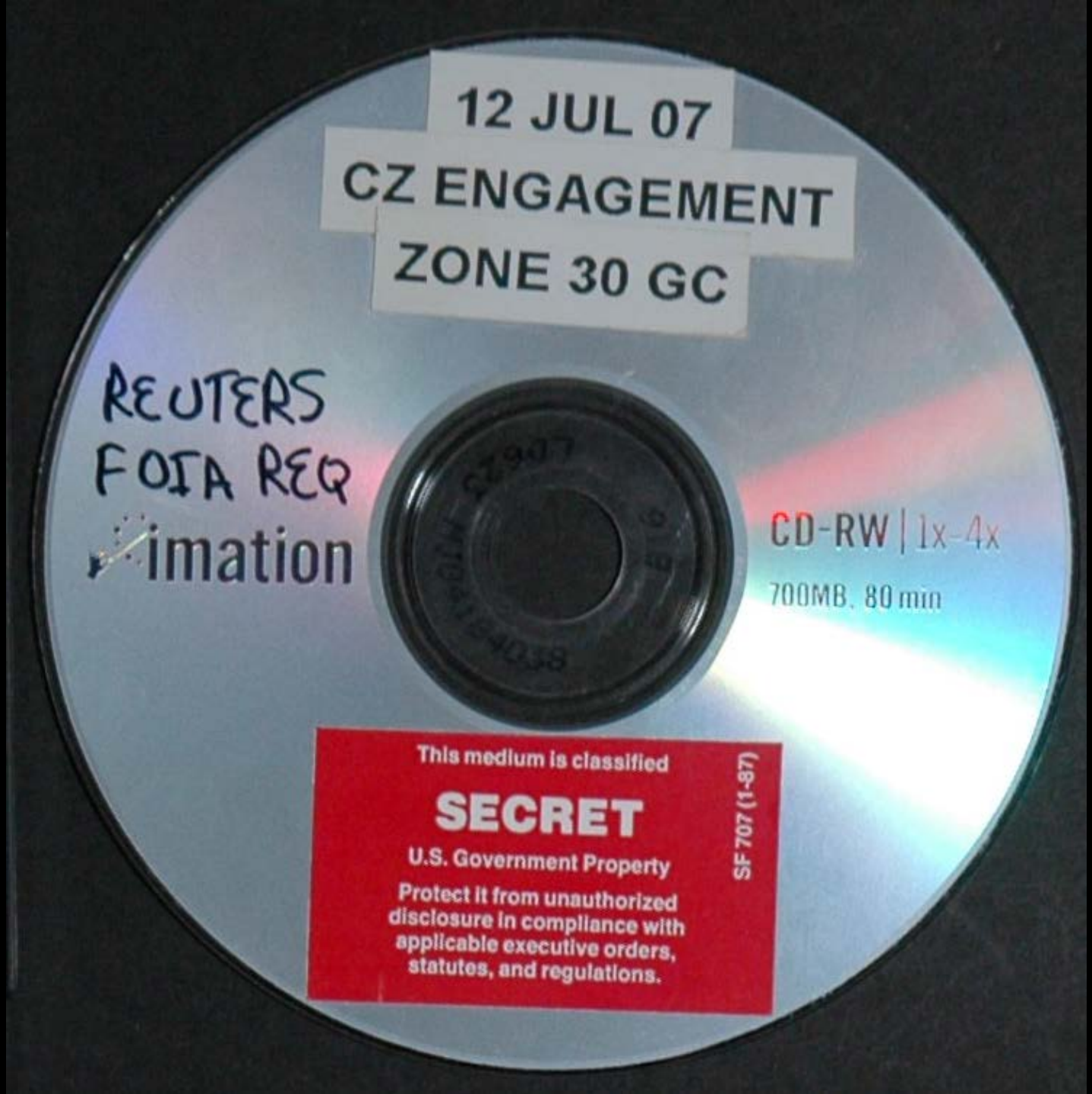
Others that may be used/seen:

SF 706

SF 711 - Data Descriptor Label
(yellow & black)

SF 712 - CLASSIFIED SCI Label
(yellow & white)

SF 710


12 JUL 07
CZ ENGAGEMENT
ZONE 30 GC
REUTERS
FOIA REQ
imation
CD-RW | 1x-4x
700MB, 80 min
This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.
SF 707 (1-87)

PE 15

OPSEC

The enemy will attempt to discover how and when we are conducting operations, knowing this, we must protect our activities from detection.

We do this by:

- **Identifying - Critical Information**
- **Analyzing - Threat**

Critical Information

- Photos
- Installation maps with highlights of designated points of interest (sleep/work, CDR, dining facility, etc)
- Security Operating Procedures (SOPs)
- Tactics, Techniques and Procedures (TTPs)
- Unit Capabilities and Intent
- Unit morale
- Personal/Family Information

Sensitive Information

Prevent Disclosure

- **DON'T DISCUSS OPERATIONAL ACTIVITIES ON THE WEB or E-mail**
- Ensure information posted has no significant value to the adversary
- Consider the audience when you're posting to a blog, personal web page or Email
- Always assume the adversary is reading your material
- Work with your OPSEC Officer – follow policies and procedures!

Remember it is called the World Wide Web for a reason

Al Qaeda

AKA: Usama Bin Ladin Organization

- Extreme Sunni (Wahabi) Islam
- NO religious tolerance
- Loose structure, little secrecy about leadership
- Network with many other like-minded groups
- State support (?)

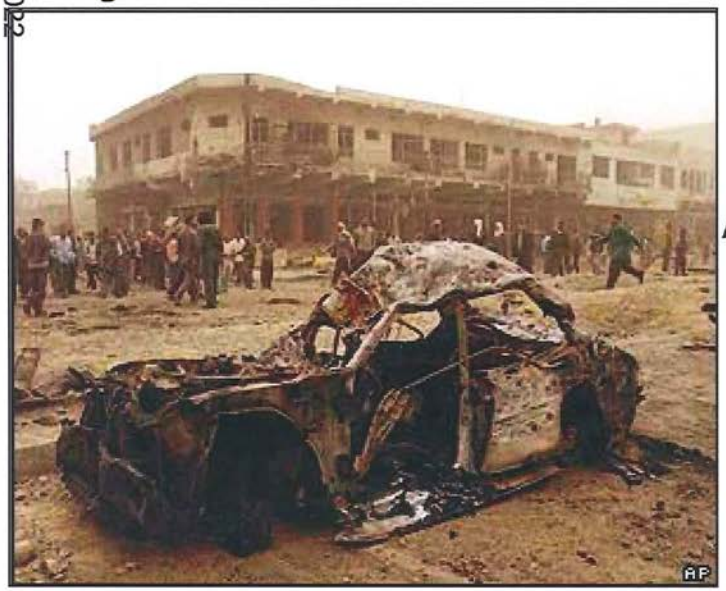
Tanzim Qaeda al-Jihad fi Bilad al-Rafidayn (QJBR)
AKA: Al Qaeda in Iraq (AQI), Tawhid and Jihad, AQIZ

Abu Musab al-Zarqawi
Killed 7 Jun 06

Abu Ayyub al-Masri an Egyptian operative is believed to be the new leader of Al Qaeda in Iraq.

- **"Monotheism and Holy War"**
  - The al Qaeda Group for Jihad in Iraq
- **Ties to al-Qaeda**
- **Kidnappings and executions**
- **Has also attacked Iraqi Police & Security Forces**

Recruiting



Baghdad
April 2003

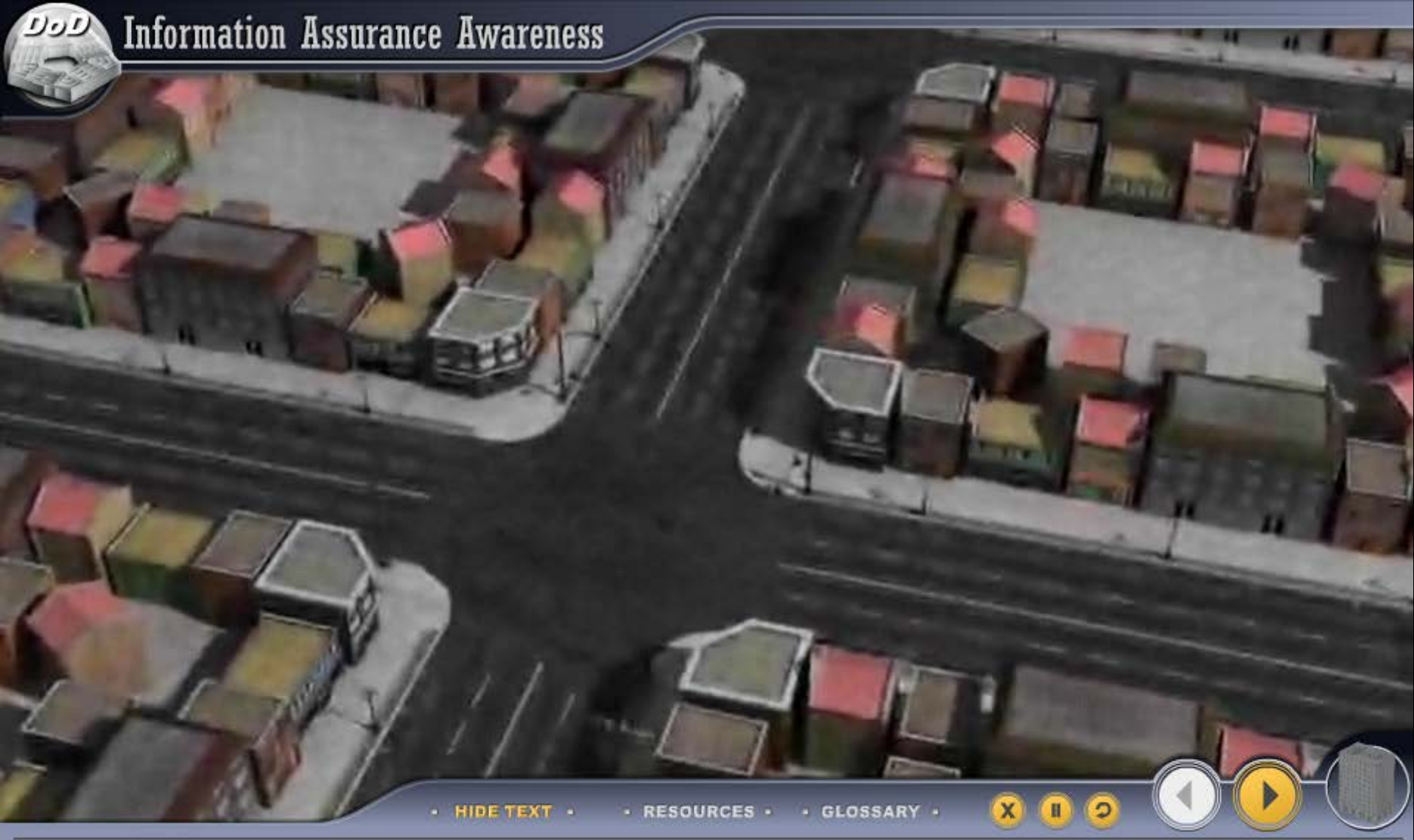
Islamic extremists are exploiting the Iraqi conflict to recruit new anti US Jihadists.

221

Recruiting

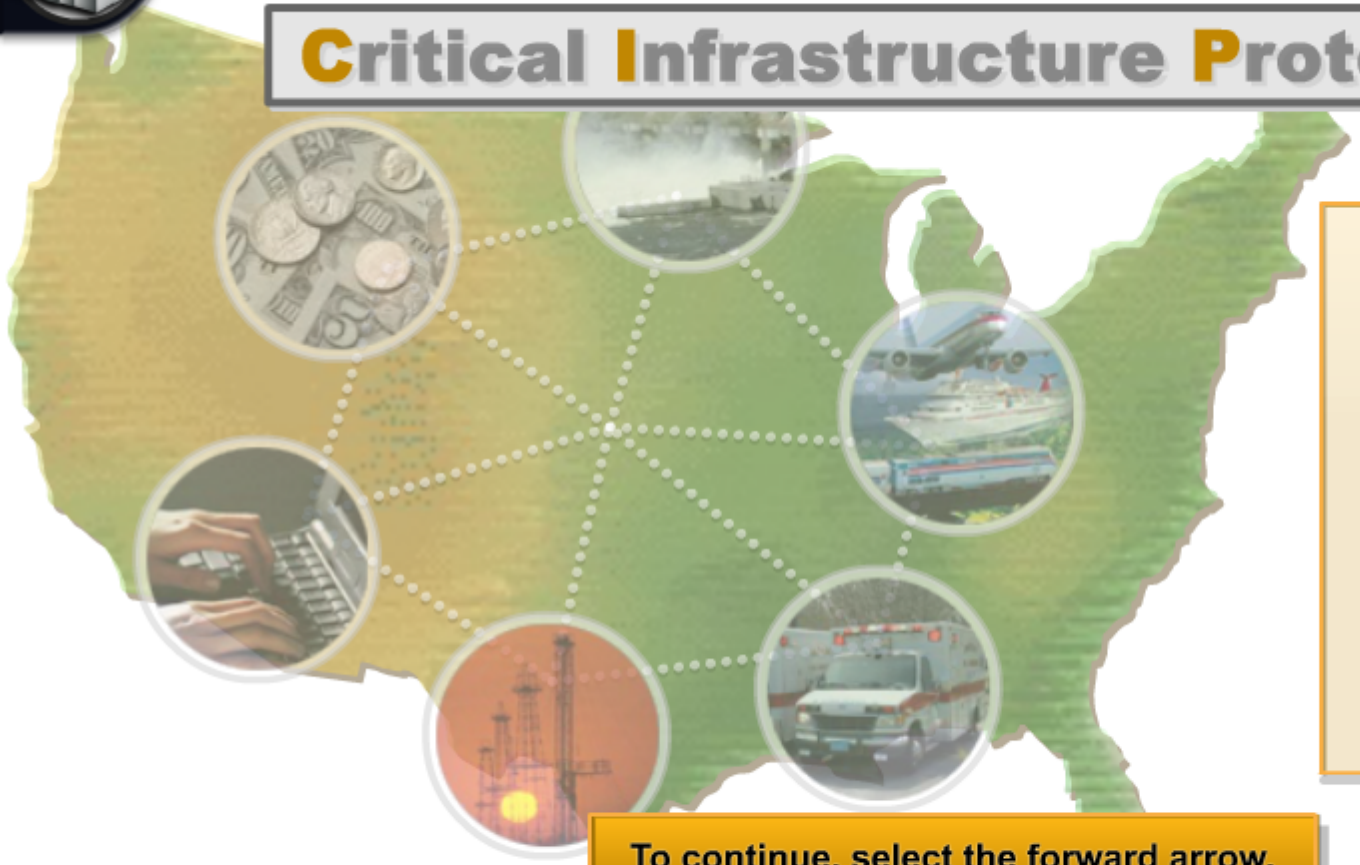
"No thanks, just browsing."

Over the last ten years, the number of terrorist sites has jumped from less than 100 to as many as 4,000. Many insurgency groups have many sites and message boards to help their network.



Okay, it might be a little farfetched, but it's not impossible. Each and every one of us plays a vital role in keeping DoD information and information systems safe. It only takes one security incident to start off a chain of events with serious consequences. So how do we prevent this from happening? By being aware of information assurance, or IA, and always following our organization's policies and general IA best practices.

Critical Infrastructure Protection



Critical infrastructure includes:

- Information technology and telecommunications
- Energy
- Banking and finance
- Transportation and border security
- Water
- Emergency services

To continue, select the forward arrow.

In the past, computers were standalone systems that were relatively easy to protect. What was once a collection of separate systems is now best understood as a single, globally connected network, including infrastructures neither owned nor controlled by DoD. Because of the interconnected nature of our information systems, a risk to one is a risk to all. If information and information systems are compromised, it can impact our missions, our national security, and ultimately, lives. In addition, because information systems are a vital part of the critical infrastructure of our country, our way of life is potentially at risk if information systems aren't adequately

To continue, select the forward arrow.

event. A system's environment, including poor building wiring or insufficient cooling for the systems, can also cause harm to information systems. Human threats can be internal or external. Internal threats can be careless, malicious or disgruntled users, users in the employ of terrorist groups or foreign countries, or can be self-inflicted unintentional damage, such as accidents or bad habits. External threats can be hackers, organized crime, terrorist groups, foreign countries, or protesters.

Operations Security (OPSEC)

PV2 Manning, Bradley

D Company, 305th Military Intelligence Battalion

Friday, 13 Jun 08

Executive Summary

- Definition of OPSEC
- Types of OPSEC Information
- Common OPSEC Violations
- Protection from Adversaries
- Conclusion

Definition of OPSEC

- Operations Security (OPSEC)
- Protection of Information:
  - Public Assets
  - Military Assets
  - Personnel
  - Families of Personnel
  - National Security

Types of Information

- Unclassified Information
  - Dates
  - Times
  - Locations
  - Names
- For Official Use Only (FOUO)
  - Mission Critical Information
  - Capabilities
  - Vulnerabilities

Dates and Times

- Events
  - Large groups
    - Public
    - Military Personnel
    - Department of Defense Civilians
    - Contractors
  - Officials
    - High Ranking NCO's
    - Commanders
  - VIP's
    - Politicians
    - Diplomats

Location Information

- Government Facilities
  - Public Buildings
  - Government Agencies
- Military Installations
  - Secure Facilities
  - Weapons and Equipment
  - Training Locations
  - Barracks

Individual Information

- Personal Information
  - Names
  - Dates of Birth
  - Addresses
  - Social Security Numbers
  - Credit Information
  - Family Members

Official Information

- Methods
  - Intelligence Gathering
- Equipment
  - Weapons
  - Vehicles
- Capabilities
- Vulnerabilities
- Mission Critical Information

Adversaries

- Foreign Governments
  - Rivals
  - Enemies
- Non-Government Organizations
  - Corporations
  - Political Groups
  - Terrorists
- Anyone
  - Activists
  - Hackers

Common OPSEC Leaks

- Written Sources
  - Newspapers
  - Magazines
- Television
  - News Programs
  - Documentaries
- Internet
  - Discussion Boards
  - Chat Rooms
  - Social Networking
  - Videos

Conclusion

- Avoid Disclosure of Information
  - Public Conversations
  - Journalists
  - Posting Information
    - Newsletters
    - Fliers
    - Internet
- Use Common Sense
  - Many Enemies
  - Free and Open Society

You can currently contact our investigations editor directly in Iceland +354 862 3481 ; 24 hour service; ask for "Julian Assange".

WikiLeaks ✓
@wikileaks

Follow

Have encrypted videos of US bomb strikes on civilians http://bit.ly/wlafghan2 we need super computer time http://ljsf.org/

Reply Retweet Favorite More

147 RETWEETS **37** FAVORITES

12:10 PM - 8 Jan 10

PE 32b

Items of Historical Significance for Two Wars:

Iraq and Afghanistan Significant Activities (SIGACTs) between 0000 on 01 JAN 2004 and 2359 on 31 DEC 2009 (Iraq local time, and Afghanistan local time)

CSV extracts are from the Department of Defense (DoD) Combined Information and Data Exchange (CIDNE) Database.

It's already been sanitized of any source identifying information.

You might need to sit on this information, perhaps 90-180 days, to figure out how best to release such a large amount of data, and to protect source.

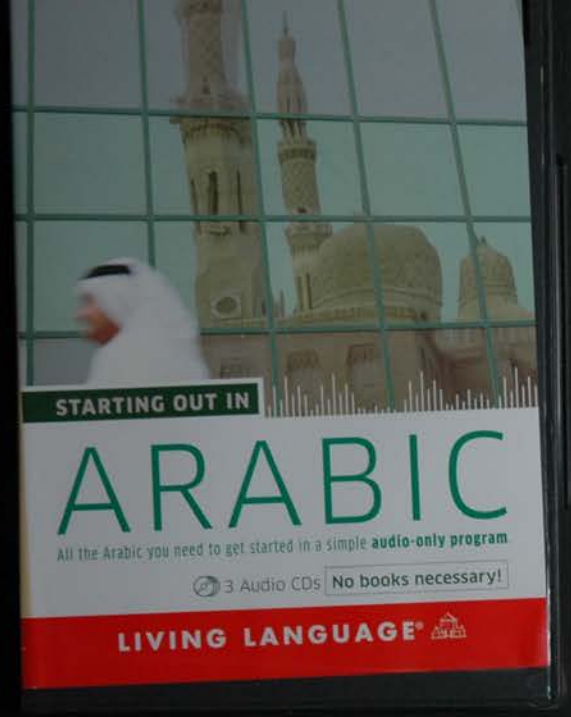
This is possibly one of the more significant documents of our time, removing the fog of war, and revealing the true nature of 21st century asymmetric warfare.

Have a good day.

PE 40

On 5/19/10 6:22 PM, Bradley Manning wrote:

> Good question.
>
> There's a few answers I have to various other questions as well:
>
> 1. I approved the edits without actually viewing the video. (Had a written description.)
>
> 2. I "saw" an RPG and many, many more weapons the first time I saw the video. I was numb. I explored it further, and found out what actually happened later. I wanted the video to challenge that cognitive bias that every young Iraqi male is an insurgent.
>
> 3. I instructed there to be an Orwell quote, description of the journalists, and some general context. Assange came up with "Collateral Murder," with my approval. It literally means "unintentional murder."
>
> 4. Public Relations is an area WikiLeaks needed some desperate help in, since the only people who had heard of them before were people in the hacker, journalist, and intelligence communities.
>
> 5. Video personally pissed off Assange, and he wanted to "get out of exhile."

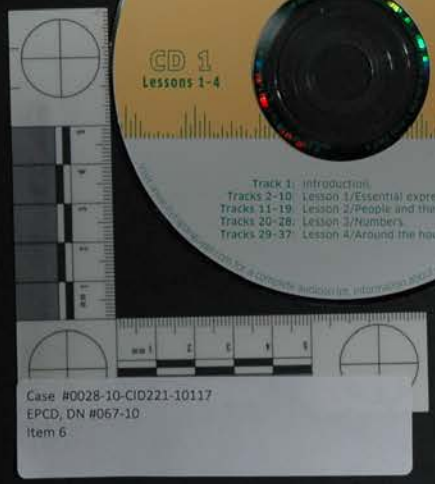

STARTING OUT IN
ARABIC
All the Arabic you need to get started in a simple audio-only program
3 Audio CDs
No books necessary!
LIVING LANGUAGE


12 JUL 07
CZ ENGAGEMENT
ZONE 30 GC
REUTERS
FOIA REQ
imation
CD-RW
700MB 80 min
This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.


STARTING OUT IN
ARABIC
CD 3
Lessons 9-10
Dialogues
LIVING LANGUAGE


STARTING OUT IN
ARABIC
CD 1
Lessons 1-4
LIVING LANGUAGE
Track 1: Introduction
Tracks 2-10: Lesson 1/Essential expressions
Tracks 11-19: Lesson 2/People and the family
Tracks 20-28: Lesson 3/Numbers
Tracks 29-37: Lesson 4/Around the house


STARTING OUT IN
ARABIC
CD 2
Lessons 5-9
LIVING LANGUAGE
Tracks 1-9: Lesson 5/Describing things
Tracks 10-18: Lesson 6/Around town
Tracks 19-27: Lesson 7/At a restaurant
Tracks 28-36: Lesson 8/Everyday life
Tracks 37-42: Lesson 9/At work
(One more time.)


Case #0028-10-CID221-10117
EPCD, DN #067-10
Item 6


0115 / 28MAY10 / FBI

PE 15

A NOTE ON SOURCES AND METHODS

Most of this book is based on events I personally observed between January 2007, when I first met the 2-16, and June 2008, the month of the Ranger Ball. I spent a total of eight months with the 2-16 in Iraq and made additional reporting trips to Fort Riley, in Kansas; Brooke Army Medical Center, in San Antonio, Texas; the National Naval Medical Center, in Bethesda, Maryland; and Walter Reed Army Medical Center, in Washington, D.C.

The book also contains some scenes for which I wasn't present. In those instances, the details, descriptions, and dialogue used in the book were verified through internal army reports, photographs, videos, after-the-fact observation, and interviews with as many participants as conditions would permit. All of the people described and quoted in the book knew that I was a journalist and that everything I was seeing and hearing was on the record.

It is to the army's credit, I believe, that during the length of my reporting, there were only two times that I was asked to treat something as off the record. Both requests involved classified technological applications in use by the soldiers, the revealing of which could conceivably put subsequent soldiers using the applications at increased risk, and I agreed to do so.

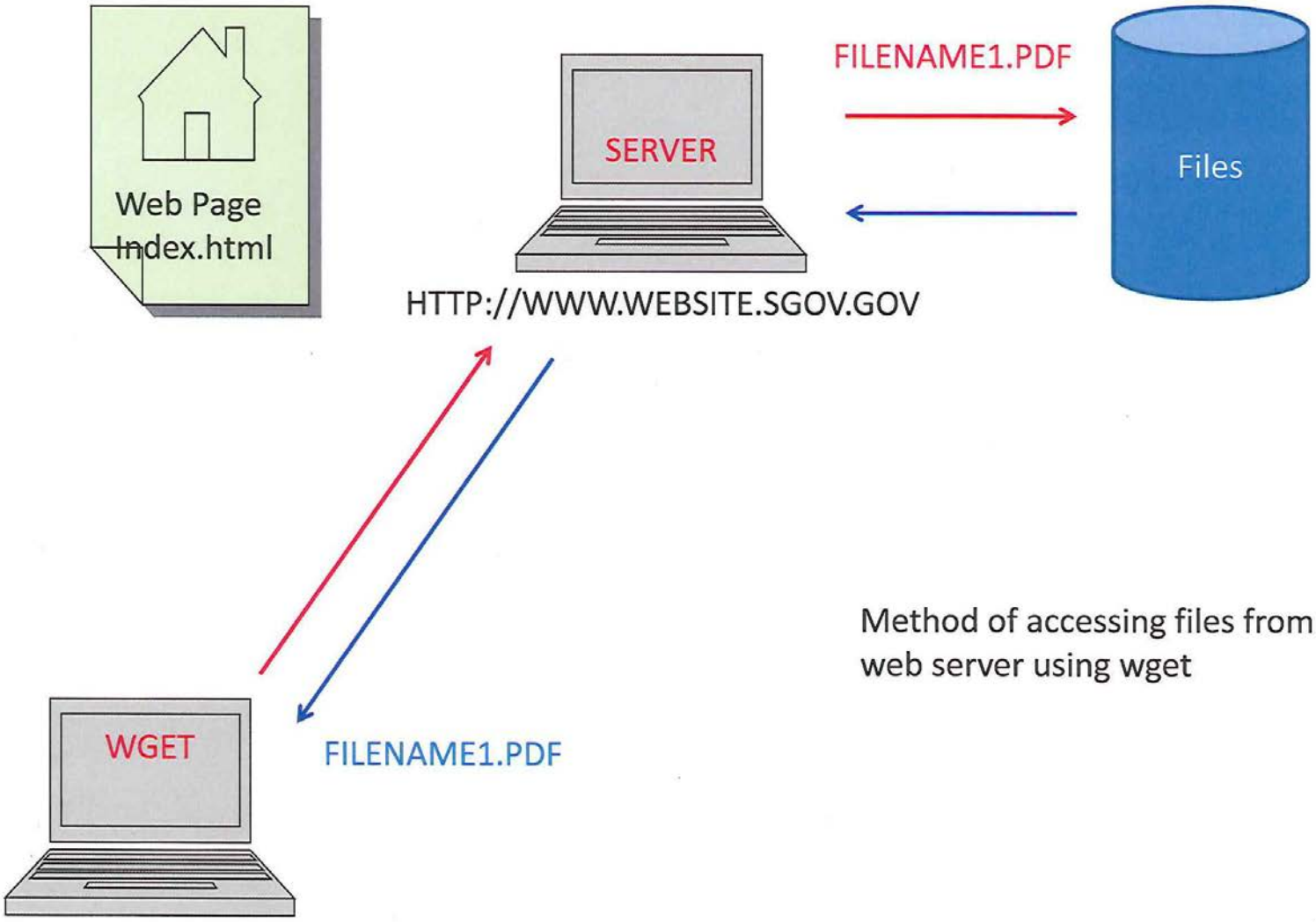
And it is to the 2-16 soldiers' credit that they tolerated a journalist being among them, and in almost all cases welcomed me with their trust. From the beginning, I explained to them that my intent was to document their corner of the war, without agenda. This book, then, is that corner, unshaded. I feel privileged to have been its witness, and to write the story of what happened.

```
                                    wget-help
GNU Wget 1.11.4, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version           display the version of Wget and exit.
  -h,  --help              print this help.
  -b,  --background        go to background after startup.
  -e,  --execute=COMMAND   execute a  .wgetrc'-style command.

Logging and input file:
  -o,  --output-file=FILE    log messages to FILE.
  -a,  --append-output=FILE  append messages to FILE.
  -d,  --debug               print lots of debugging information.
  -q,  --quiet               quiet (no output).
  -v,  --verbose             be verbose (this is the default).
  -nv, --no-verbose          turn off verboseness, without being quiet.
  -i,  --input-file=FILE     download URLs found in FILE.
  -F,  --force-html          treat input file as HTML.
  -B,  --base=URL            prepends URL to relative links in -F -i file.
```


Web Page
Index.html
SERVER
FILENAME1.PDF
Files
HTTP://WWW.WEBSITE.SGOV.GOV
WGET
FILENAME1.PDF
Method of accessing files from a web server using wget
2

WikiLeaks

@wikileaks

Follow

We would like a list of as many .mil email addresses as possible. Please contact editor@wikileaks.org or submit

Reply Retweet Favorite More

37 RETWEETS **9** FAVORITES

2:37 PM - 7 May 10

Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First [redacted]
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First [redacted]
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First [redacted]
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First [redacted]
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=(b) (6) [redacted]
/o=2BCT10MTN/ou=First [redacted]

PE 148b

[redacted], John MSG MNF-I EOD
[redacted], Christopher SPC 1AAB S2 ANALYST
[redacted], Rayn R MAJ BUCCA JIDC OIC
[redacted], Guy D 1SG 155th ICTC
[redacted], Ryan E SSG 306th MP BN
[redacted], John W SPC 328th MP CO Sallyport
[redacted], Lena C IT1 SOFTLEIZ NCOIC
[redacted], Michael W SPC 4/2 HHC S6
[redacted], Shawn H SPC MNC-I 86 CSH Light Wheeled Mech
[redacted], Tasha R SSG Mission CDR
[redacted], Tracy H SGT PLL Clerk
[redacted], Zachary J PFC C 114th IN SDC Guard
[redacted], Jessica L SGT 259th CSSB HR SPEC
[redacted], Thomas J. A1C USAF 532 ESFS Security Force USA
[redacted], Muhammad SGT 702d BSB SPO Mortuary Affairs
[redacted], Ryan V, CPO,NPDB-5
[redacted], Olasunkanmi SPC G1 USD-C, B CO G-1 Strength Clerk

PE 147b

Full Path \1 Customer\Unallocated Clusters
File Offset 66637168640

TASK: Acquire and exfiltrate Global Address List from United States Forces - Iraq (USF-I) Microsoft Outlook / Sharepoint Exchange server

PURPOSE: To e-mail classified messages from USF-I's CIDNE event log from 2004 to 2009.

METHOD: Acquire document

ENDSTATE:

TARGET: United States Forces - Iraq (USF-I) Outlook / Sharepoint Exchange Server

OBJECTIVE: