Operations Security (OPSEC)

NOST-USOPSEC-3.0

18 MAR 2020

(Materials reproduced from TWMS)

Operations Security (OPSEC) Annual Training

2019

Developed by: The Naval OPSEC Support Team

References

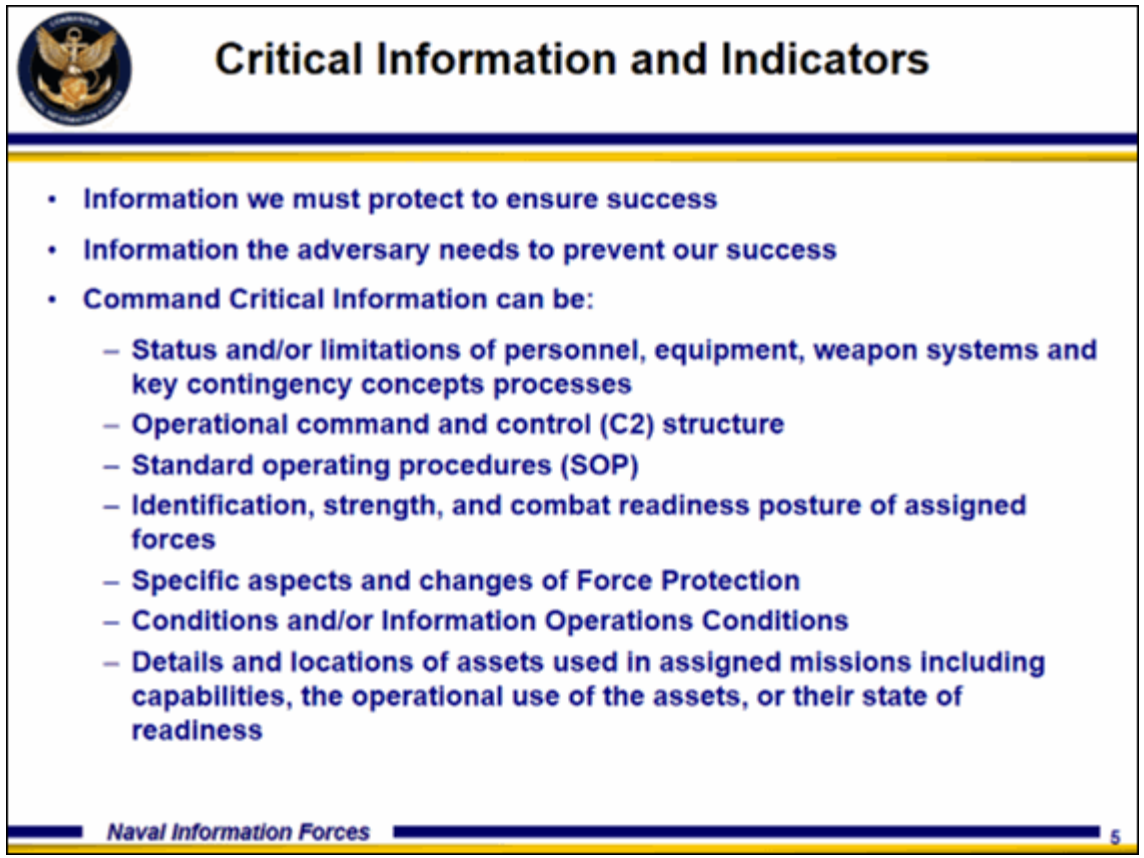
- Department of Defense Directive (DoDD 5205.02(series))
- Secretary of the Navy Instruction (SECNAVINST 3070.2A)
- Chief of Naval Operations (OPNAVINST 3432.1(series))
- Navy Tactics, Techniques and Procedures (NTTP 3-13.3M)
- Local command policy

Learning Objectives

- Upon completion of this training, you will better understand:
- The definition of OPSEC
- The five step process
- Roles and responsibilities of:
  - Command Leadership
  - Public Affairs
  - Acquisitions/Supply
  - Planners
  - Program Managers

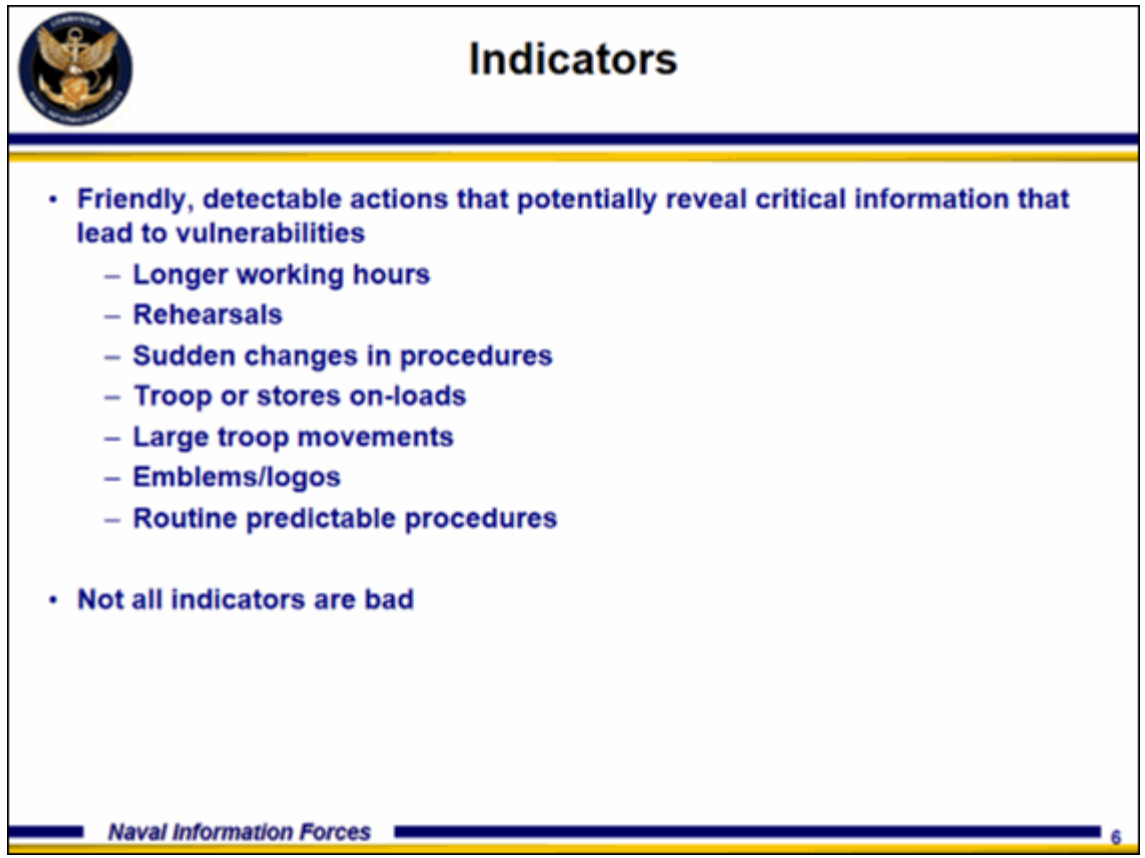
Operations Security

- Operations Security (OPSEC) is a process that identifies unclassified critical information (CI) and indicators, analyzes potential threats and vulnerabilities, assesses risks and develops countermeasures to safeguard critical information.
- OPSEC is one of several Information Related Capabilities (IRC)
- Operations depend on successfully implementing the OPSEC five step process.
- The five steps:
  - Identify critical information
  - Analyze threat
  - Analyze vulnerabilities
  - Assess risk
  - Apply countermeasures



Critical information: Specific facts about friendly (U.S.) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for accomplishment of friendly objectives.

These are examples of what critical information could be. Discuss how this information can be critical. What can happen if the adversary were to gain knowledge of this information? Can you think of any other information that might be critical?

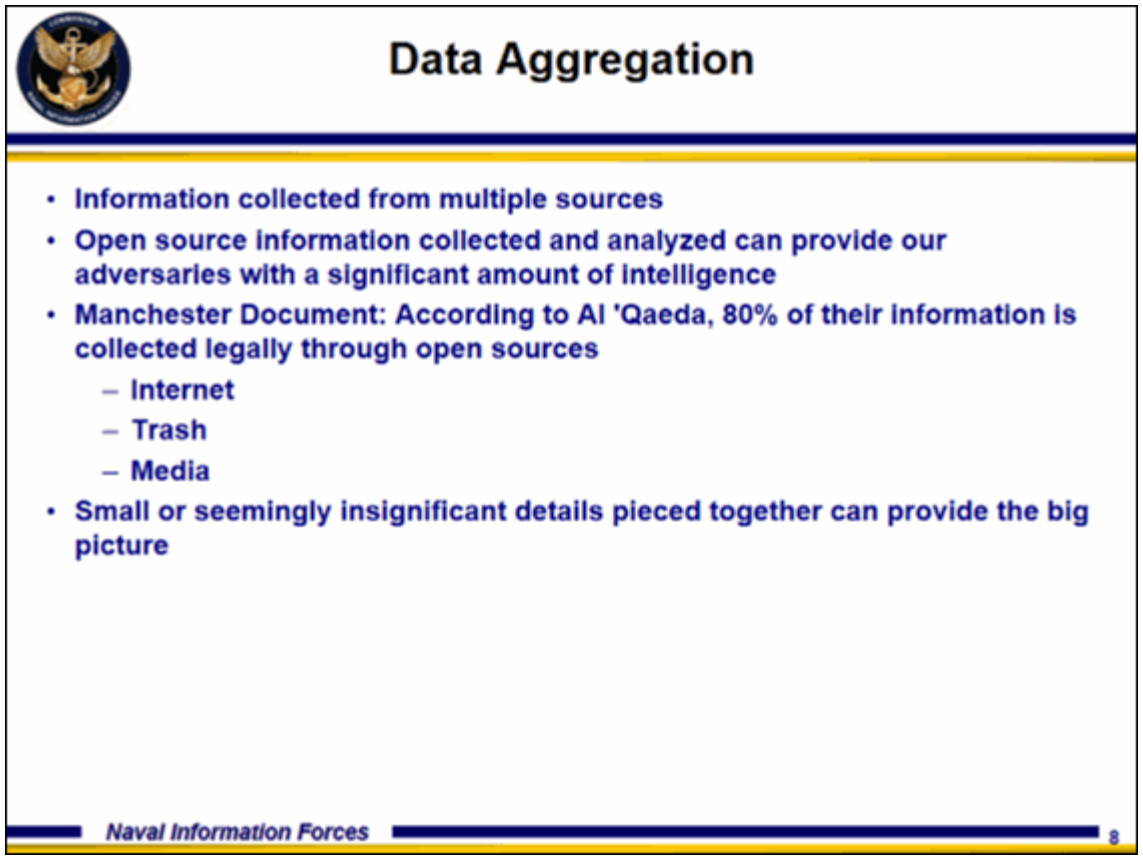


Indicators are friendly detectable actions that reveal critical information, which then leads to vulnerabilities. Discuss how these things can be an indicator. What could they mean? For example, let's say that your unit was all of a sudden working until the middle of the night. What could that possibly mean? Would an adversary want to investigate this further? For example, huge stores on-loads on a pier could indicate a ship getting underway for a major deployment.

Not all indicators are bad. That ADT sign in the front yard indicates a house that is alarmed, whether or not it even works. That one indicator could potentially keep a thief (adversary) from hitting your home.

Discuss what could be good indicators in the military. A large security presence with heavy weapons could indicate that they are guarding something or someone important. The weapons could possibly keep the adversary from trying to access that area.

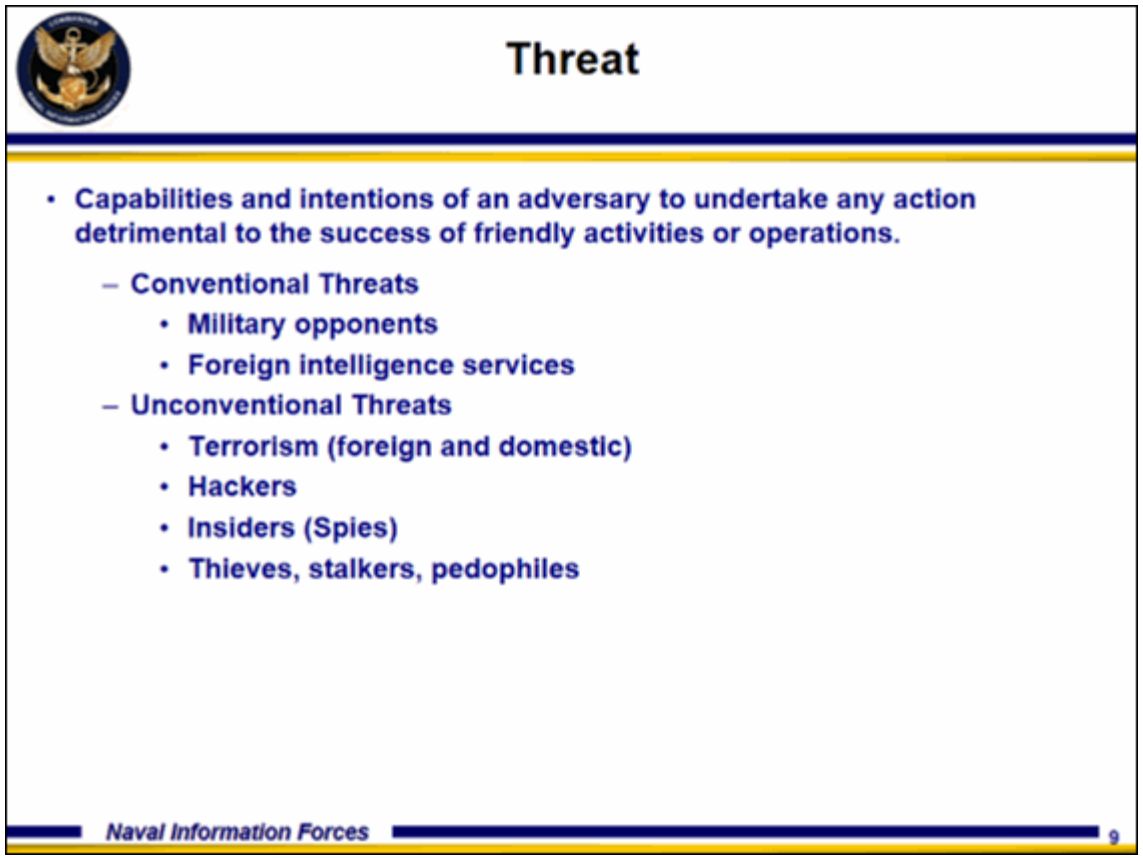
Not all indicators can be eliminated or controlled but can still convey information to our adversaries if they are watching. For example, an onload aboard an amphibious ship….coupled with an onload of Harpoon missiles aboard a cruiser and ……the onload of Marines aboard the same amphib would indicate an Amphibious Readiness Group (ARG) will get underway.



Data aggregation – information collection from multiple sources. Each piece of information collected might seem innocent and worthless by itself. If enough pieces of relevant information are collected, the big picture can be revealed. Sometimes, data aggregation can even lead to classified information.

Many do not understand how easy it is to aggregate information on the internet. For information that is already made public, there is no reason to verify the information by posting additional details about missions or personal information.

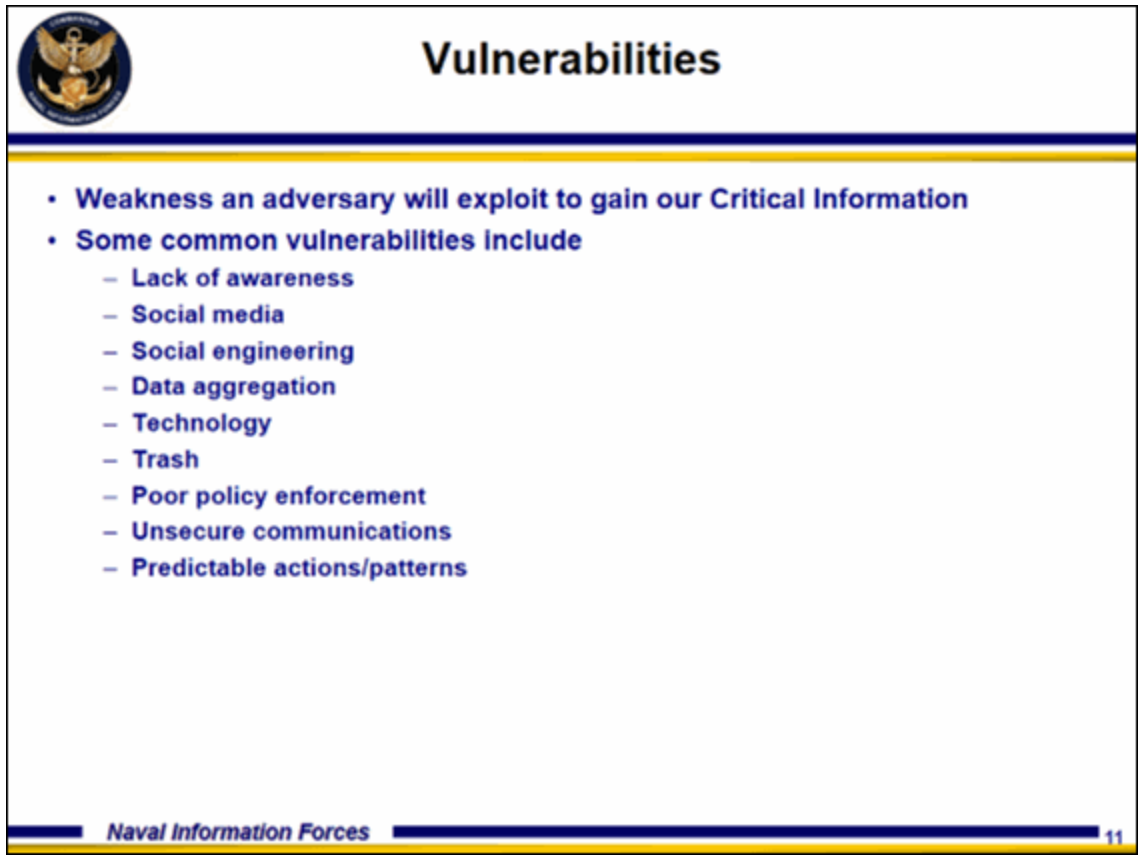
The Manchester Document was an al Qaeda handbook on how they conduct operations. It was found in Manchester, England in 2000. In the handbook, it said that 80% of the information they collect is open source information, which means that they collected it through legal means, most of it done on the internet. Now, it is estimated that that number is over 90%. Why the change? Where are they getting information now that they couldn't back then? The answer is social media. Our adversaries use social media a lot for information collection and recruiting, and are very successful at it.



Of conventional and unconventional, which are main types of threats we are dealing with today? The answer is definitely unconventional. The main threat in the United States right now is foreign intelligence services (spies trying to gather information). They are very active, especially in the DC metro area and near military bases. Why are they targeting these places?

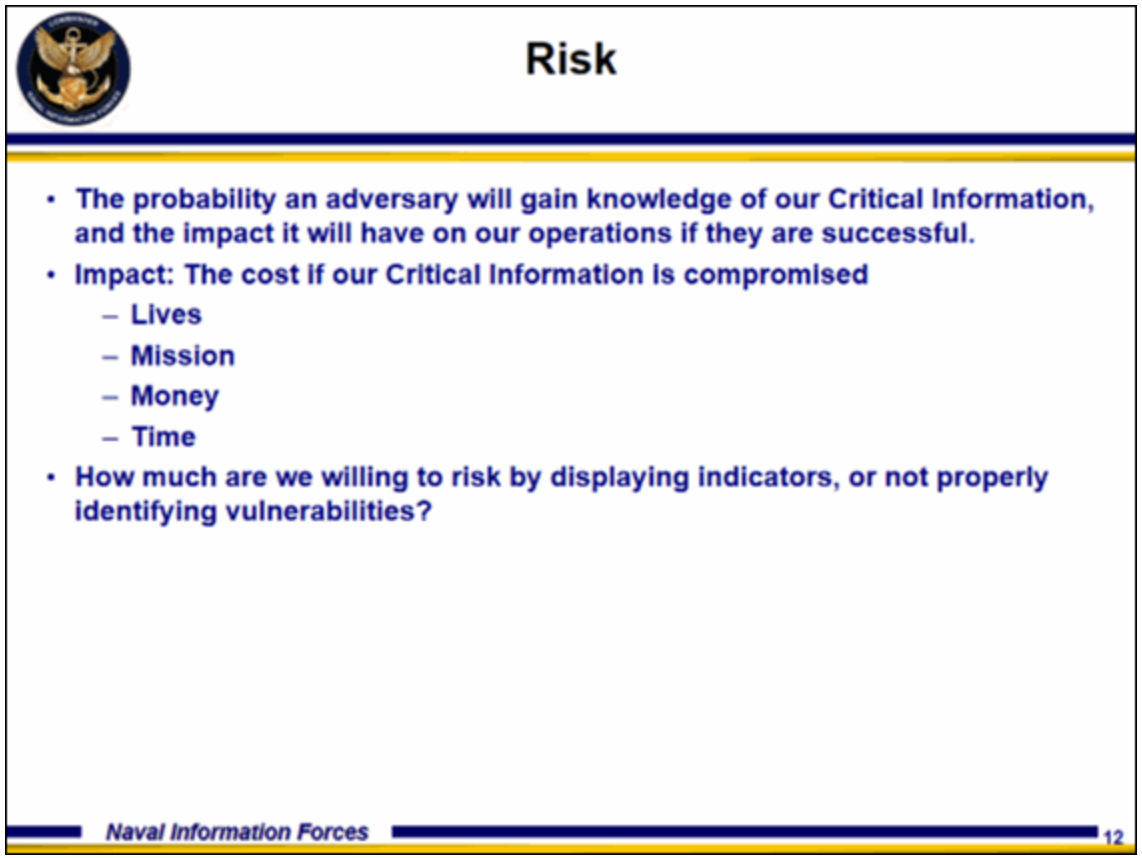
Threat information can be obtained from either a command's S2/N2 shop or any local NCIS area office. Much of what NCIS provides in the US is available from the NCIS MTAC site or other on line sites.

Why is this information important? Discuss why the adversary would want to know these things. How could they use this information to their advantage?



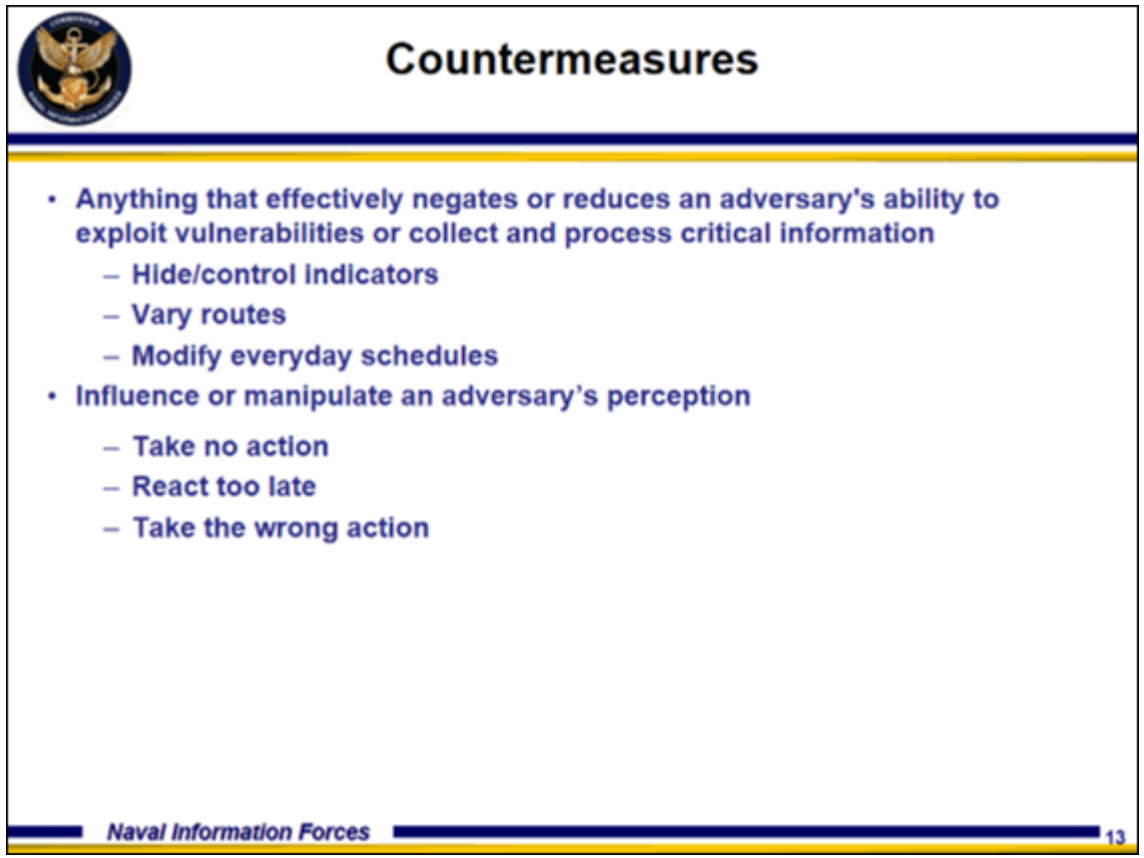
Vulnerability: A weakness the adversary can exploit to get critical information. A vulnerability is anything that makes your critical information susceptible to intelligence collection. Discuss how these things are vulnerabilities.

- Lack of awareness. Many just are not aware of the vulnerabilities when posting information
- Social media. There are billions of users, and none of the sites are 100 percent secure. Essentially, you could be posting information to billions
- Social engineering. We are naturally friendly and like to talk about our work or personal experiences. Don't share this information with strangers, regardless of home harmless they may seem.
- Understand the aggregation issues and how the internet/world wide web makes it easy
- Technology. For every new gadget that's developed, you can be sure there is a vulnerability associated with it.
- Trash. Be sure to shred/burn all personal of official correspondence, to include junk mail
- Poor policy enforcement. Policies are only as good as how they are enforced. An all shred policy is great as long as everyone participates. No cell phone policy in the spaces for security purposes must be enforced.
- Many people think cell phones are secure. Most methods of communications used today are not secure
- Don't be predictable.



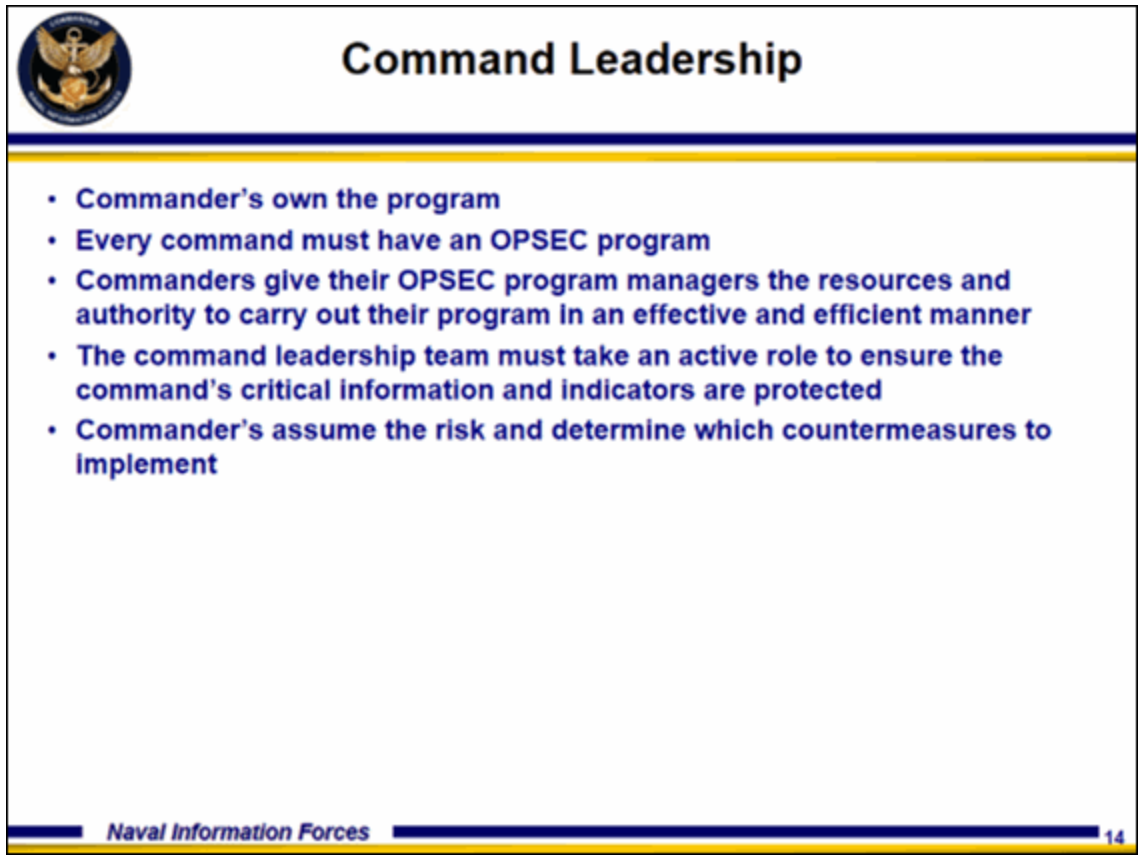
Risk is the probability an adversary will gain knowledge of your critical information and the impact it will have on your mission if they are successful. When assessing risk, you must think about how it could impact the lives of personnel, the mission, how much the organizations stands to lose in money, and time lost as a result of the mission being impacted.

Commanders have to decide what level of risk they are willing to accept if their critical information is exploited and acted upon.

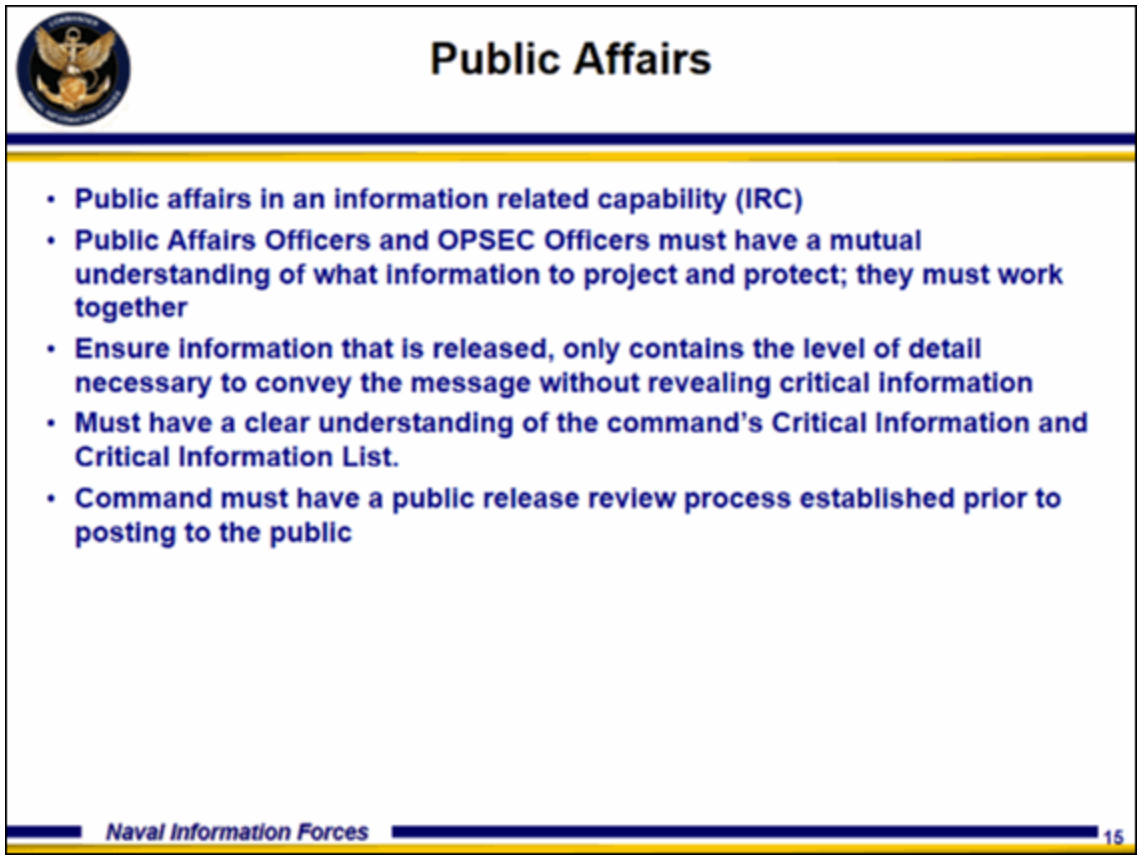


Think back to vulnerabilities. Look at lack of awareness. How can you make that not a vulnerability? You can provide training so personnel now understand what information to protect and how to protect it.

What about the rest of the vulnerabilities? Discuss what some possible countermeasures could be for them.

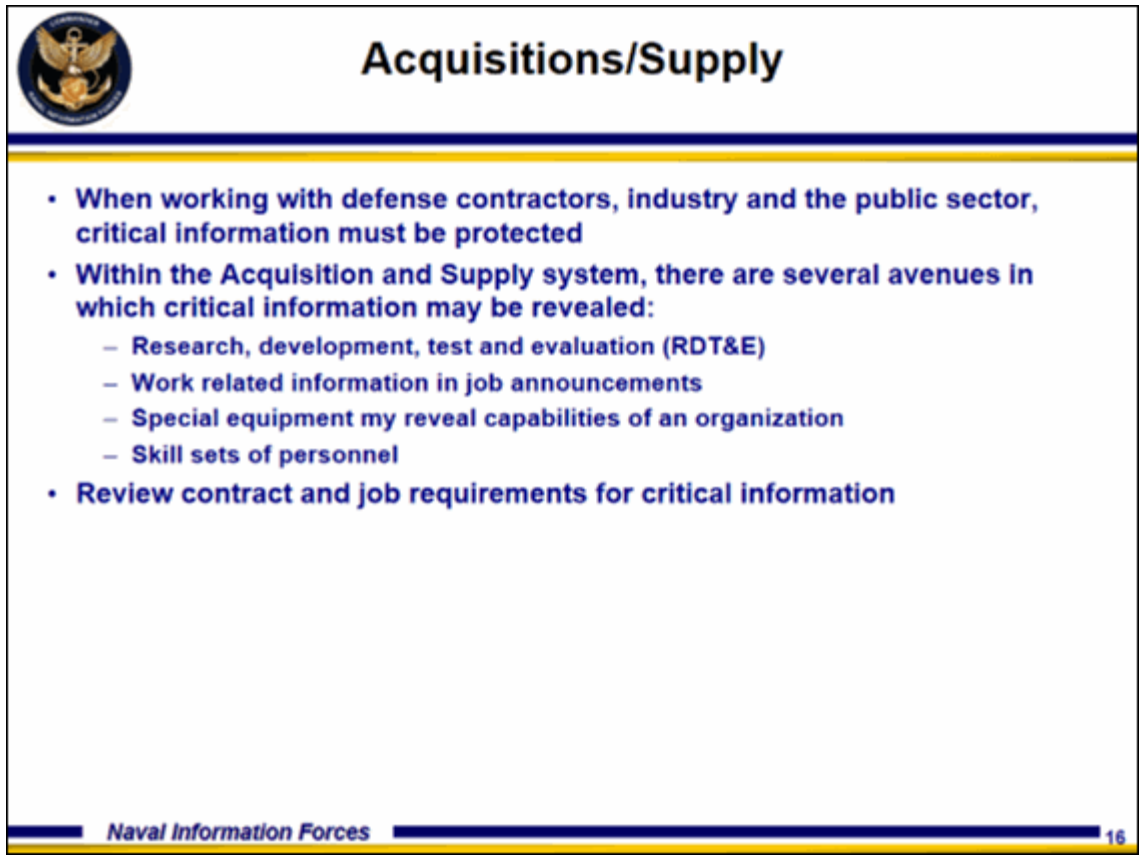


Why is the OPSEC program useless without CO's support? If the CO doesn't care, then nobody will.



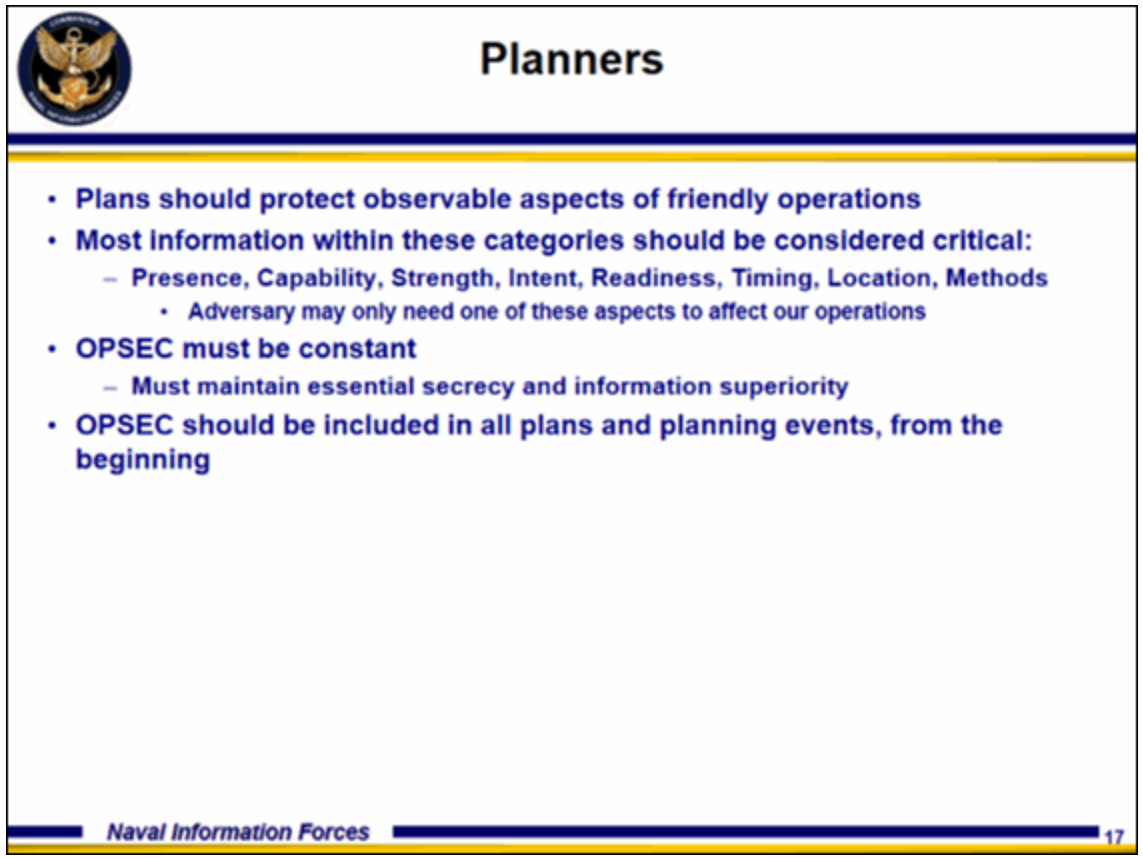
Why do public affairs and OPSEC need to have a relationship? Public affairs is trying to release information to the public. OPSEC is trying to control the information as much as possible. To ensure that public affairs does not inadvertently release any critical information, they need to know what that information is. It goes back to lack of awareness as a vulnerability. If public affairs does not know that certain pieces of information are not allowed to be released, then they very well may release that information.

Public release review process – Before information is released to the public, it should go through at least the OPSEC officer to make sure that no critical information is being released, the public affairs officer to make sure that everything is acceptable, and hopefully the CO/XO/SEL to make sure that the information being released is accurate and that is the message the command is trying to convey.



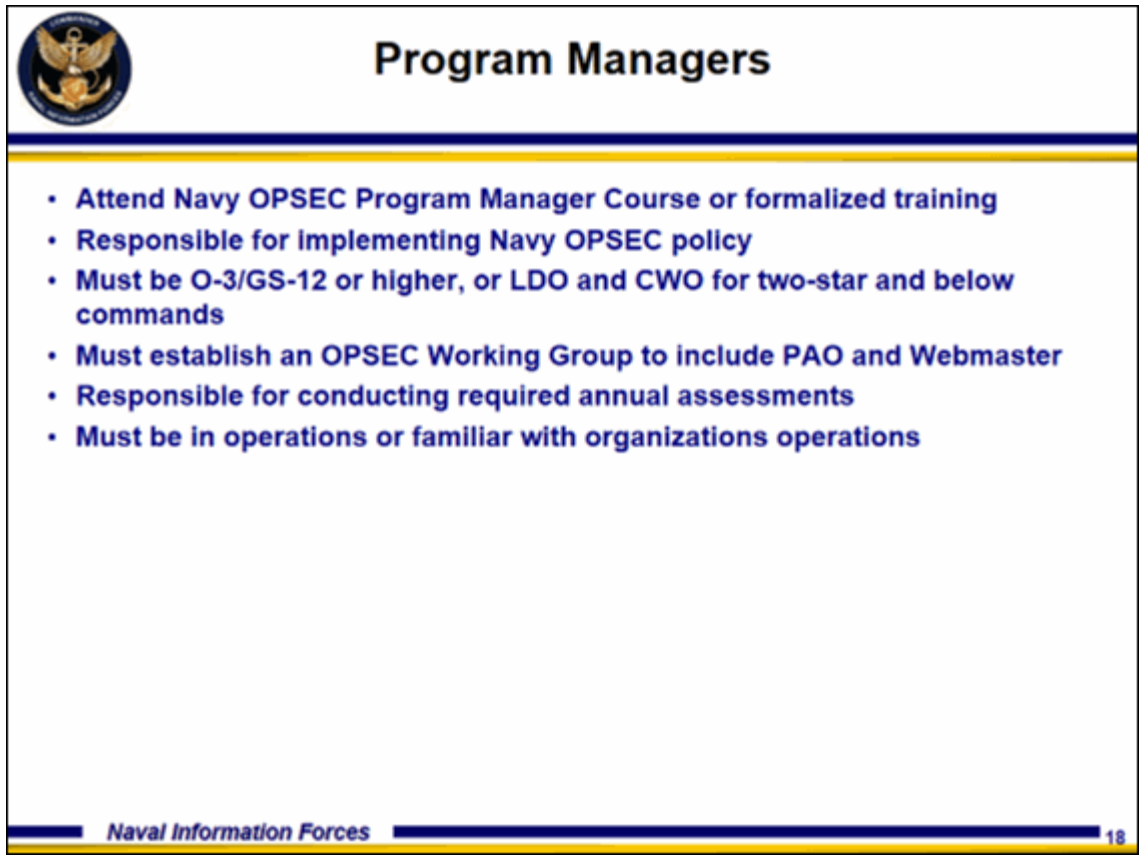
Research and development, testing, evaluation, contracting, acquisitions, and hiring processes - all require significant interaction with industry partners.

For example, a ship is pulling into a foreign port. The port employees need to know well in advance that a ship is coming so they are able to make all of the necessary preparations. Do you know who the port employees are talking to? Of course not. That is a risk that the Navy is willing to take when it comes to port visits.



Observable aspects of friendly operations: presence, capability, strength, intent, readiness, timing, location, methods. If an adversary were to discover what method an adversary is using (amphibious, land invasion, etc.), then that would definitely give them the upper hand on the ensuing operation.

OPSEC needs to be in all of the planning meetings from the very beginning. You can't go in at the very end and put an OPSEC spin on the operation.



A working group consists of a representative from each department at the command. This ensures that the command's CIL is thorough, and that the entire command understands OPSEC.

The CIL should be a part of the command instruction so the CO does not have to sign several different OPSEC documents. When the CO approves the instruction, he also approves the CIL.

Questions

OPSEC@Navy.mil
757-203-3656
opsec@navy.mil
Naval Information Forces
115 Lake View Drive
Suffolk, VA 23435

www.navy.mil/OPSEC
Naval OPSEC App

Youtube.com/USNOPSEC

Congratulations!

You have completed this course.

You must continue to the next page to record your training as complete and to view or print your certificate.