THE OFFICE OF SECURITY

Operations Security (OPSEC)

GOOD SECURITY IS A GROUP EFFORT

Operations Security (OPSEC)

"Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."

— George Washington, known OPSEC practitioner

Why OPSEC ?

- Our enemy took us by surprise 11 September, 2001 and we will never be the same country again. In order to effectively bring the enemy to justice, we need to maintain the element of surprise. Every element of our operation is more sensitive than ever before. We must rededicate ourselves to our mission and our country to help ensure that what transpired on September 11th will not be repeated. Security must be incorporated into every aspect of our jobs. If we are not vigilant in protecting critical information, it will happen again. The future of America depends on changing the way we look at security. OPSEC can make the difference. It is absolutely essential that we understand and incorporate it into everything we do, personally as well as professionally.

What Is OPSEC?

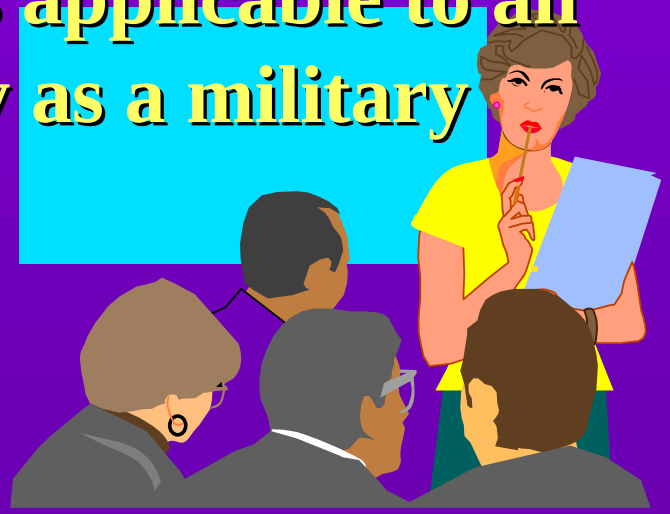
- OPSEC Defined
- The OPSEC Process
  - Critical Information
  - Indicators
  - Adversaries
  - Vulnerabilities
  - Protective Measures

OPSEC at Home

- You have probably been practicing OPSEC in your personal life without knowing it! When you are getting ready to go on a trip have you ever:
- Stopped the delivery of the newspaper so that they would not pile up outside?
- Asked your neighbor to pick up your mail so the mailbox would not fill up?
- Connected your porch lights and inside lights to a timer so they would go on at preset times?
- Connected a radio to a timer so that it comes on at various times?

What Is OPSEC?

A process to deny potential adversaries information about capabilities and/or intentions by identifying, controlling, and protecting unclassified information that gives evidence of the planning and execution of sensitive activities. It is just as applicable to an administrative or R&D facility as a military operation.



OPSEC

A Process With Five Components

Identify *YOUR* Critical Information

Analyze *YOUR* Threat

Analyze *YOUR* Vulnerabilities

Assess *YOUR* Risk

Employ *appropriate* Protective Measures

Critical Information

Critical information is the core secrets of an activity, capability, or intention that if known to the adversary, could weaken or defeat the operation.

Critical Information

- Critical information is the information about your operations an adversary needs to achieve their goals.
- Critical information usually involves only a few key items.
- If those items are unavailable to us they could impact the way we conduct business.
- Our critical information is information required to be successful in our jobs.

Critical Information

Our adversaries may want to harm personnel and/or damage property and resources

Critical Information could relate to:

Employees' Safety (911)
Fleet of ships and aircraft (USS Cole)
Facilities Design (Oklahoma City)
Security Vulnerabilities (Anthrax Mailings)
Satellite Data (Weather, Environmental)
Law Enforcement Activities (Fisheries)
Management Decisions (All levels)

Indicators

- Information may be collected by monitoring telephone and public conversations, analyzing telephone directories, financial or purchasing documents, position or "job" announcements, travel documents, blueprints or drawings, distribution lists, shipping and receiving documents, even personal information or items found in the trash.

Need-to-know

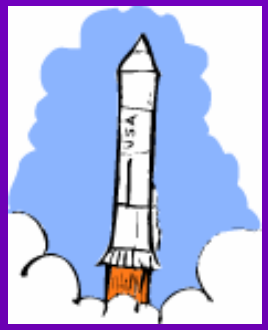
Our adversary's makeup has changed, but the need to know and understand your *Critical Information* is still the means for their success.

If you don't protect it, then prepare to lose it!

Adversary

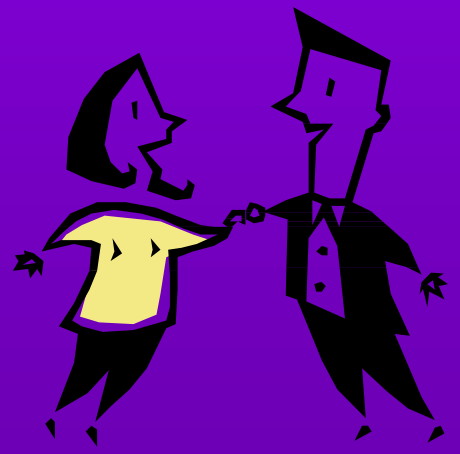
- Who are we talking about? In the Cold War days you knew it was the communist threat. Today, the Cold War is over but new threats have emerged.

- Economic superiority and political gain are other driving forces. Our former allies during the Cold War and Desert Storm are now collecting technology from us to gain an advantage in the global market.



Terrorist

- Terrorism has recently become the most significant threat to our way of life.



Terrorist

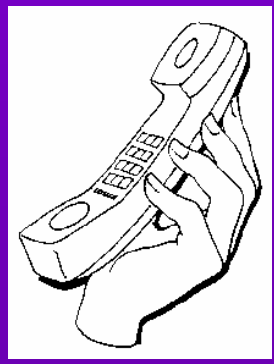
- Media reports indicate some terrorist training schools ran curricula which included irregular naval warfare techniques such as Ship Mining, Sabotage and Civil Aviation Terrorism. Another school ran programs dedicated to espionage and counter-espionage techniques which helped “graduates” run clandestine terrorist networks overseas.

Terrorist

- Those selected to become top-level terrorists received training in Foreign Languages, Principles of Espionage and Counter-intelligence as well as Code Making and Deciphering.

Political/Economic Competition

- Remember that there are other adversaries - foreign intelligence services continue to collect information on us that could be used against us in the future. It is a certainty that our adversaries will continually look for and find any weak links.

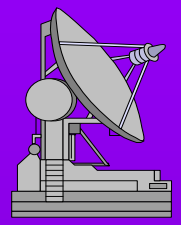


Political/Economic Competition

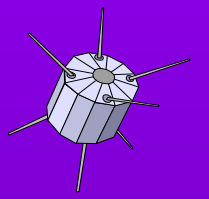
- Economic superiority is another driving force. Although not as lethal as terrorism it still impacts our way of life. Our former allies during the Cold War and Desert Storm are now making efforts to acquire our technology at minimal costs to gain an advantage in the global market

Information Collection

Signals Intelligence (SIGINT)



Imagery Intelligence (IMINT)



Human Intelligence (HUMINT)

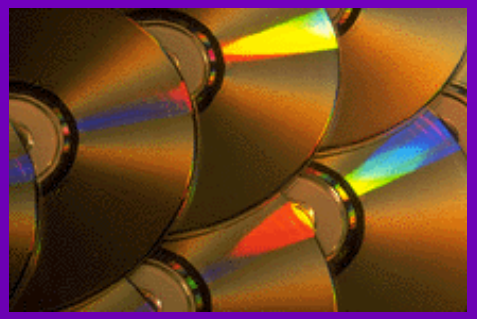
Open Source Intelligence (OSINT)

Traditional Collection

- **SIGINT: Signals Intelligence is the interception of Electro -magnetic signals from telephones, faxes, computers, radios, and/or anything else transmitted in the open.**
- **IMINT: Photographic imagery includes overhead photography by satellite or any other means including individuals with cameras.**
- **HUMINT: Traditional spy. Least likely means!**

Open Source Intelligence

- **OSINT:** In the world of secret services, Open Source Intelligence (OSINT) means useful information gleaned from public sources, such as scientific articles, newspapers, phone books and price lists.



Open Source Intelligence

- Open source intelligence includes internet probes which are very effective. Adversaries are not the only ones interested in our e-mail. Sailors aboard USS *Cole* were shocked to find out that the personal e-mail messages they sent home to family and friends were forwarded to the media to be used as quoted material in news stories without their permission.

Vulnerabilities

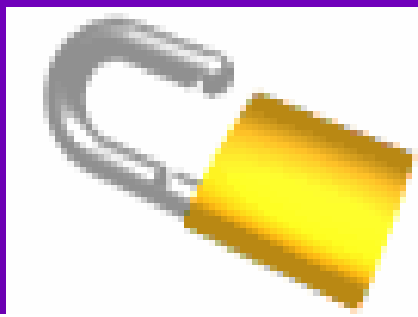
- **Vulnerabilities are defined as the characteristics of a system which can cause it to suffer degradation as a result of having been subjected to some level of a hostile threat.**

Vulnerabilities

- Determining our vulnerabilities involves analyzing how we conduct operations. We must look at ourselves as the adversary would.
- From this perspective we can determine what are the true, rather than the hypothetical, vulnerabilities.

Protective Measures

- Vulnerabilities and specific threats must be matched. Where the vulnerabilities are great and the threat is evident, the risk of exploitation should be expected. A high priority for protection should be assigned and corrective action taken. Where the vulnerability is slight and the adversary has a marginal collection capability, the priority should be lower.



Countermeasures

- Countermeasures need to be developed that eliminate the vulnerabilities, threats, or utility of the information to the adversaries. The possible countermeasures should include alternatives that may vary in effectiveness, feasibility and cost.

Countermeasures

- Countermeasures may include anything that is likely to work in a particular situation. The decision of whether to implement countermeasures must be based on cost/benefit analysis and an evaluation of the overall program objectives.

The Threat Is REAL!

- Protect our technological advantage
- Asymmetric Threats (threats from nontraditional and/or unknown origin) are today's concern and not always clearly evident
- Practice common sense and include OPSEC in your daily routines

The Bottom Line

The adversary is watching!

Are you?