RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

#RSAC

SESSION ID: STR-F02

The Library of Sparta: Applying Military Doctrine to CyberSecurity

MODERATOR:

Tom Cross

CTO
Drawbridge Networks
@_decius_

PANELISTS:

Greg Conti

Associate Professor
United States Military Academy at West Point
@cyberbgone

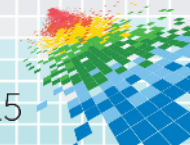
David Raymond

Associate Professor
United States Military Academy at West Point
@dnomyard

Disclaimer

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

DRAWBRIDGE NETWORKS



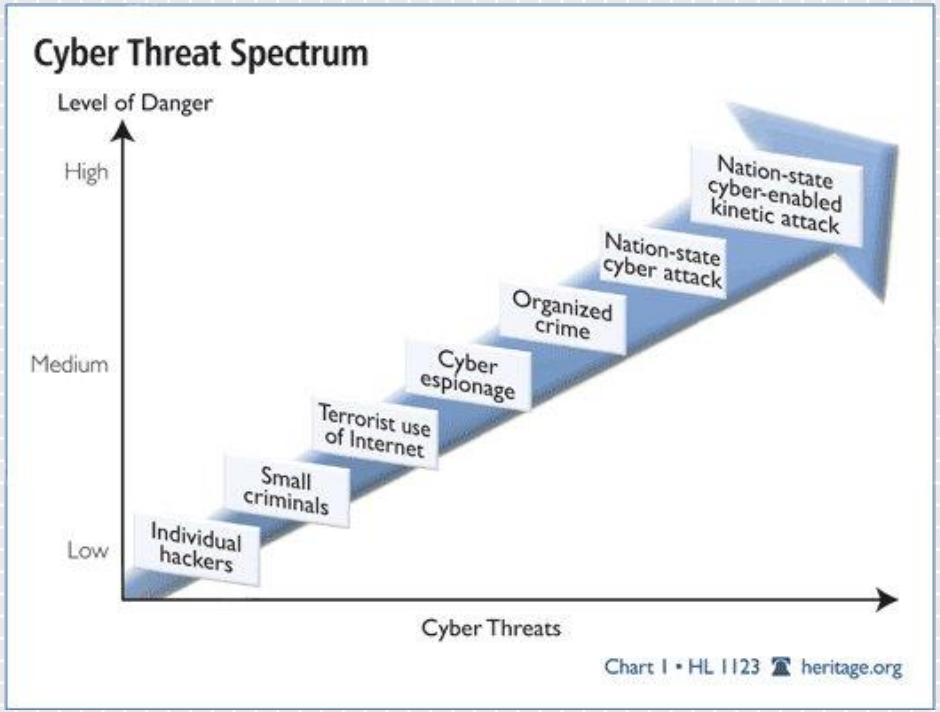
Our Background...

Tom Cross
Drawbridge Networks
@_decius_

Greg Conti
West Point
@cyberbgone

David Raymond
West Point
@dnomyard

Why, So What, and Who Cares…



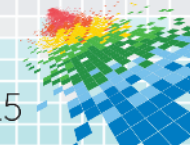
You used to be fighting individuals . . .

. . . now you are defending yourselves against nation-states

On the Internet, the offense has all the cards

What is Doctrine?

DRAWBRIDGE NETWORKS



A Sacred Text For Some

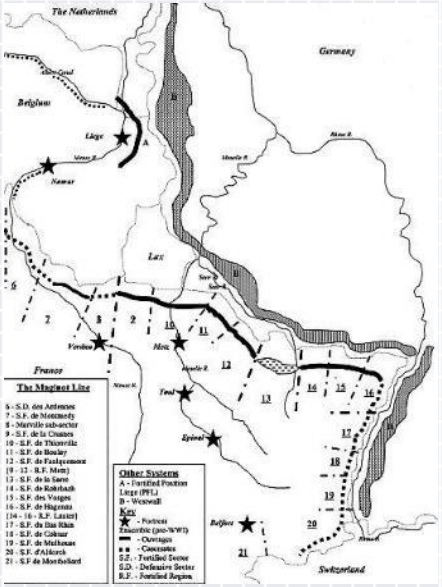
An Anathema to Others

"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

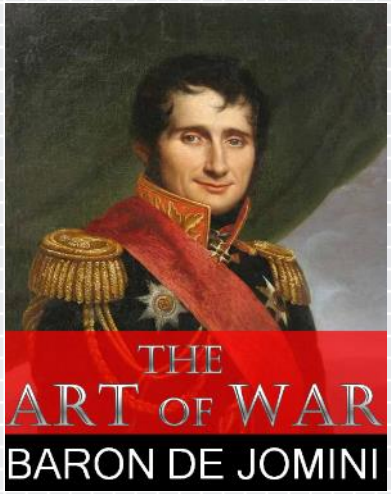
The Answer is Somewhere in the Middle

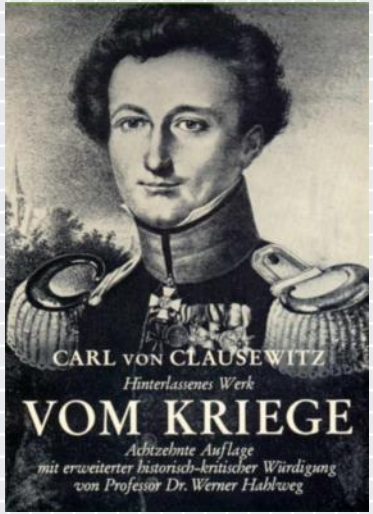


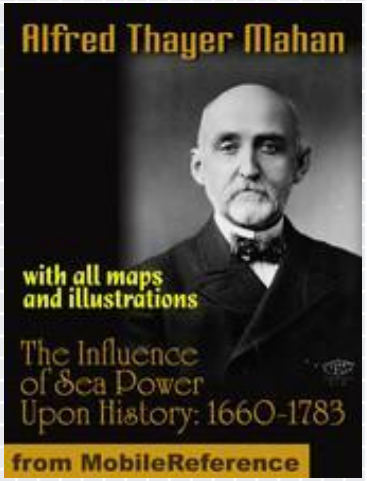
Bad Doctrine

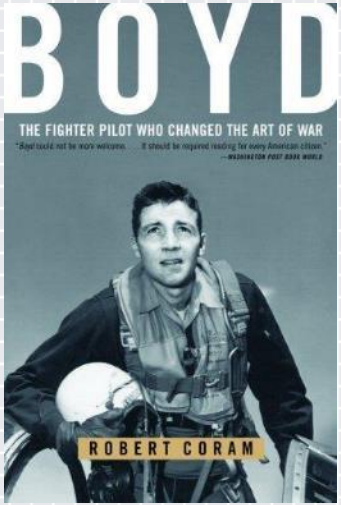
Good Doctrine

Foundations of Military Doctrine









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

- Karl Von Clausewitz

Doctrine: Finding What You Are Looking For

U.S. doctrinal manuals are numbered hierarchically.
First digit uses the *continental staff numbering system*:

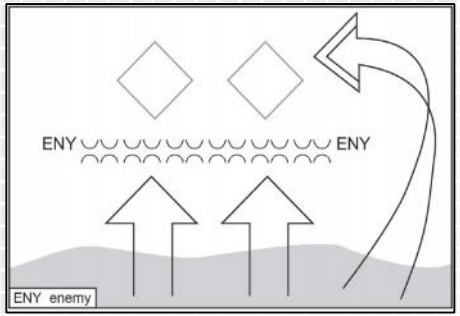
1. manpower or personnel
2. **intelligence**
3. operations
4. logistics
5. plans
6. signal (communications or IT)
7. training
8. finance and contracts
9. civil-military operations or civil affairs

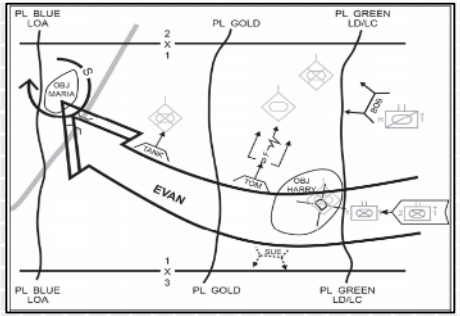
e.g.: Army FM **2**-0 is “Intelligence Operations”
FM **2**-91.4 is “Intelligence Support to Urban Operations”

Some Specific Examples...

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

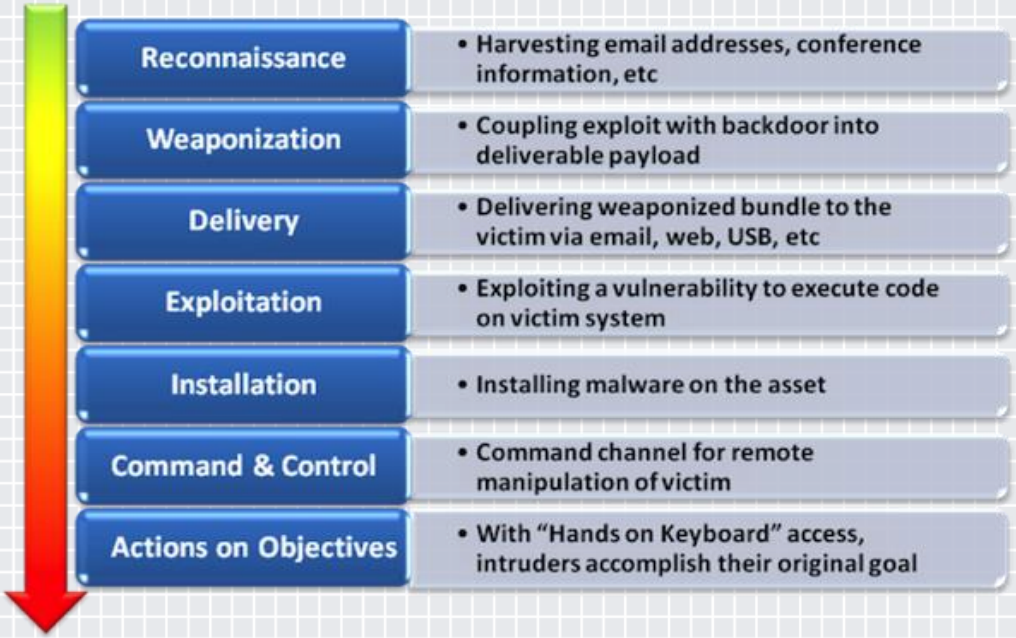
- Kill Chain
- OPSEC
- Cyber Terrain
- Disinformation (Denial and Deception)
- Threat Intelligence & TTPs
- Intel Gain/Loss
- OODA Loop
- Targeting





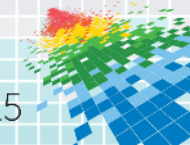
Cyber Kill Chain

- Kill Chain was a US Air Force targeting process dating to late 1990's (Find, Fix, Track, Target, Engage, Assess)
- 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

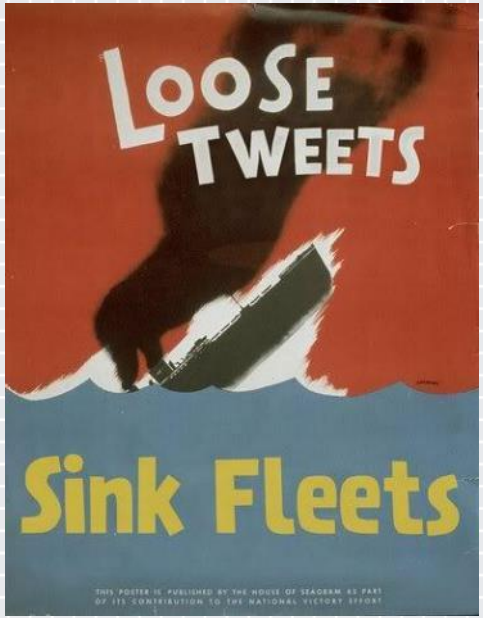
- Drives the defender to take a comprehensive view of the lifecycle of an attack rather than focusing on a single stage.
- Provides a framework for organizing artifacts of an attack collected during an investigation.
- Turns asymmetry on its head – the attacker must remain covert through each stage of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



Operations Security (OPSEC)*

- The **OPSEC process is a systematic method used** to identify, control, and protect critical information.
- The purpose of operations security (OPSEC) is to **reduce the vulnerability** of forces from successful adversary exploitation of critical information.
- 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.
- Secrecy of information about the operation.
- Secrecy of the identity of the operators.

Defenders:

- What can attackers learn about your organization through open sources?
- Focus on the most important secrets – it is hard for large commercial organizations to maintain good OPSEC.

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?

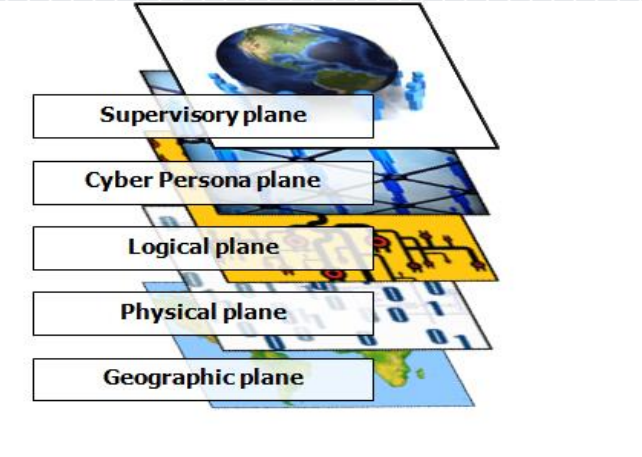
4. Assessment of Risk

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

5. Application of Appropriate Operations Security Countermeasures

   Plug the holes!

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**
  - 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

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

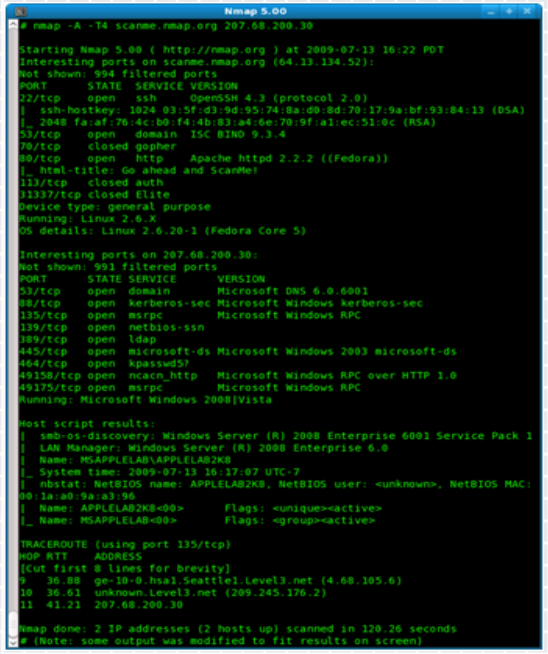
  How can I make my network harder to attack?
- Key Terrain

  Cyber terrain that can provide a ‘marked advantage’
- Avenues of Approach

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

DRAWBRIDGE NETWORKS

Observation and Fields of Fire



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 and Deception

TRICKERY ON WAR

Lists Roosevelt 'Subterfuges' at Garden Rally—Wheeler Charges Secret Pledges

The text of Mr. Lindbergh's speech will be found on Page 4.

Declaring that "there is no danger to this nation from without" but that "our only danger lies from within," Charles A. Lindbergh charged last night that the American people were being led into war by subterfuge. He appealed to them to unite behind a demand for "a leadership of integrity" in Washington.

- **Denial** - Blocking of adversary access to accurate information, regarding one's actions or intentions.
- **Deception** - Construction of a false reality for the adversary, via intentionally "leaked" false information, or other measures.
- **False Flag** - Covert operation designed to deceive, such that ops appear to be carried out by other entities, groups or nations.

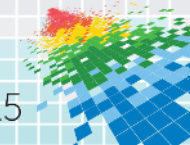
Network Denial & Deception

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.

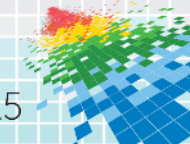
DRAWBRIDGE NETWORKS



Focus - Target for Cyber Deception

	Attacker	Defender
Human	• Decoy web page • Honeynet	• Convincing IT Help Desk to reset password • Phishing
Code / Machine	• Analysis VM environment convinces malware it is “real” • Spoofed network service banners	• Spoofing browser user agent • Spoofing IP address • Spoof packet header data

DRAWBRIDGE NETWORKS



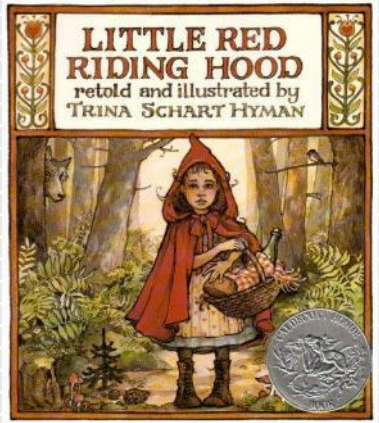
Effects

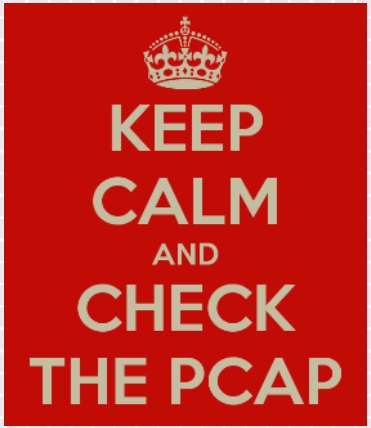
- **Deceive** - Cause a person to believe what is not true
- **Degrade** - Temporary reduction in effectiveness
- **Delay** - Slow the time of arrival of forces or capabilities
- **Deny** - Withhold information about capabilities
- **Destroy** - Enemy capability cannot be restored
- **Disrupt** - Interrupt or impede capabilities or systems
- **Divert** - Force adversary to change course or direction
- **Exploit** - Gain access to systems to collect or plant information
- **Neutralize** - Render adversary incapable of interfering with activity
- **Suppress** - Temporarily degrade adversary/tool below level to accomplish mission

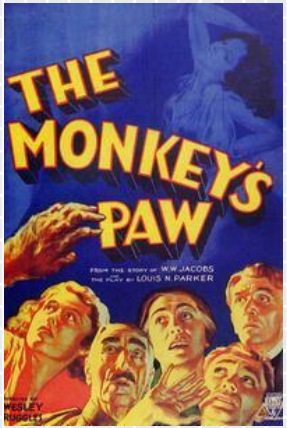
Example Cyber Deception Effects for Attacker and Defender

	Attacker	Defender
Fail to observe	Prevent the defender from detecting the attack.	Prevent the attacker from discovering their target.
Reveal	Trick the defender into providing access.	Trick the attacker into revealing their presence.
Waste Time	Focus the defender's attention on the wrong aspects of the incident.	Focus the attacker's efforts on the wrong target.
Underestimate	Induce the defender to think the attack is unsophisticated, not targeted.	Induce the attacker into thinking that the sought after thing is not here.
Disengage	Induce the defender into thinking that the attack is contained or completed.	Induce the attacker into thinking that their have already achieved their goal.
Misdirect	Focus the defender on a different attacker.	Encourage the attacker to target a different victim.
Misattribute	Induce the defender into thinking that the attacker is someone else.	Induce the attacker into thinking that they've compromised the wrong network.

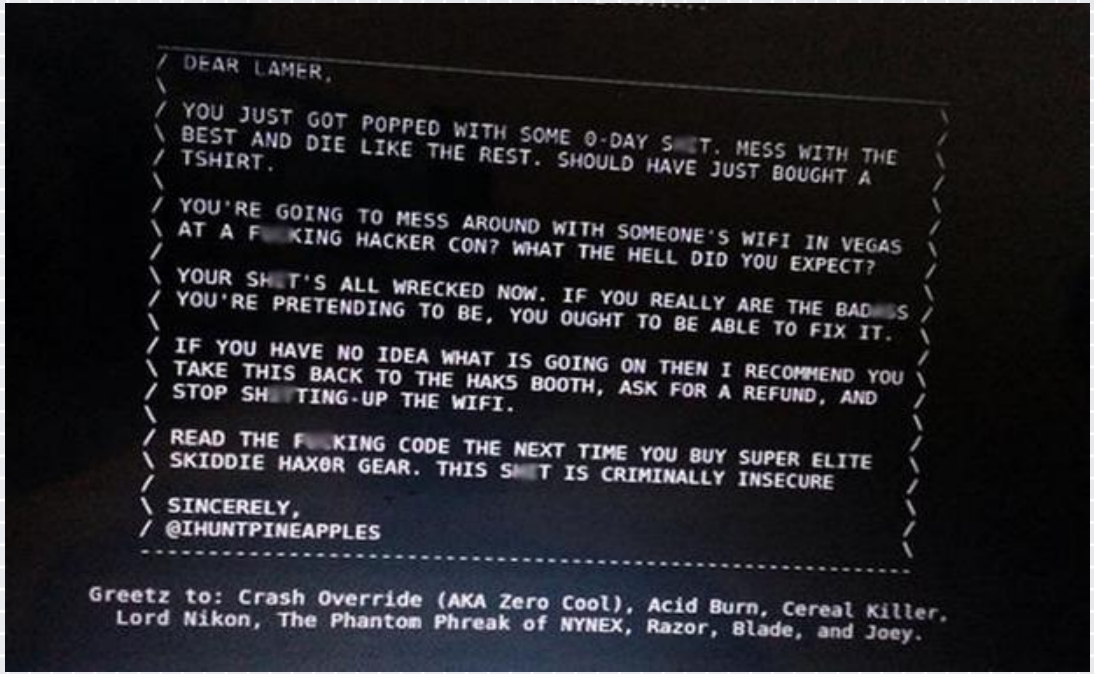
Deception Maxims







Secure Your Deception!



What is Threat Intelligence?

00dbb9e1c09dbdafb360f3163ba5a3de
00f24328b282b28bc39960d55603e380
0115338e11f85d7a2226933712acaae8
0141955eb5b90ce25b506757ce151275
0149b7bd7218aab4e257d28469fddb0d
016da6ee744b16656a2ba3107c7a4a29
01e0dc079d4e33d8edd050c4900818da
024fd07dbdacc7da227bede3449c2b6a
0285bd1fbdd70fd5165260a490564ac8
02a2d148faba3b6310e7ba81eb62739d
02c65973b6018f5d473d701b3e7508b2

aoldaily.com
aolon1ine.com
applesoftupdate.com
arrowservice.net
attnpower.com
aunewsonline.com
avvmail.com
bigdepression.net
bigish.net
blackberrycluter.com
blackcake.net

12.38.236.32
71.6.141.230
72.240.45.65
203.231.234.23
202.64.109.187
223.25.233.36

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

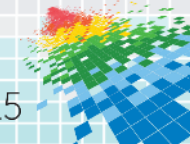
- Accuracy
- Timeliness
- Usability
- Completeness
- Precision
- Reliability

Additional Criteria

- Relevant
- Predictive
- Tailored

- Commanders' Considerations include
- Reducing operational uncertainty
- Determine appropriate balance between time alloted 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.

DRAWBRIDGE NETWORKS



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.

*** JP 1-02, DoD Dictionary of Military and Associated Terms, 8 Nov. 2010, available at http://www.dtic.mil/doctrine/**

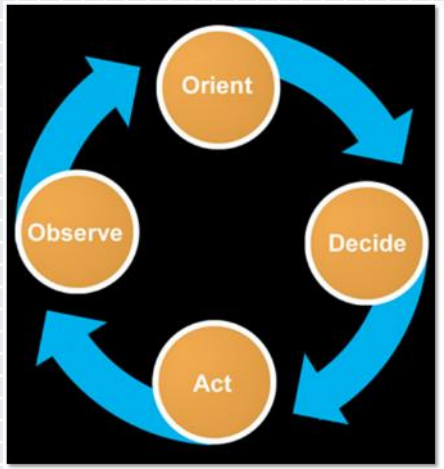
Risk Analysis

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*

- Based on work by COL John Boyd, USAF
- Observation and Orientation (OO) increases your perceptive boundaries.
- Sampling Rate of the OO is relative to the rate of 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.
- 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

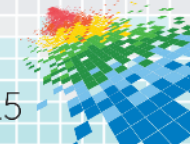
Targeting Methodology

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)



Deconstructing Adversary Doctrine

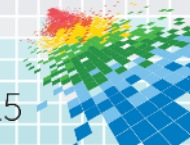
- Timothy Thomas' trilogy and Chinese Information Warfare doctrine, published by the Army's Foreign Military Studies Office at Fort Leavenworth.
  - *Dragon Bytes*, 2003
  - *Decoding the Virtual Dragon*, 2007
  - *The Dragon's Quantum Leap*, 2009

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

Apply what you have learned today:

- Near Term:
  - Dig deeper into sources on relevant doctrine referenced here
  - Read a book on foreign adversary doctrine

- Within the next six months:
  - Apply OPSEC principles to your defensive posture
  - Look at creating deceptive features within your network that can help identify sophisticated, targeted attackers
  - Consider the depth of your threat intelligence analysis process
  - Examine your incident response team's OODA loop.



Backup Slides:

DRAWBRIDGE NETWORKS

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
- Cyber Defense Review: http://www.cyberdefensereview.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/