



The Library of Sparta

*David Raymond
Greg Conti
Tom Cross*

Disclaimer

The views expressed in this talk are those of the authors and do not reflect the official policy or position of Lancope, West Point, the Department of the Army, the Department of Defense, or the United States Government.

Our Background...



David Raymond
West Point

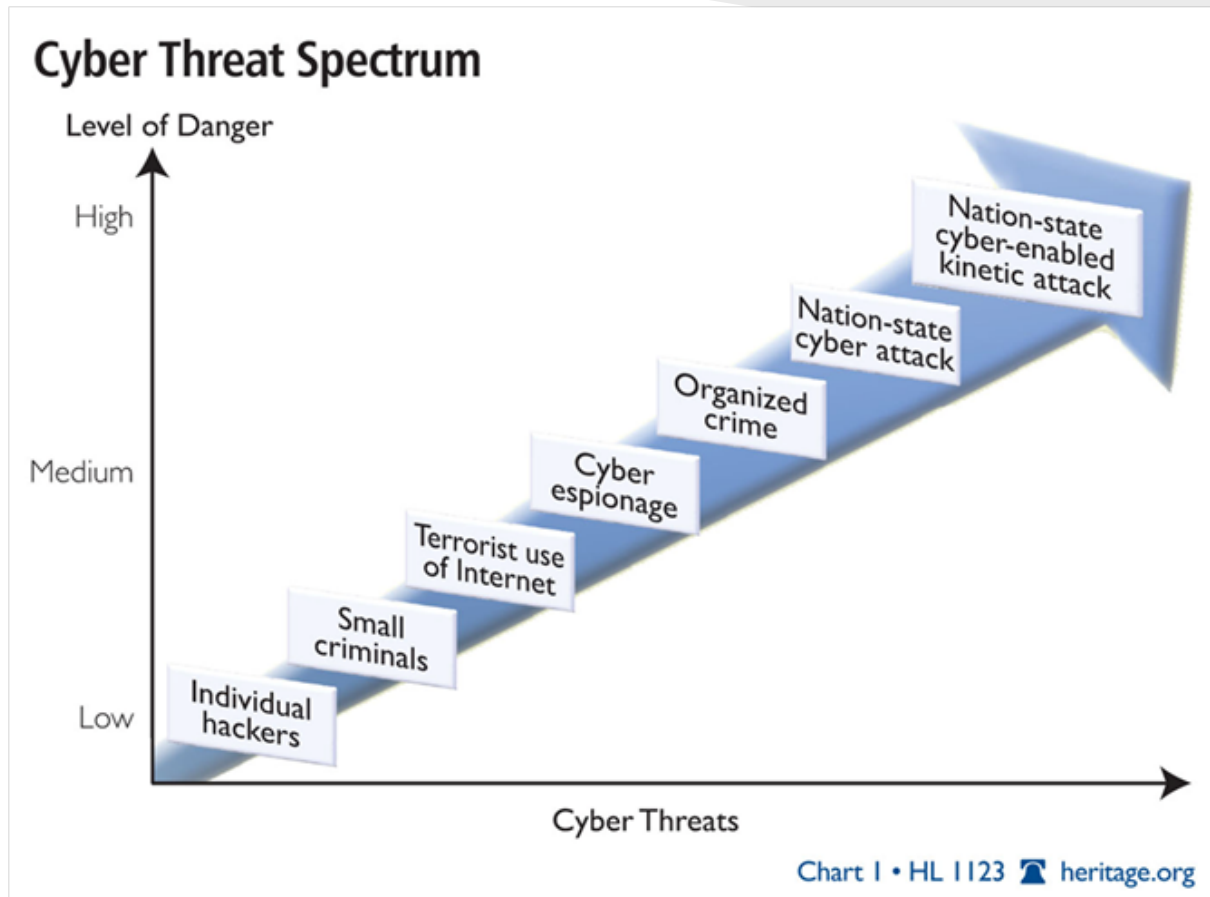


Greg Conti
West Point



Tom Cross
Lancoppe

Why, So What, and Who Cares...



You used to be fighting individuals . . .

now you are defending yourselves against nation-states

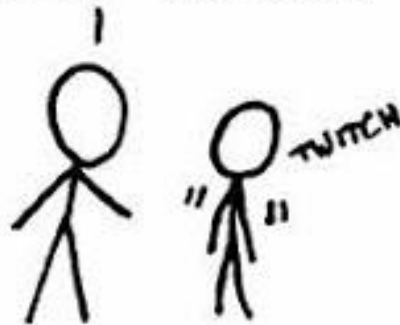
On the Internet, the offense
has all the cards



Also...

THE BEST PART OF GETTING
OLDER IS GONNA BE
INTENTIONALLY MISUSING SLANG
AROUND TEENAGERS JUST
TO WATCH THEM SQUIRM.

OH MAN, THAT SONG
IS SO PWNED!



What We AREN'T Covering

- Not another intelligence-based network defense talk
- Not a step-by-step guide
- ***No easy answers*** - it requires you to do some reading and research
- No APT (or other amorphous concepts)

What is Doctrine?

A Sacred Text For Some



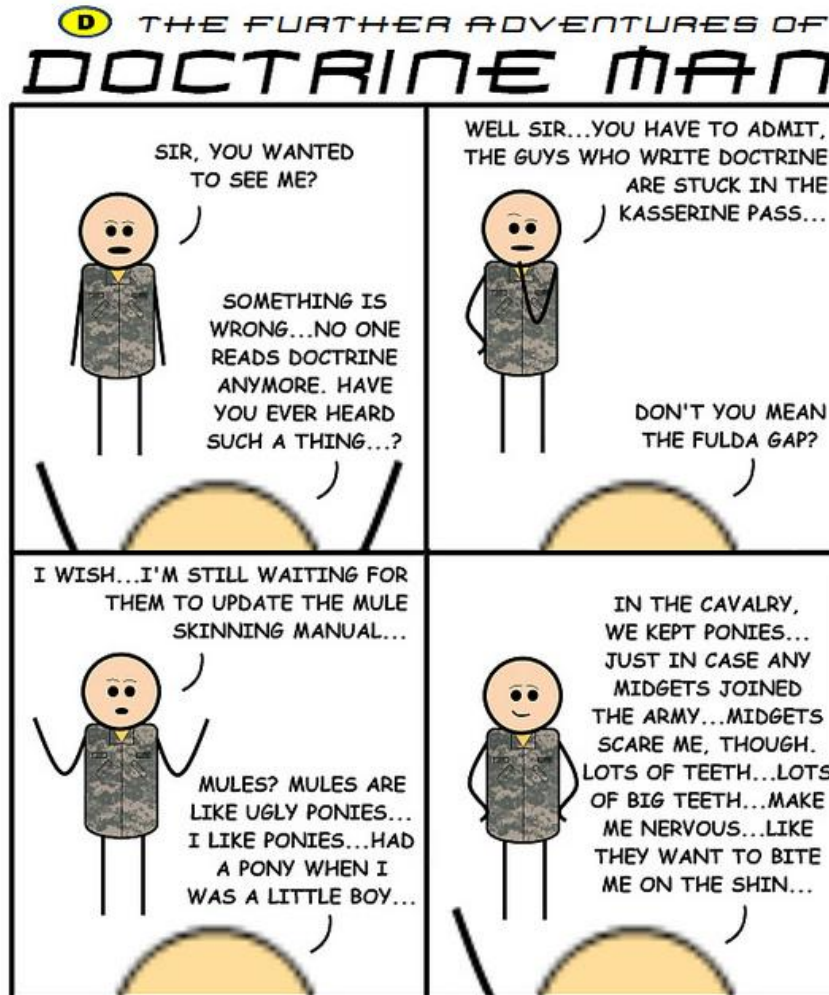
An Anathema to Others

“The most difficult thing about planning against the Americans, is that they do not read their own doctrine, and they would feel no particular obligation to follow it if they did.”

Admiral Sergey Gorshkov

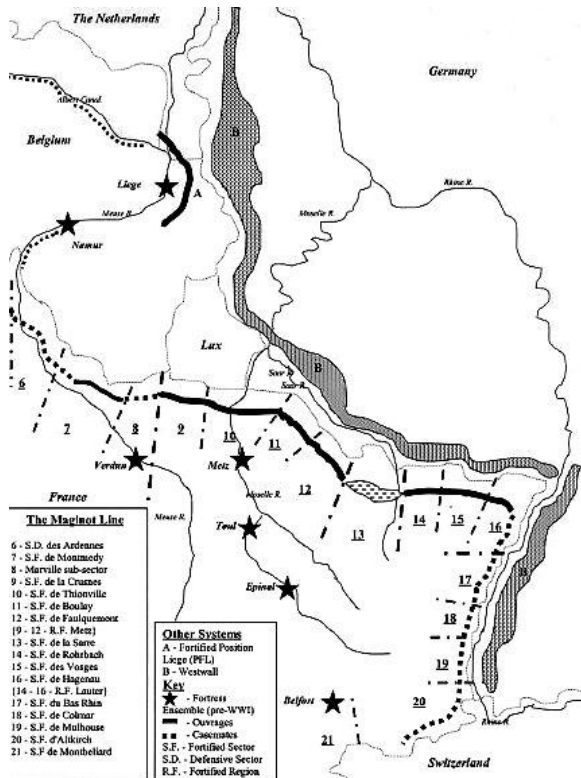
Commander, Soviet Naval Forces, 1956 - 1985

And then there is Doctrine Man...



The Answer is Somewhere in the Middle


https://en.wikipedia.org/wiki/Maginot_Line#mediaviewer/File:Maginot_Line_Karte.jpg



Bad Doctrine

Good Doctrine

Sources of Military Thought



SMALL WARS
JOURNAL

HOME JOURNAL SWJ BLOG EL CENTRO LIBRARY COUNCIL ABOUT

Small wars are operations undertaken under executive authority, wherein military force is combined with diplomatic pressure in the internal or external affairs of another state whose government is unstable, inadequate, or unsatisfactory for the preservation of life and of such interests as are determined by the foreign policy of our Nation.

-- *Small Wars Manual*, 1940

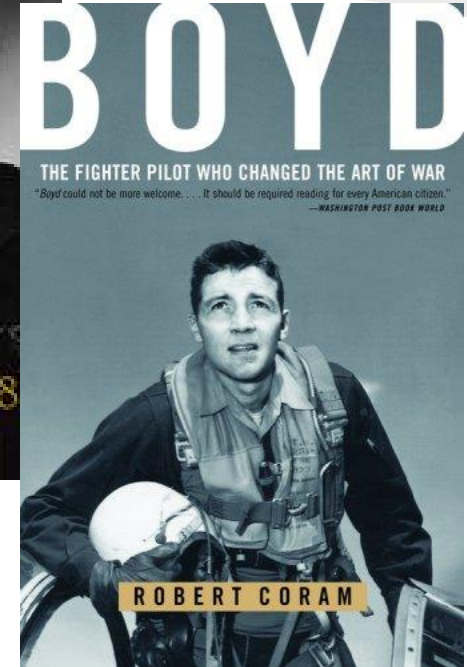
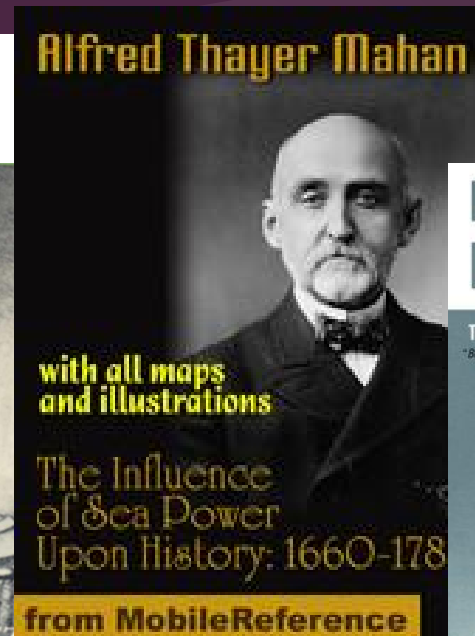
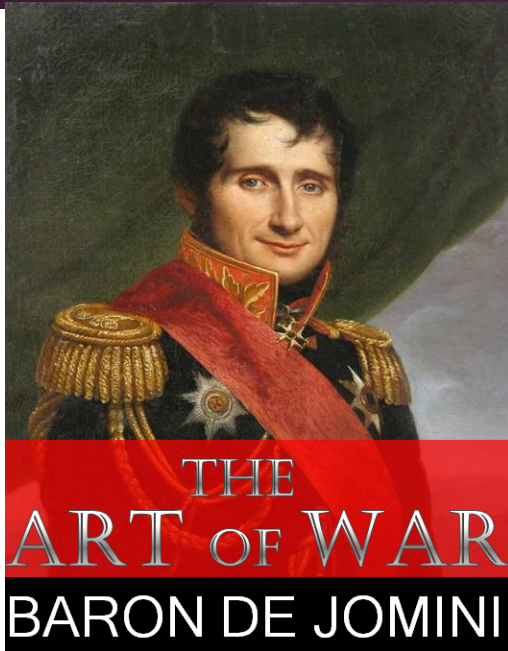
Welcome. *Small Wars Journal* publishes contributed work from across the spectrum of stakeholders in small wars. We look for articles from serious, authentic voices that add richness, breadth and depth to the dialog that too often occurs in cloistered venues. We do not screen articles for conformance with a house view; our only position is that small wars are wicked problems warranting consideration of myriad views before action, to inform what will no doubt be imperfect decisions with significant unintended consequences. On the continuum from paralysis by analysis, to informed action with recognition & maybe mitigation of cascading effects, to bold & ignorant decisiveness, we strive to help our readers find the middle ground.

Our content is generally available to any internet user. You need an *SWJ Username* to comment. **Register** or **Login**, it is free and easy. Please note that our discussion board, **Small Wars Council**, uses a separate *Council Username* – [more about that here](#).

JOURNAL	SWJ BLOG
Fighting Fire with Fire by Nathan A. Jennings June 22, 2014 11:34 PM Comments (0) Fighting Fire with Fire: Texas Rangers and Counterinsurgency in the 1847 Mexico City Campaign	23 June SWJ Roundup by SWJ Editors June 22, 2014 11:05 PM Comments (0) Continue on for today's SWJ news and opinion roundup.
Services No Longer Required? Challenges to the State as Primary Security Provider in the Age of Digital Fabrication by Clint Arizmendi, Ben Pronk and Jacob Choi June 22, 2014 11:10 PM Comments (0)	Nigeria Military Studies Sri Lankan Tactics for Use Against Boko Haram by SWJ Editors June 22, 2014 07:51 PM Comments (4) "Nigeria is studying the military tactics used by Sri Lanka to crush the rebel Tamil Tigers for its own battle against

- Classics / Classical Thinkers
- Doctrinal Manuals
- Military Writing
 - Military Journals
 - Small Wars Journal
 - Parameters
 - Military Review
 - SIGNAL
 - ... many more
- Policies

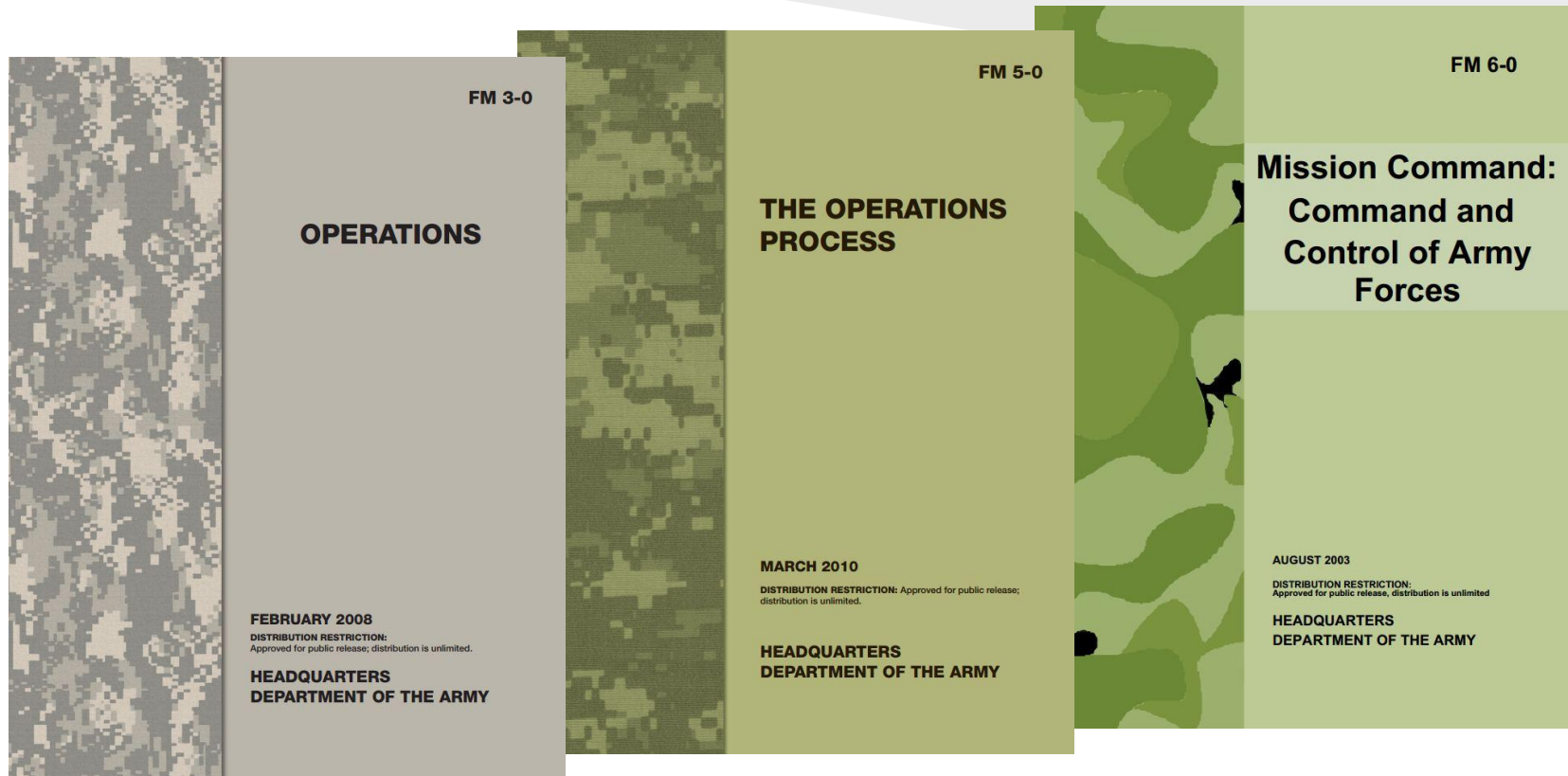
Foundations of Military Doctrine



Everything in war is very simple. But the simplest thing is difficult.

- Karl Von Clausewitz

Cornerstones of US Army Doctrine



Doctrinal manuals available online at:

(Army) http://armypubs.army.mil/doctrine/Active_FM.html

(Joint) http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

and here... <http://fas.org/irp/doddir/dod/>

Doctrine: Finding What You Are Looking For

U.S. doctrinal manuals are numbered hierarchically.

First digit uses the *continental staff numbering system*:

1. manpower or personnel
- 2. intelligence**
3. operations
4. logistics
5. plans
6. signal (communications or IT)
7. training
8. finance and contracts
9. civil-military operations or civil affairs

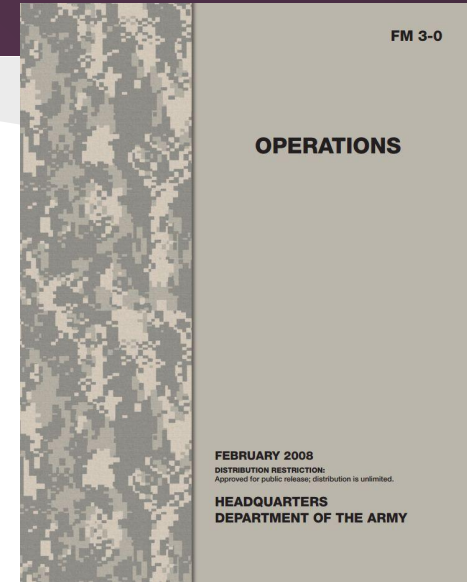
e.g.: Army FM **2-0** is “Intelligence Operations”

FM **2-91.4** is “Intelligence Support to Urban Operations”

Army Operations Doctrine

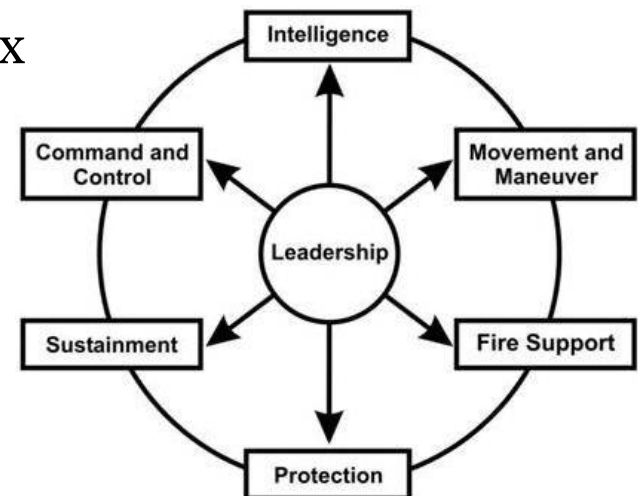
3-series FMs cover operations

- 3-0 Operations
- 3-09 Field Artillery and Fire Support
- 3-24 Counterinsurgency
- 3-60 The Targeting Process
- 3-90 Offensive and Defensive Ops



These manuals describe how to synchronize the six *warfighting functions*

- Movement and Maneuver
- Command and Control
- Intelligence
- Fire Support
- Protection
- Sustainment



A Short Story...



SMALL WARS
JOURNAL

Towards a Cyber Leader Course Modeled on Army Ranger School

By *Gregory Conti, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook, and Todd Arnold*
Journal Article | Apr 18 2014 - 11:31am

Towards a Cyber Leader Course Modeled on Army Ranger School

Gregory Conti, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook, and Todd Arnold

Since 1950, the U.S. Army Ranger School has garnered a well-earned reputation as one of the most demanding military schools in the world. Graduates have served with distinction in special operations units including the Ranger Regiment and Special Operations Command as well as line units throughout the Army. With the emergence of cyberspace as an operational domain and the critical shortage of technically and operationally competent cyber leaders, the time has come to create a U.S. Army Cyber Leader Course of equal intensity, reputation, and similar duration but focused on cyber operations (see Figure 1). This article presents a model for the creation of such a school, one that goes far beyond just a tough classroom experience by using tactical close-access missions as a core component. What we propose is unique, demanding, immersive, and fills a necessary gap in Army cyber leader development. This article is a condensed form of a more detailed analysis and description of the proposed Army Cyber Leader Course.



Figure 1: Cyber Tab. A Cyber Leader Course of similar duration and intensity to Ranger School, but tailored to cyber operations would help fill the critical shortage of technically and operationally competent cyber leaders.


We intend for this new Cyber Leader Course to be quickly recognized as the cyber operator's equivalent of Ranger School, much like the Sapper program has become the Engineer branch's 'Ranger School.' There is much to learn from Ranger School and other elite training programs that can inform a Cyber Leader Course. We face a critical shortage of qualified cyber leaders at all ranks and a demanding and rigorous Cyber Leader Course would develop the knowledge, skills, and abilities required of technically and operationally competent cyber leaders. A cadre of highly qualified cyber leaders is critical to the professionalization of the cyber career field, but the Army currently lacks a method for developing these leaders. While we propose the creation of an Army Cyber Leader Course, due to the inherently Joint

“Towards a Cyber Leader Course Modeled on Army Ranger School”


Small Wars Journal
18 April 2014

And Doctrine Man was There...

facebook [Sign Up](#) Keep me logged in

 **Doctrine Man!!**
April 18 at 3:06pm · 🌐

A Cyber Ranger School? This could get interesting.



Towards a Cyber Leader Course Modeled on Army Ranger School | Small Wars Journal
Since 1950, the U.S. Army Ranger School has garnered a well-earned...

English (US)
Facebook ©



Paul Dalen You have to write code 19 hours a day for 60 days with little food.

👍 16 · April 18 at 3:21pm

↪ 4 Replies



Brandon Owens I knew Ranger School would eventually become an online school.

👍 11 · April 18 at 3:24pm



Eric Graves Brandon - I love it when a good thing gets subverted by morons.

👍 4 · April 18 at 4:27pm



William Johnson if they go thru in winter do they get to sew on their cyber tab with white thread?

👍 4 · April 18 at 3:39pm



Duncan Idho When they complete do they get a Mentat badge and a new type of dip?

👍 4 · April 18 at 3:35pm



Bil Jihadwal I agree with most everything, except the stupid tab.

👍 4 · April 18 at 3:22pm



Glenn J Gambrell No Red Bull and Cheetos for 52 days.

👍 4 · April 18 at 3:10pm



Tristan Johnson ALL I WANNA BE IS A COMM SQUAD RANGER!
MAKIN MY LIVING OFF OF INTERNET DANGER!
COMM SQUAD RANGER!... [See More](#)

👍 3 · April 18 at 4:20pm

“You have to write code 19 hours a day with little food.”

Some Specific Examples...

We've picked a few key concepts of relevance to the infosec community:

- OPSEC
- Kill Chain
- Cyber Terrain
- Disinformation (Denial and Deception)
- Threat Intelligence & TTPs
- Intel Gain/Loss
- OODA Loop
- Targeting

Operations Security (OPSEC)*

- The **OPSEC process is a systematic method used** to identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations.
- The purpose of operations security (OPSEC) is to **reduce the vulnerability** of US and multinational forces from successful adversary exploitation of critical information. OPSEC applies to all activities that prepare, sustain, or employ forces.
- There is an entire Joint Publication on OPSEC...
Joint Publication 3-13.3



* JP 3-13.3, Operations Security, 4 January 2012, available at <https://publicintelligence.net/jcs-opsec/>

So How Can Good OPSEC Help Me?

Attackers:

- **Secrecy of the fact of the operation**
 - Avoiding detection
 - When detected, appear to be something else
- **Secrecy of information about the operation**
 - Protect details of the operation
 - Prevent defenders who are aware of the operation from being able to stop it
 - C&C addresses, vulnerabilities, malware samples, etc...
- **Secrecy of the identity of the operators**
 - Prevent defenders from directly striking the attacker
 - Is it possible to connect aspects of your operation to your real identity and location?

So How Can Good OPSEC Help Me?

Defenders:

- What can attackers learn about your organization through open sources?
 - Material for Spear Phishing attacks
 - Aspects of your Information Security Program
 - What products do you use?
 - What do your IT staff say on their resumes, linkedin profiles, and twitter accounts?
- Its hard for large commercial organizations to maintain good OPSEC - focus on the most important secrets.

The OPSEC Process from JP3-13.3

1. Identification of Critical Information

What are you trying to protect?

2. Analysis of Threats

Who is trying to get it?

3. Analysis of Vulnerabilities

How might they get to it?

4. Assessment of Risk

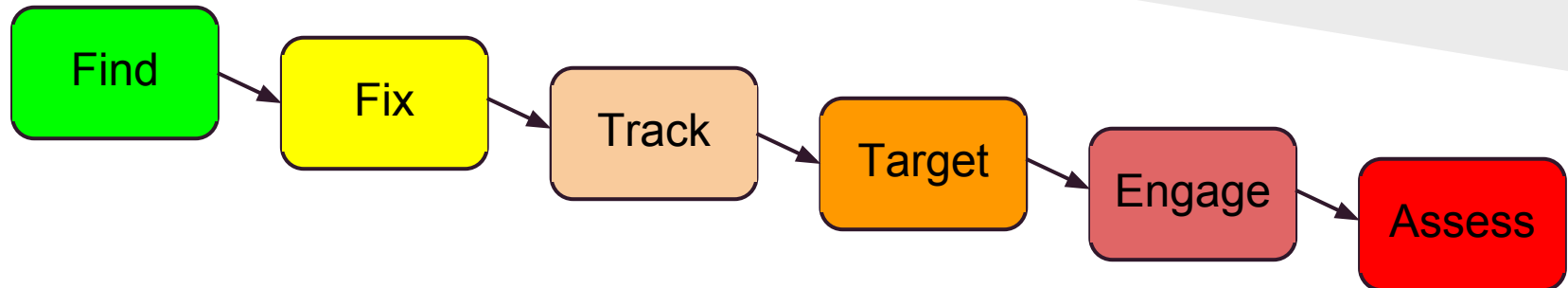
Risk = threat \times vulnerability; what are you willing to accept?

5. Application of Appropriate Operations Security Countermeasures

Plug the holes!



Kill Chain

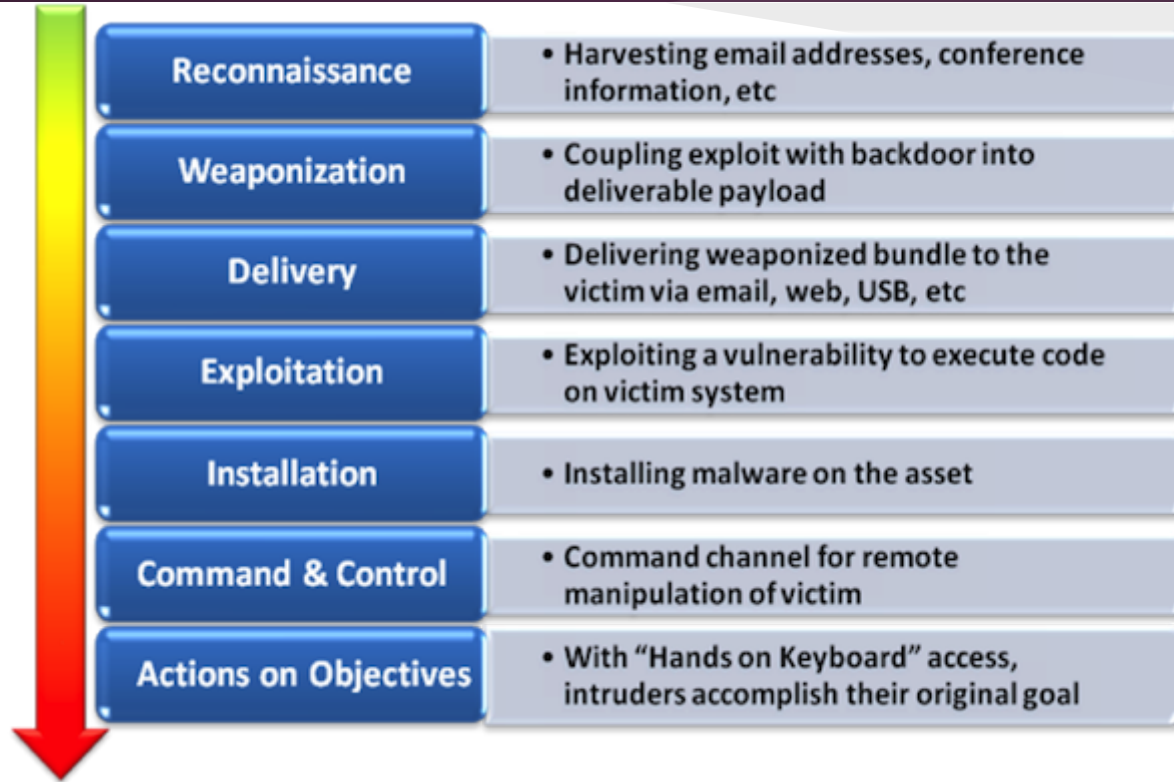


- US Air Force targeting methodology dating to late 1990's
- Also referred to by clever acronym:
F2T2EA

"In the first quarter of the 21st century, it will become possible to find, fix or track, and target anything that moves on the surface of the Earth."

GEN Ronald R. Fogleman, USAF Chief of Staff
October 1996

Cyber Kill Chain

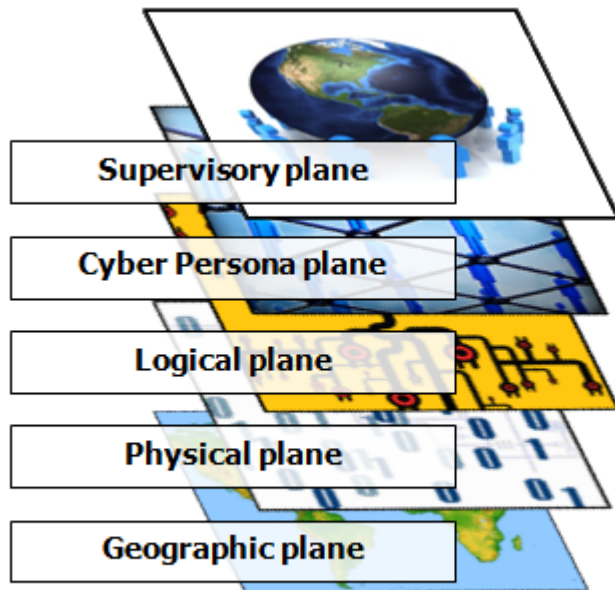


- Cyber Kill Chain first proposed in a 2010 Lockheed-Martin whitepaper: ***“Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”***, by Hutchins, et. al.

The Value of the Kill Chain

- Drives the defender to take a comprehensive view of the lifecycle of an attack rather than focusing on a single stage.
- Provides a framework for organizing artifacts of an attack collected during an investigation.
- Turns asymmetry on its head – the attacker must remain covert through each stage of their operation – each stage presents the defender with an opportunity to detect the attack.

Cyberspace Planes and Cyber Terrain



Most references to ***cyber terrain*** consider only the ***physical plane***.

- Supervisory plane
 - Command and Control
- Cyber persona plane
 - Persons or ‘accounts’
- Logical plane further divided into top 6 OSI layers (data link – application)
 - Operating system and application programs
 - Services – web, email, file systems
 - Logical network protocols
- Physical plane == OSI PHY layer (layer 1)
 - Network devices – switches, routers
- Geographic plane == physical location
 - Location in which an info system resides

For more on cyber terrain and cyber key terrain, see Raymond, et. al, “Key Terrain in Cyberspace: Seeking the High Ground,” in *6th Annual NATO Conference on Cyber Conflict*, Tallinn, Estonia, June 2014.

Cyber Terrain Analysis (OCOKA)

- Observation and Fields of Fire

What portions of my network can be seen from where?

- Cover and Concealment

What can I hide from observation?

- Obstacles

How can I make my network harder to attack?

- Key Terrain

Cyber terrain that can provide a 'marked advantage'

- Avenues of Approach

Don't just think of routers and cables . . .

Leveraging Cyber Key Terrain

An approach to leveraging key terrain emerges from considering the terrain analysis as an **attacker** and as a **defender**.

As a defender:

- Identify Potentially Targeted Assets
- Enumerate Avenues of Approach
- Consider Observation and Fields of Fire
- Place Obstacles, Cover, and Concealment

Observation and Fields of Fire

```
Nmap 5.00
# nmap -A -T4 scanme.nmap.org 207.68.200.30

Starting Nmap 5.00 ( http://nmap.org ) at 2009-07-13 16:22 PDT
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey: 1024 03:5f:d3:9d:95:74:8a:00:8d:70:17:9a:bf:93:84:13 (DSA)
|_ 2048 fa:af:76:4c:b0:f4:4b:83:a4:0e:70:9f:a1:ec:51:0c (RSA)
53/tcp    open  domain   ISC BIND 9.3.4
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.2.2 ((Fedora))
|_ html-title: Go ahead and ScanMe!
113/tcp   closed auth
13337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)

Interesting ports on 207.68.200.30:
Not shown: 991 filtered ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Microsoft DNS 6.0.6001
88/tcp    open  kerberos-sec    Microsoft Windows kerberos-sec
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows 2000 netbios-ssn
389/tcp   open  ldap            Microsoft Windows 2000 microsoft-ld
464/tcp   open  kpasswd5?
49158/tcp open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
49175/tcp open  msrpc           Microsoft Windows RPC
Running: Microsoft Windows 2008|Vista

Most script results:
|_ smb-os-discovery: Windows Server (R) 2008 Enterprise 6001 Service Pack 1
|_ LAN Manager: Windows Server (R) 2008 Enterprise 6.0
|_ Name: MSAPPLELAB\APPLELAB2KB
|_ System time: 2009-07-13 16:17:07 UTC-7
|_ nbstat: NetBIOS name: APPLELAB2KB, NetBIOS user: <unknown>, NetBIOS MAC:
00:1a:a0:9a:a3:96
|_ Name: APPLELAB2KB<00>      Flags: <unique><active>
|_ Name: MSAPPLELAB<00>     Flags: <group><active>

TRACEROUTE (using port 135/tcp)
HOP RTT ADDRESS
[Cut first 8 lines for brevity]
9 36.88 ge-10-0-hsa1.Seanette1.Level3.net (4.68.105.6)
10 36.61 unknown.Level3.net (209.245.176.2)
11 41.21 207.68.200.30

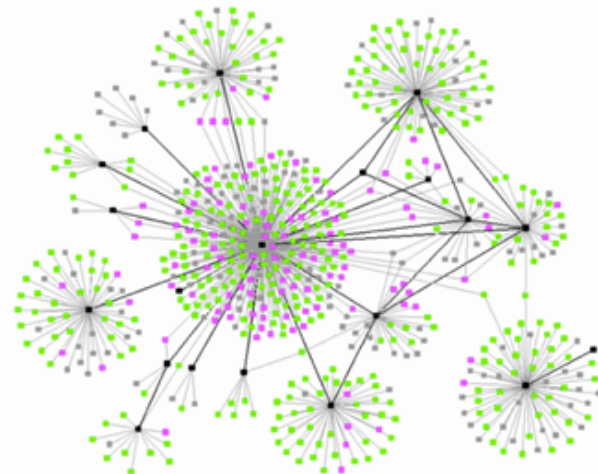
Nmap done: 2 IP addresses (2 hosts up) scanned in 120.26 seconds
# (Note: some output was modified to fit results on screen)
```

What does an attacker need access to in order to observe or attack a particular interface associated with a potentially targeted asset?

This is **an iterative analysis**. For example, if the attacker needs access to a particular network in order to reach a critical asset, how can that network, in turn, be accessed?

It is through this iterative analysis that a picture of **Key Terrain** begins to emerge, which include highly interconnected resources as well as resources with connectivity to critical assets.

Its important to consider terrain that your organization doesn't control – attacks on supply chain integrity, waterhole attacks, etc...



Lessons from Cyber Terrain Analysis

- Battlefield Terrain Analysis maps fairly closely to the sort of analysis that network security people perform when thinking about a network's exposures.
- Defenders know the terrain they are defending – attackers must discover it through iterative reconnaissance.
- Defenders can exploit an attacker's lack of knowledge of the terrain.

Exploiting the Human

- It is often observed that the human is the weakest link in any network defense.
- Often, the human is also the weakest link in any network offense.
- What are you doing in your network defense to exploit the human behind the attacks that are targeting you?

Denial*

- **Denial** includes those measures designed to hinder or deny the enemy the knowledge of an object, by hiding or disrupting the means of observation of the object.
- The basis of **denial** is *dissimulation*, the concealing of the truth.

Deception*

- **Deception** is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
- The basis of **deception** is *simulation*, the presentation of that which is false.

Network Denial & Deception

On the Internet, there is no way to tell whether or not something is actually real.

- Denial
 - Hidden file systems
 - Real services on unusual ports
- Deception
 - Fake database records (Canaries)
 - Fake employees or user accounts
 - Phoney systems and services

Remember - what is important to you isn't necessarily what is important to your adversary.

What is Threat Intelligence?

00dbb9e1c09dbdafb360f3163ba5a3de
00f24328b282b28bc39960d55603e380
0115338e11f85d7a2226933712acaae8
0141955eb5b90ce25b506757ce151275
0149b7bd7218aab4e257d28469fddbod
016da6ee744b16656a2ba3107c7a4a29
01eodc079d4e33d8eddo50c4900818da
024fd07dbdacc7da227bede3449c2b6a
0285bd1fbdd7ofd5165260a490564ac8
02a2d148faba3b6310e7ba81eb62739d
02c65973b6018f5d473d701b3e7508b2
034374db2d35cf9da6558f54cec8a455
03ae71eba61af2d497e226da3954f3af
0469a42d71b4a55118b9579c8c772bb6
0496e3b17cf40c45f495188a368c203a
04a7b7dab5ff8ba1486df9dbe68c748c
04e83832146034f9797d2e8145413daa
04f481d6710ac5d68doeacac2600a041
0501bb10d646b29cab7d17a8407010d9
0522e955aaee70b102e843f14c13a92c
052eco4866e4a67f31845d656531830d
0545a524a6bbobo42f4booda53fec948
05552a77620933dd8of1e176736f8fe7
0583f58ac3d804d28cd433d369b096b8
0588ffa0a244a2c4431c5c4faac60b1f

aoldaily.com
aolon1ine.com
applesoftupdate.com 12.38.236.32
arrowservice.net 71.6.141.230
attnpower.com 72.240.45.65
aunewsonline.com 203.231.234.23
avvmail.com 202.64.109.187
bigdepression.net 223.25.233.36
bigish.net
blackberrycluter.com
blackcake.net
bluecoate.com
booksonlineclub.com
bpyoyo.com
businessconsults.net
businessformars.com
basketball.com
canadatvsite.com
canoedaily.com
chileexe77.com
cnndaily.com
cnndaily.net
cnnnewsdaily.com

Doctrinal Definition of Intelligence

- Joint Publication 2-0, Joint Intelligence*:
“The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.”
- In practice, it is a **thorough analysis** and **understanding** of the threat’s **capabilities**, **strategy**, and **tactics** and how they can be used on the **cyber terrain** comprising your operational environment.

* Definition from JP 2-0, Joint Intelligence, 22 October 2013, available at <http://www.dtic.mil/doctrine/index.html>

The Intelligence Cycle

Planning and direction

Collection

Processing and exploitation

Analysis and production

Dissemination and integration

Evaluation and feedback

Nothing is more worthy of the attention of a good general than the endeavor to penetrate the designs of the enemy.

Niccolò Machiavelli
Discourses, 1517

Characteristics of Effective Intelligence

Information Quality Criteria

- Accuracy
- Timeliness
- Usability
- Completeness
- Precision
- Reliability

Additional Criteria

- Relevant
- Predictive
- Tailored

Commanders' Considerations include

Reducing operational uncertainty

Determine appropriate balance between time allotted for collection and operational necessity

Prioritize finite resources and capabilities, including network bandwidth

Employing internal and supporting intel assets as well as planning, coordinating, and articulating requirements to leverage the entire intelligence enterprise.

Tactics, Techniques, and Procedures (TTPs)

Tactics - The employment and ordered arrangement of forces in relation to each other

Techniques - Non-prescriptive ways or methods used to perform missions, functions, or tasks

Procedures - Standard, detailed steps that prescribe how to perform specific tasks

The term TTP is used to refer broadly to the actions that one might take in a particular problem domain.

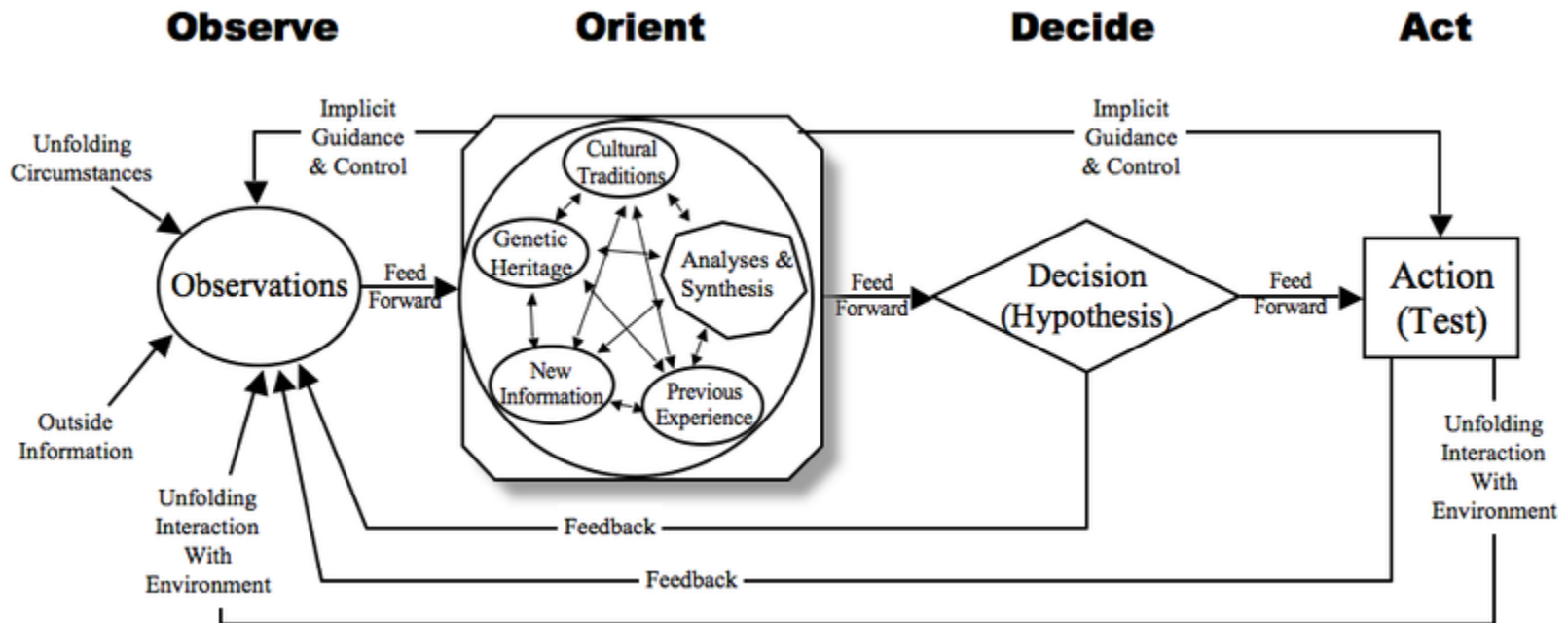
Risk Analysis

Intel Gain/Loss Calculus

- You've discovered an attacker in your network. You could kick them out, but they'd notice that.
- How do you decide when to kick them out and when to let them continue?
- Counter-intuitively, the risk of allowing them to continue increases the more that you know about them.

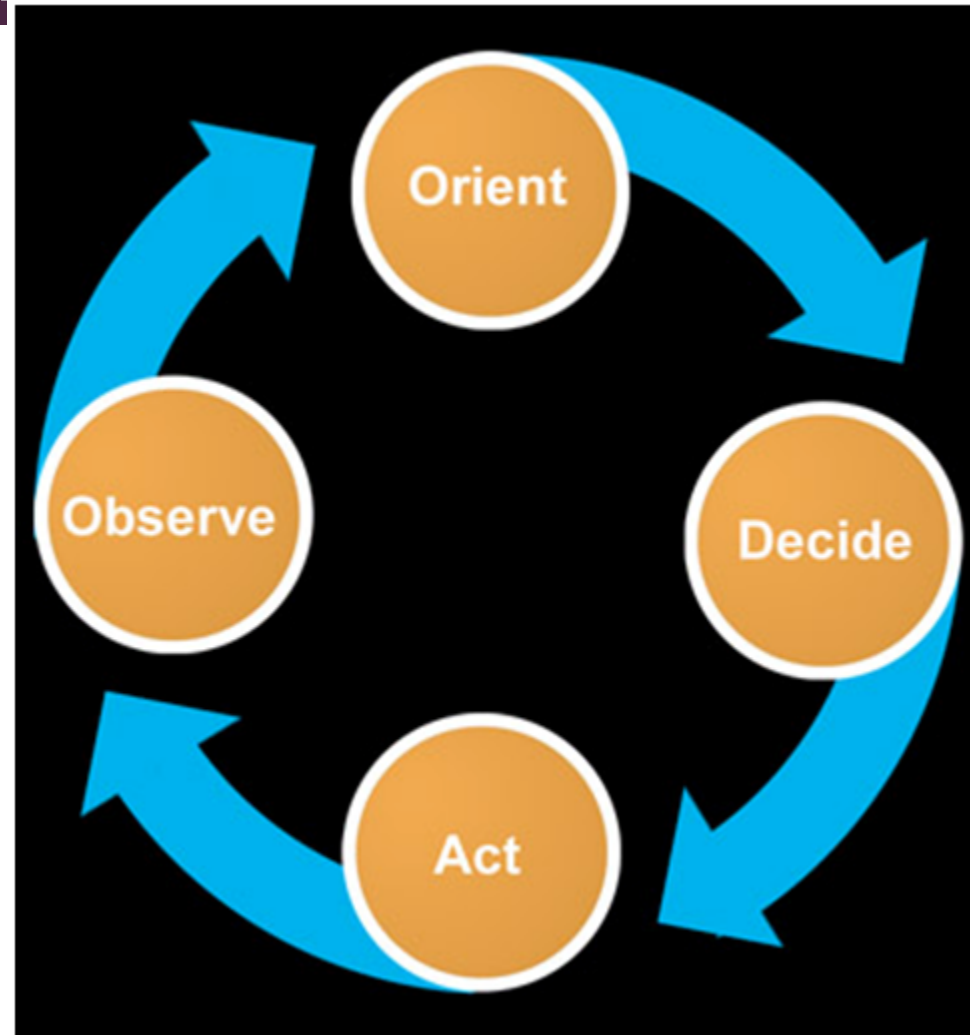
The OODA Loop

- COL John Boyd, USAF
- Writings can be found at <http://dnipogo.org/john-r-boyd/>, provided by the *Project on Government Oversight*



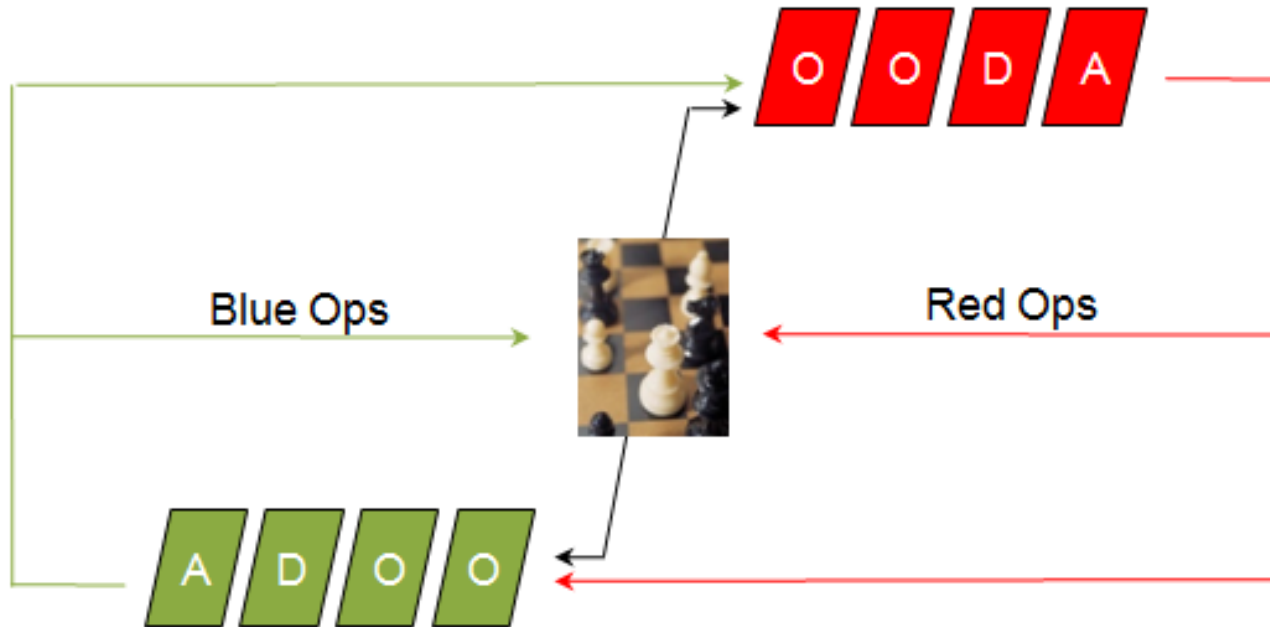
Simplified OODA in the Context of Time

- **Intelligence**
 - Observation
 - Orientation
- **Execution**
 - Decision
 - Action



OODA for Cyber Security

Conflict: Red vs. Blue



Spin your loop faster than your adversary

OODA Loop Summary*

- Observation and Orientation (OO) increases your perceptive boundaries.
Superior Situational Awareness
- Sampling Rate of the OO is relative to the rate of change
Fast enough to represent change
- Decision and Actions raise the cost to your adversaries'
Observation/Orientation
- Operate at a faster tempo or rhythm than our adversaries

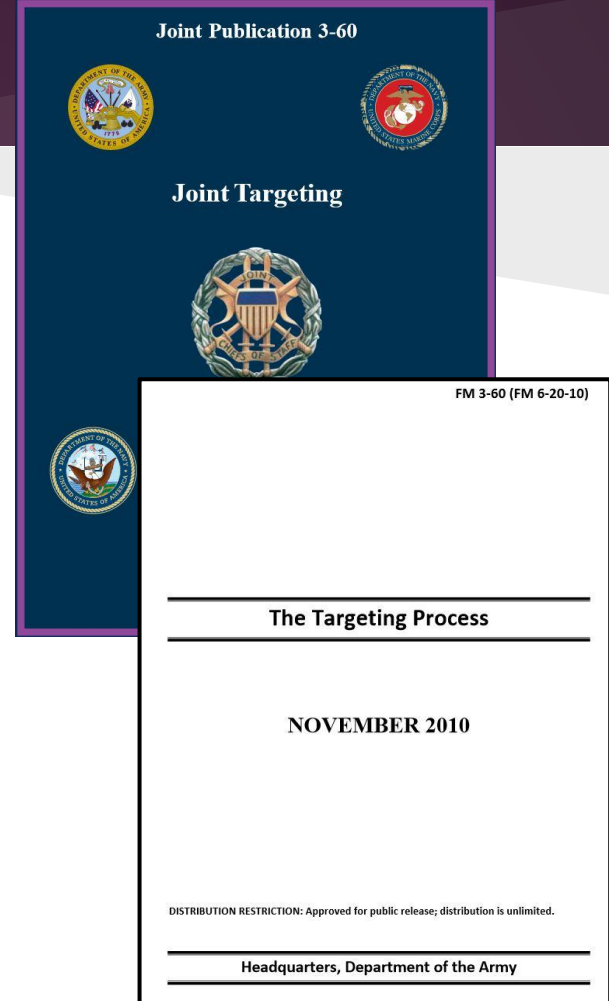
Ultimately you are making it more expensive for the adversary to operate and hide

Targeting

Targeting: The process of selecting and prioritizing **targets** and matching the appropriate response to them.

Target: An entity or object considered for possible engagement or action . . . to support commander's objectives.

Purpose: integrate and synchronize fires into joint operations.



What is Targeting good for?

- Targeting is a continuous cycle that begins with an analysis of the effects the commander wants to achieve
- Can be lethal or “non-lethal”
Effects might include
 - Deceive
 - Degrade
 - Destroy
 - Influence
- Gives commanders a continuous process to influence their battlespace

Targeting Methodology

DECIDE

Scheme of Maneuver/Fires, High-Payoff Target List

DETECT

Execute Intelligence Collection Plan

DELIVER

Execute Attack Guidance Matrix

ASSESS

Combat Assessment

How Does This Apply to Cyber Ops?

Computer-based effects can be used as part of, or instead of, lethal military action.

- Israeli cyber attack on Syrian air defense systems (2007)
- Russia's coordinated virtual attack and physical invasion of Georgia (2008)
- Stuxnet (2010)

Other Useful Doctrinal Concepts

The following discussion provides pointers to other areas that warrant continued research.

Military Operational Planning

Planners use the Military Decision Making Process (MDMP)

Step 1: Receipt of Mission

Step 2: Mission Analysis

Step 3: Course of Action (COA) Development

Step 4: COA Analysis (wargaming)

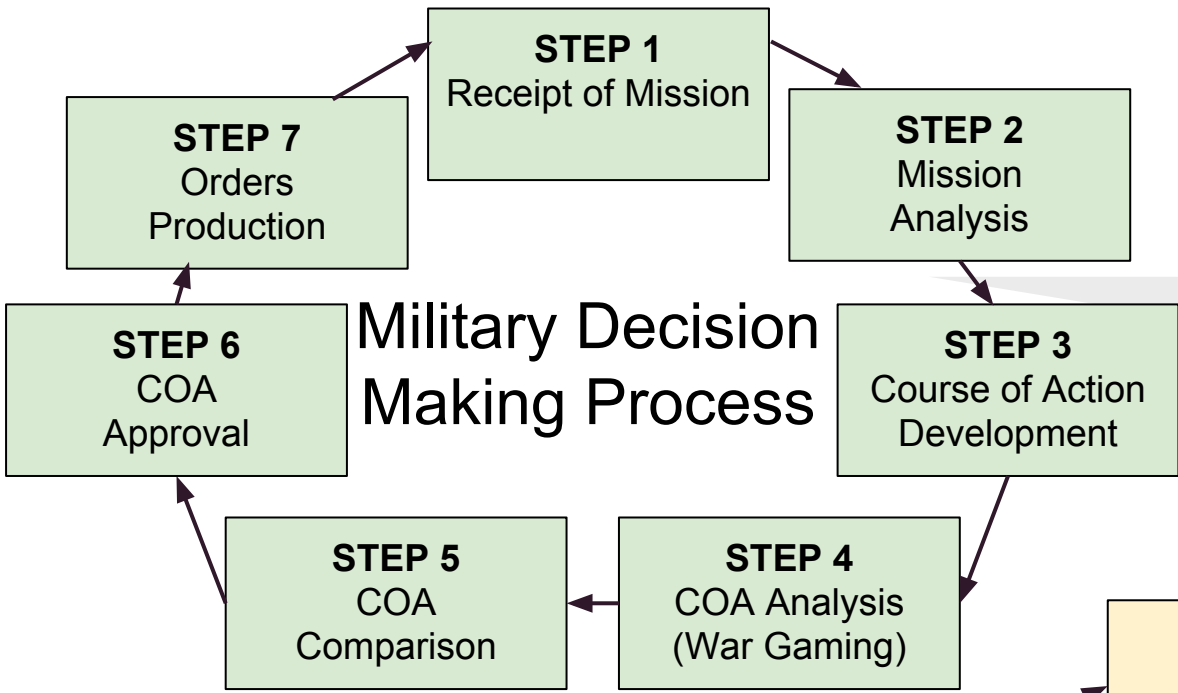
Step 5: COA Comparison

Step 6: COA Approval

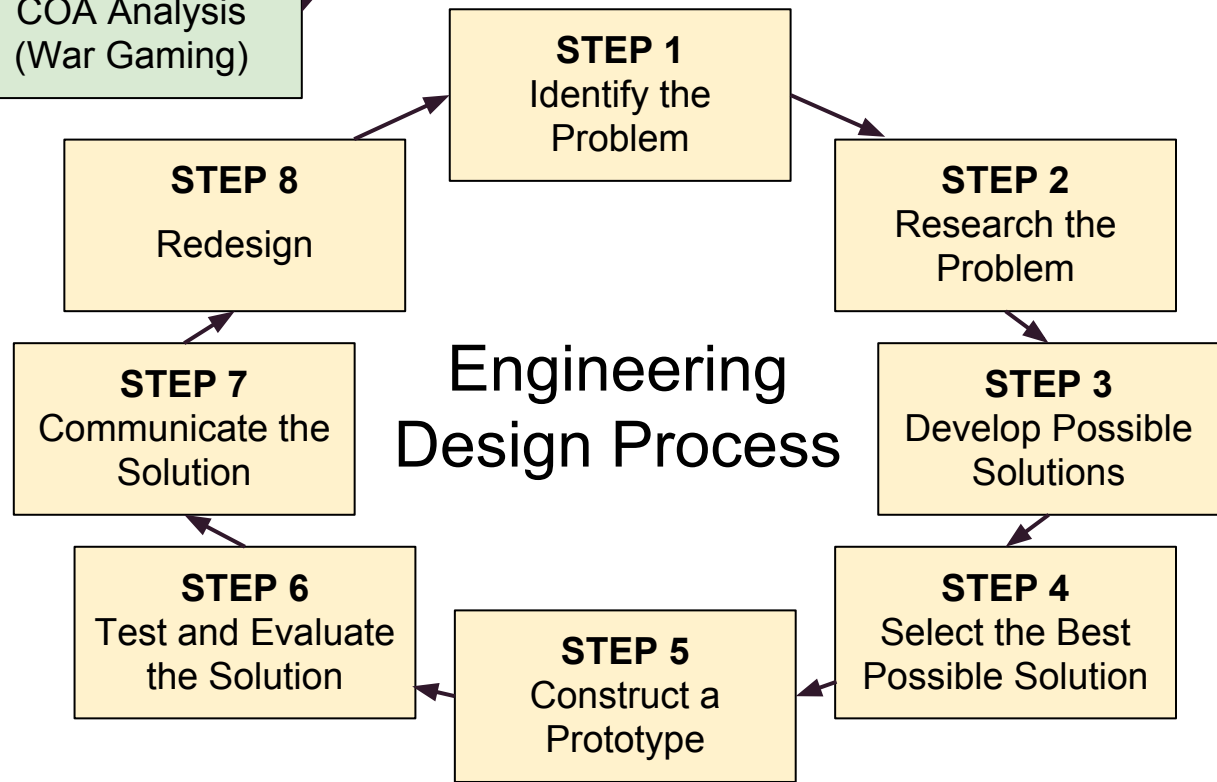
Step 7: Orders Production

Appendix B of Army FM 5-0, The Operations Process, provides excellent coverage of MDMP. This systematic decision-making process mirrors the **Engineering Design Process**, which should be familiar to many in this audience.

Military Decision Making Process



Engineering Design Process



“Design” - the DoD’s latest doctrinal buzzword

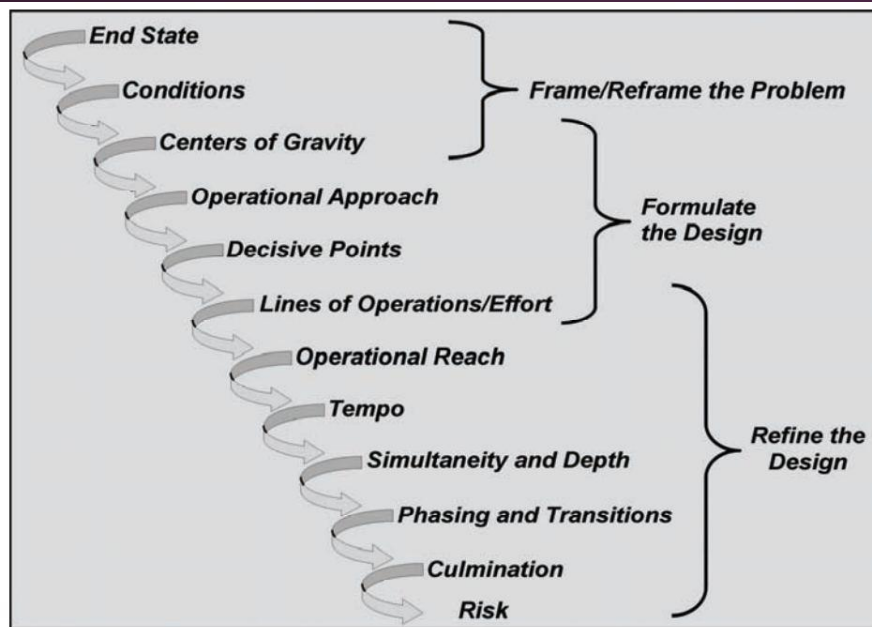


Figure 6-4. Linking the elements of operational design

- Conceived at the School for Advanced Military Studies, or SAMS, in mid-2000’s
- Intended as a thought process for the commander to translate desired strategic effects to tactical actions on the battlefield
- Actually useful as a conceptual model!

Design (or “Operational Design”):

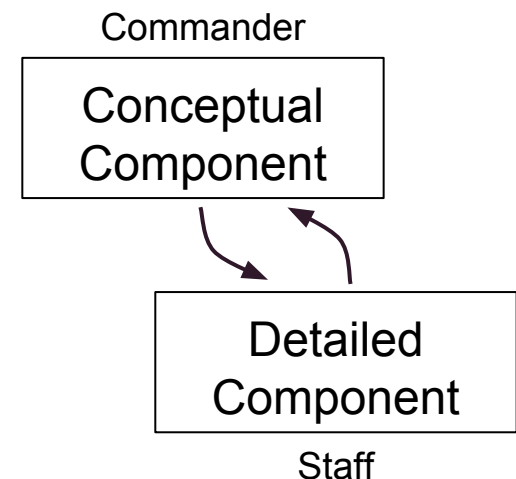
- Introduced in Joint Pub 3-0, Operations in chapter on “The Art of Joint Command”
- Refined in doctrinal manuals on planning (e.g.: FM5-0, The Operations Process)

“Design” Explained

*Design is a methodology for applying critical and creative thinking to understand, visualize, and describe **complex, ill-structured problems** and develop approaches to solve them.*

































Army FM 5-0 The Operations Process

- Emphasizes role of the commander
- Requires creative thinking, dialog, and collaboration
- Is executed in parallel with operational planning
- Designed to be iterative:
 - question assumptions
 - incorporate new facts
 - abandon dead ends
 - refine the problem statement



* Best doctrinal reference: Army FM 5-0:
<https://www.fas.org/irp/doddir/army/fm5-0.pdf>

Graphics and Symbology

Description	Friend	Hostile	Neutral	Unknown
Seaport of Debarcation/Seaport of Embarkation (SPOD/SPOE)				
Aerial Port of Debarcation/Aerial Port of Embarkation (APOD/APOE)				
Maintenance				
Maintenance Symbol: Double Wrench				
Maintenance Heavy				
Maintenance Electro-Optical				
Maintenance Recovery				
Maintenance Ordnance				
Maintenance Missile Ordnance				

484 pages of operational terms and graphics.

See FM 1-02

http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm1_02.pdf

Great Resources for More Information

DoD and Military Branch doctrine:

- Intelligence and Security Doctrine (including DoD and all military branches) Federation of American Scientists' Intelligence Resource Program <http://www.fas.org/irp/doddir>
- DOD Dictionary. http://www.dtic.mil/doctrine/dod_dictionary/
- Joint Doctrine. <http://www.dtic.mil/doctrine/doctrine/>
- Army Doctrine. http://armypubs.army.mil/doctrine/Active_FM.html

Publications:

- Small Wars Journal: <http://smallwarsjournal.com> (all online content)
- Military review: <http://militaryreview.army.mil> (online and print)
- Parameters: <http://strategicstudiesinstitute.army.mil/pubs/parameters> (online and print). US Army War College quarterly journal.
- Army Branch Magazines (Armor magazine, Infantry magazine, Artillery magazine, ArmyAviation magazine, etc.
- Combined Arms Research Digital Library: <http://cgsc.contentdm.oclc.org>

More resources

Military Theorists:

- Clausewitz, Carl von. *On War*, [available at www.clausewitz.com], 1832
- Jomini, Antoine Henri. *The Art of War*, [available at www.gutenberg.org], 1862
- Mitchell, William. *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military*. The University of Alabama Press, Tuscaloosa, AL. 1925
- Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Little, Brown and Company, 2002
- Mao Zedong. *On Guerilla Warfare*, [Online]. Available at <http://www.marxists.org/>, 1937
- Mahan, Alfred Thayer. *The Influence of Sea Power Upon History: 1660 - 1783*, Little, Brown and Co. 1890

- Lots more . . .

Yet more . . .

Conferences:

- NATO Conference on Cyber Conflict (CyCon): <http://ccdcoe.org/cycon/home.html>
- IEEE/AFCEA Annual Military Communications Conference (MILCON): <http://www.milcom.org/>

Other:

- Center for Army Lessons Learned: <http://usacac.army.mil/CAC2/call/>

[See our whitepaper for lots more references!]

Resources on Adversary Doctrine and Strategy: China



- Timothy Thomas' trilogy and Chinese Information Warfare doctrine, published by the Army's Foreign Military Studies Office at Fort Leavenworth.
 - *Dragon Bytes*, 2003
 - *Decoding the Virtual Dragon*, 2007
 - *The Dragon's Quantum Leap*, 2009



- Liang, Qiao and Xiangsui, Wang. *Unrestricted Warfare*. Summaries and translations abound on the web; extensively covered in Thomas' Chinese IW trilogy.

More Adversary Doctrine and Strategy: Russia

Russian Military Publications:

- “Doctrine of Information Security of the Russian Federation” (2000)
- “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space” (2011)

American Foreign Policy Council’s Defense Dossier:

- “How Russia Harnesses Cyberwarfare,” by David J. Smith.

Deconstructing <Reversing> Doctrine...

- Ukraine
- Georgia
- Estonia
- Stuxnet
 - Legal review
 - Clarke analysis
 - Collateral damage mitigation

Questions???

Backup Slides

But the government is here to help, right?

“DoD will employ new defense operating concepts to protect **DoD networks and systems.**”

- DoD Strategy for Operating in Cyberspace

“The Department of Homeland Security (DHS) is responsible for helping **Federal Executive Branch civilian departments and agencies secure their unclassified networks (.gov).**”

- DHS. *Preventing and Defending Against Cyber Attacks*. June 2011

“The mission of the [FBI] Cyber Division is to coordinate, supervise, and facilitate the FBI's **investigation of those federal violations** in which the Internet, computer systems, or networks are exploited as the principal instruments or targets . . .”

- FBI Cyber Division mission statement

Attributes of Effective Doctrine

Success in Combat

Acceptability by the Military and Nation

Adaptability and Flexibility

Relevancy

Attainability

Why Does Doctrine Change

Strategic Objectives

Strategic Environment

Changes in Leadership

Defeat/Success on the Battlefield

Changes in Technology

Changes in Available Resources

Enlightened Vision

Indicators of Doctrinal Change

Use Against a Third Party

War Games and Exercises

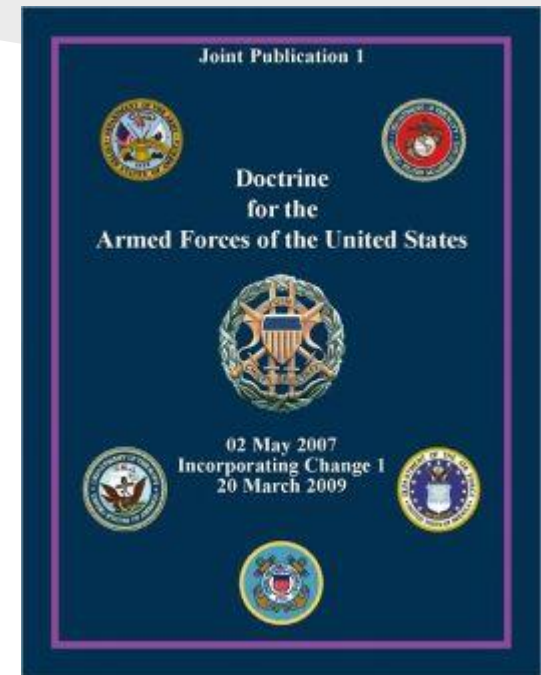
New Manuals or Doctrinal Publications

New Service School Curriculum

Professional Publications

Joint Doctrine

- Codified in **Joint Publications**
- Approved by **Chairman of the Joint Chiefs of Staff**
- Provides a **common frame of reference** among the branches of service and helps **standardize operations**
- Each service must create it's own doctrine that is nested (or compliant with) Joint Doctrine



Available online on the Joint Electronic Library. <http://www.dtic.mil/doctrine/>



US Cyber Operations Doctrine

JP 3-12 - Cyberspace Operations

- Overarching doctrine for US approach to cyberspace operations
- Unfortunately, it is classified **SECRET**

Army FM 3-28 - Cyber Electromagnetic Activities

- Describes how cyberspace operations planning is integrated into Army operational planning
- *Unclassified!*