What Would You Do With a Nation-State Cyber Army?

Gregory Conti / Director of Research / IronNet Cybersecurity / @cyberbgone

Disclaimer

The views in this talk are those of the speaker and do not reflect the policy or position of his current or former employers, which include IronNet Cybersecurity, the U.S. Department of Defense and the U.S. Army.

http://www.indiana.edu/~f351jmcd/Images/elle2.jpg

Disclaimer

The views in this talk are those of the speaker and do not reflect the policy or position of his current or former employers, which include IronNet Cybersecurity, the U.S. Department of Defense and the U.S. Army.

http://www.indiana.edu/~f351jmcd/Images/elle2.jpg

Disclaimer

The views in this talk are those of the speaker and do not reflect the policy or position of his current or former employers, which include IronNet Cybersecurity, the U.S. Department of Defense and the U.S. Army.

http://www.indiana.edu/~f351jmcd/Images/elle2.jpg

Army, Navy cyber teams say they're ready to go ... a year early

By: Mark Pomerleau November 2

Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West

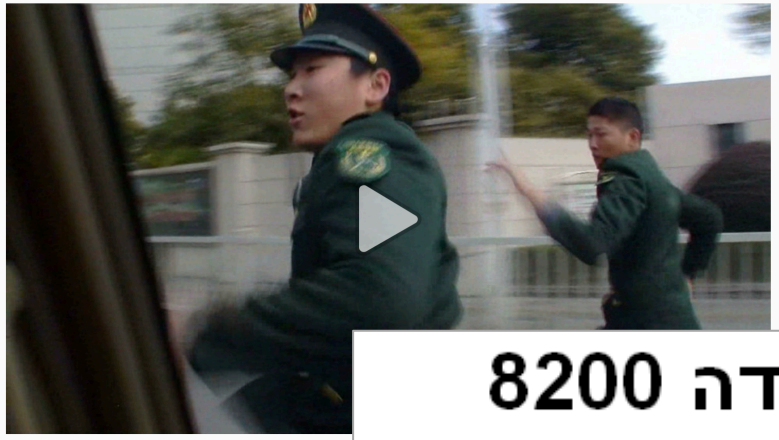
Ju-min Park, James Pearson 7 MIN READ

SEOUL (Reuters) - North Korea's main spy agency has a special cell called Unit 180 that is likely to have launched some of its most daring and successful cyber attacks, according to defectors, officials and internet security experts.

What we know about the Chinese army's alleged cyber spying unit

By Zoe Li, CNN

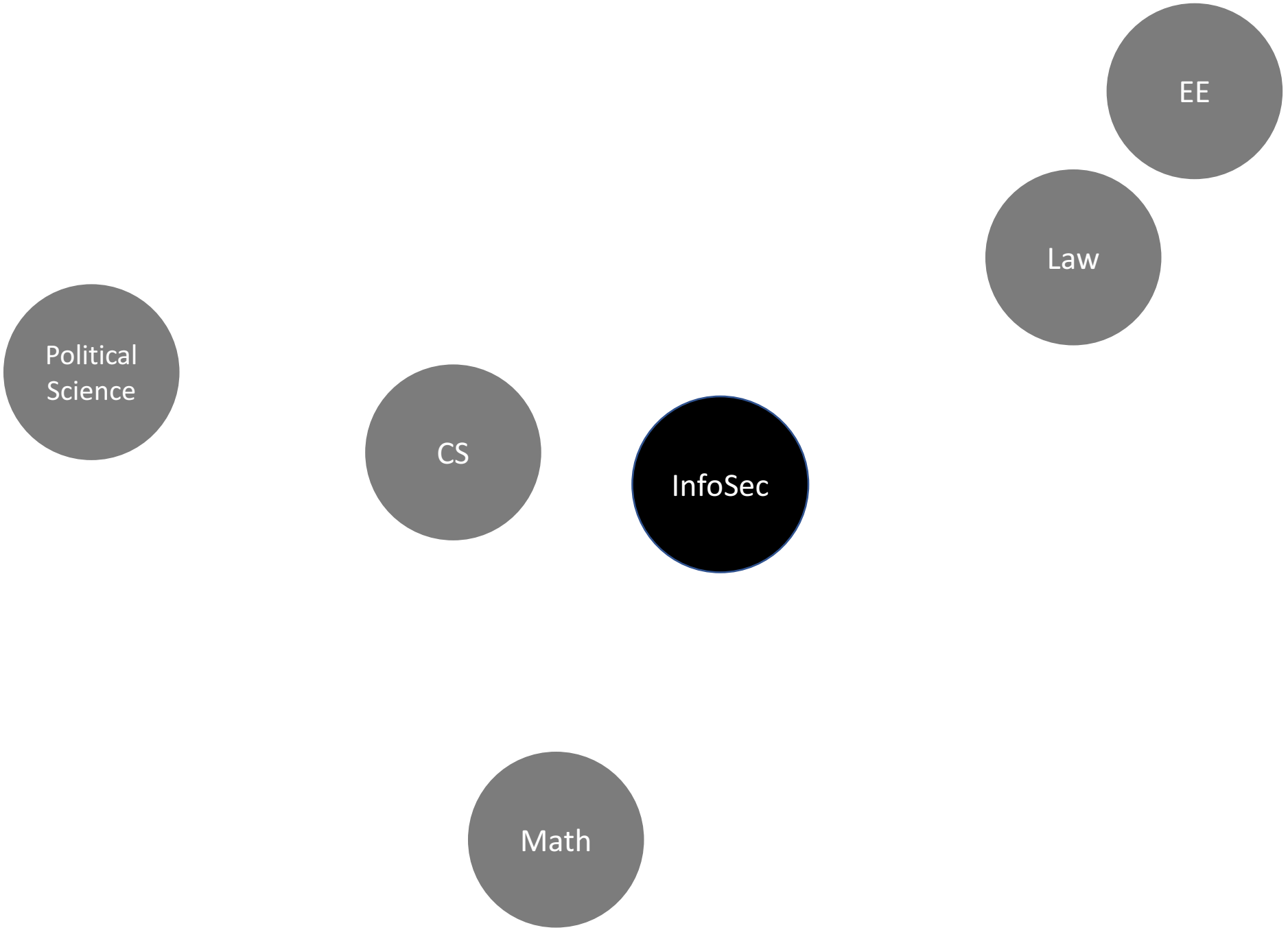
Updated 5:11 AM ET, Tue May 20, 2014

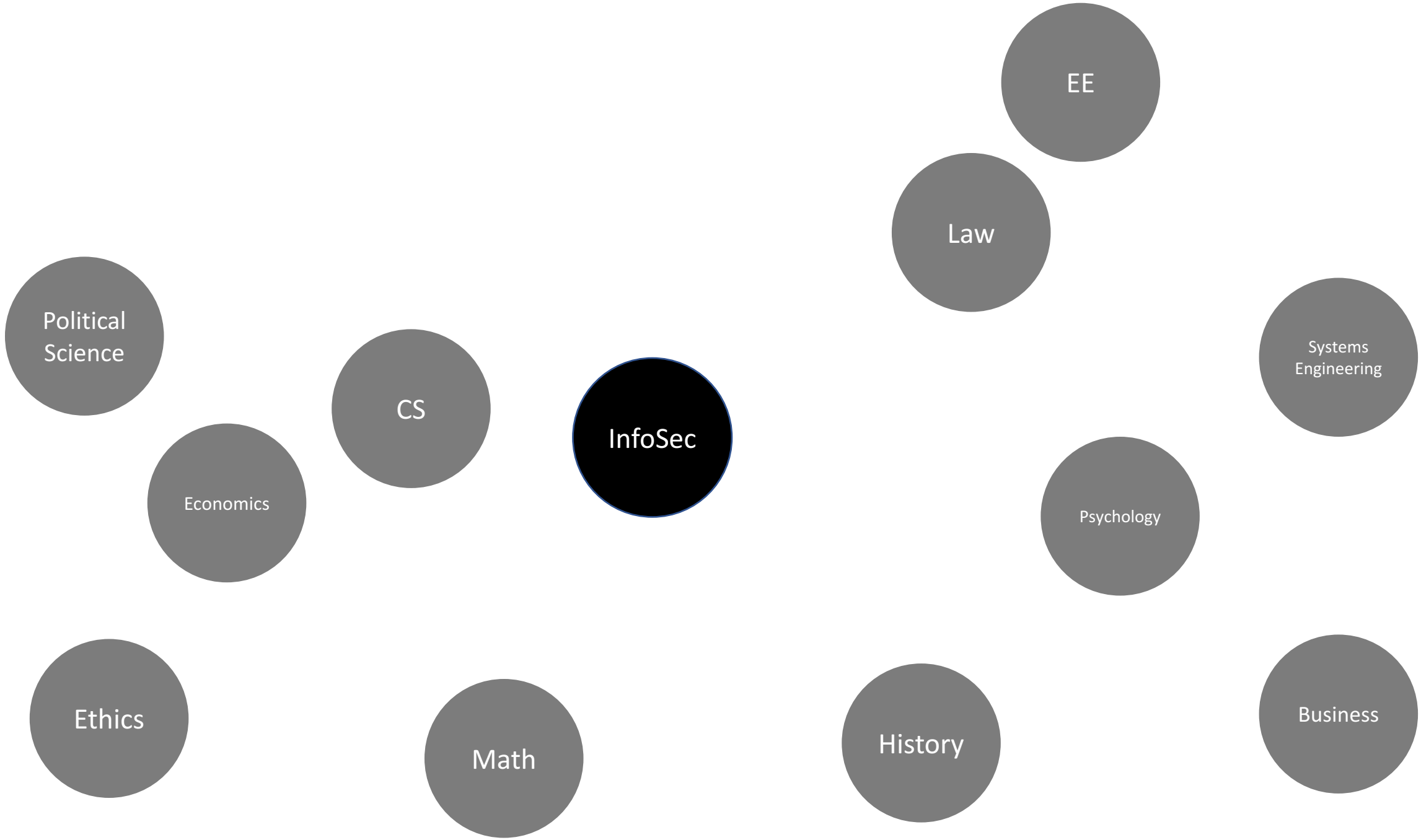


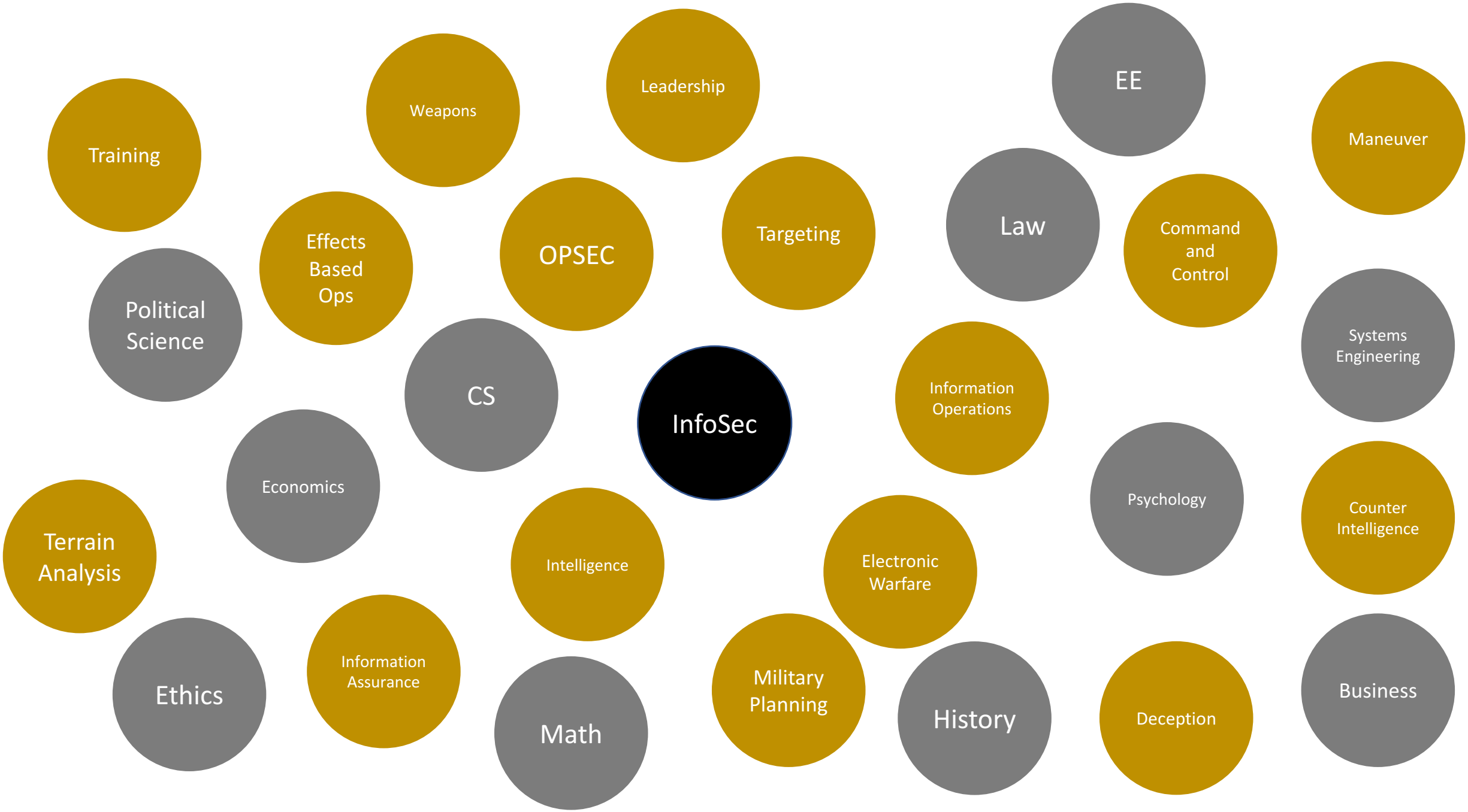
יחידה 8200

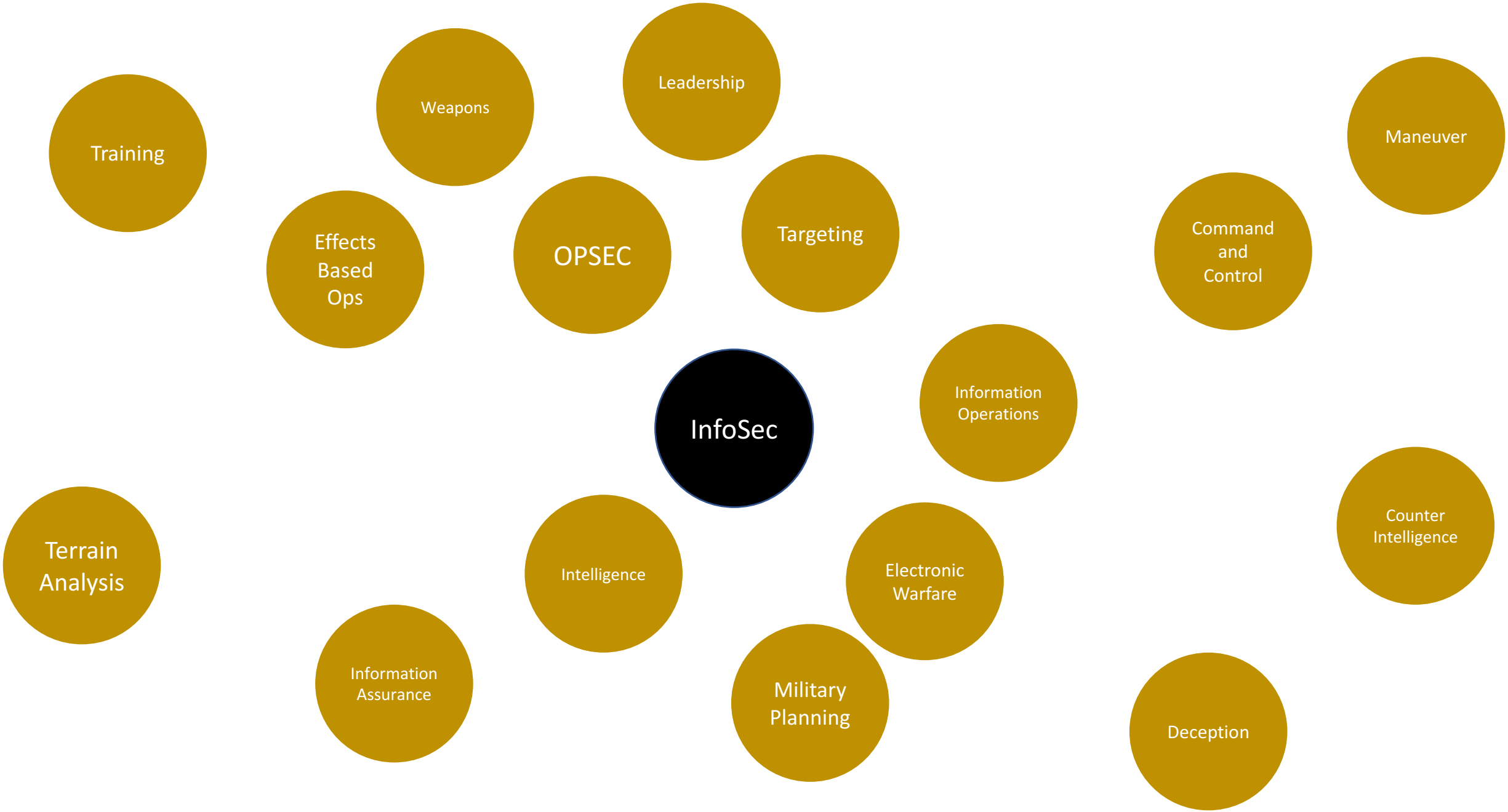
http://www.tlvfaces.com/wp-content/uploads/2013/09/8200.png
http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html
https://www.iranhumanrights.org/wp-content/uploads/IranCyberArmy-1.jpg
https://www.crowdstrike.com/blog/wp-content/uploads/2016/09/FancyBearBlog.jpg
https://www.c4isrnet.com/dod/2017/11/02/army-navy-cyber-teams-say-theyre-ready-to-go-a-year-early
https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020

From 2000 to 2009: Birth of “Cyber”

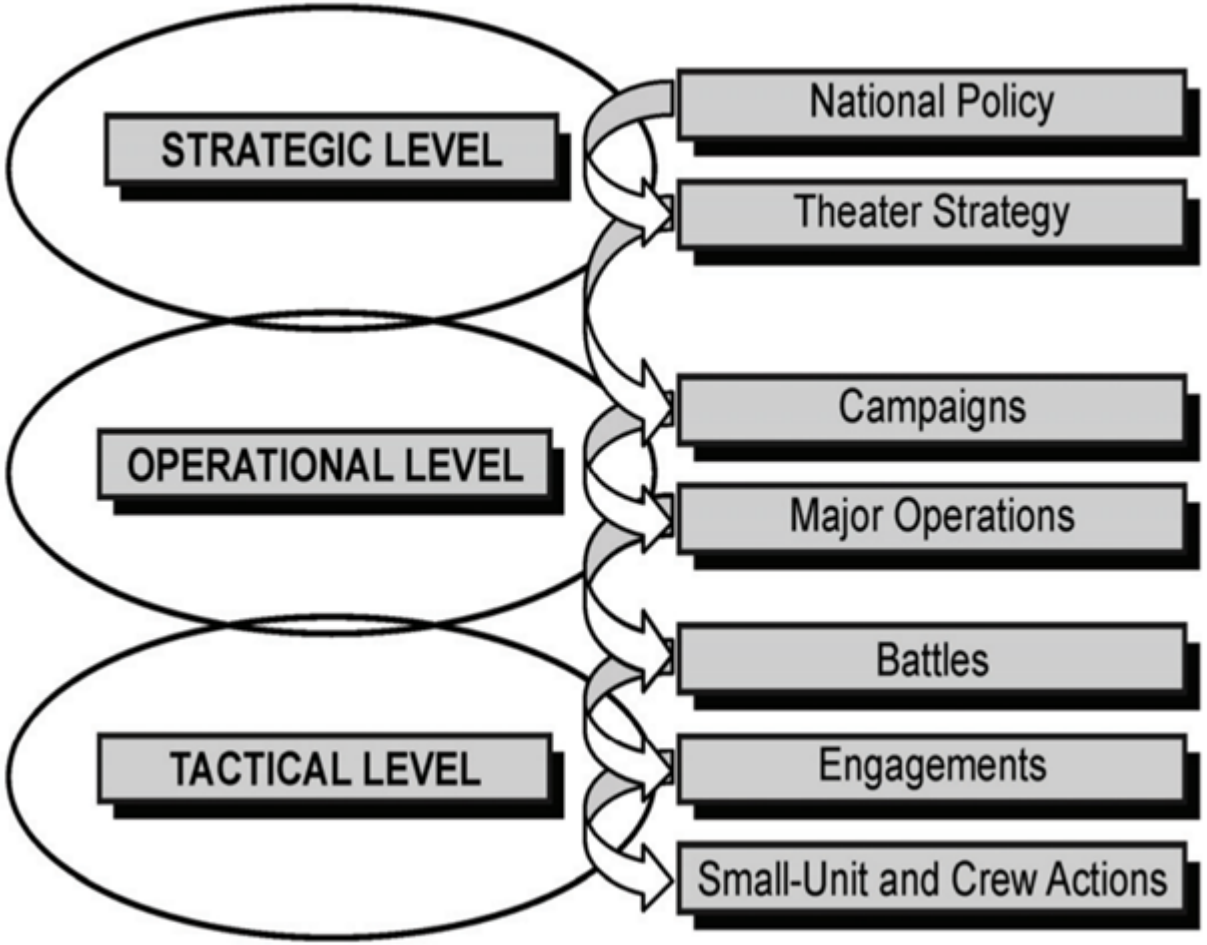

EE
Law
Political Science
CS
InfoSec
Math


EE
Law
Political Science
CS
InfoSec
Systems Engineering
Economics
Psychology
Ethics
Math
History
Business

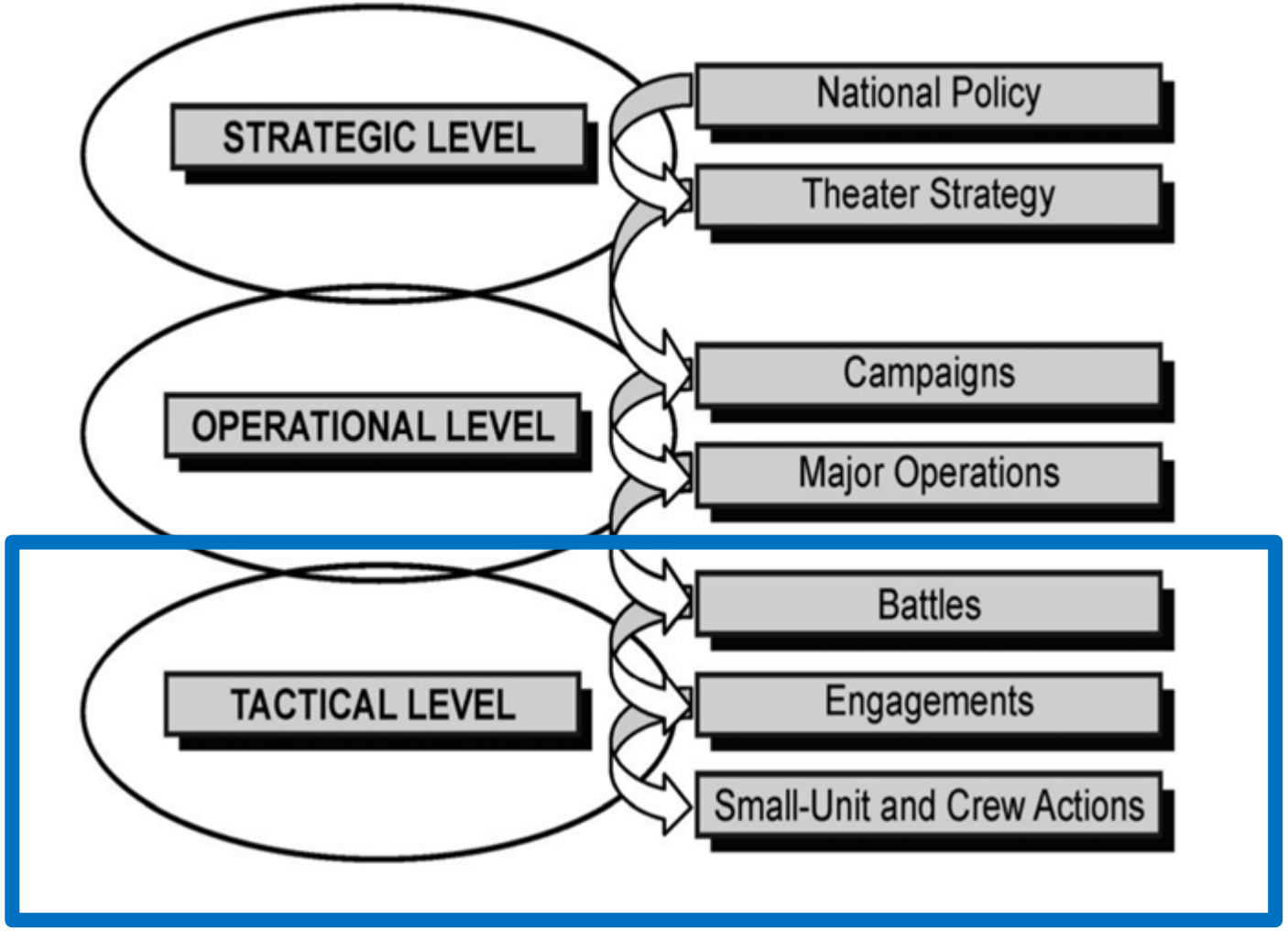

Training
Weapons
Leadership
EE
Maneuver
Effects Based Ops
OPSEC
Targeting
Law
Command and Control
Political Science
CS
InfoSec
Information Operations
Systems Engineering
Economics
Psychology
Terrain Analysis
Intelligence
Electronic Warfare
Counter Intelligence
Ethics
Information Assurance
Math
Military Planning
History
Deception
Business


Training
Weapons
Leadership
Maneuver
Effects Based Ops
OPSEC
Targeting
Command and Control
InfoSec
Information Operations
Terrain Analysis
Intelligence
Electronic Warfare
Counter Intelligence
Information Assurance
Military Planning
Deception

Levels of War

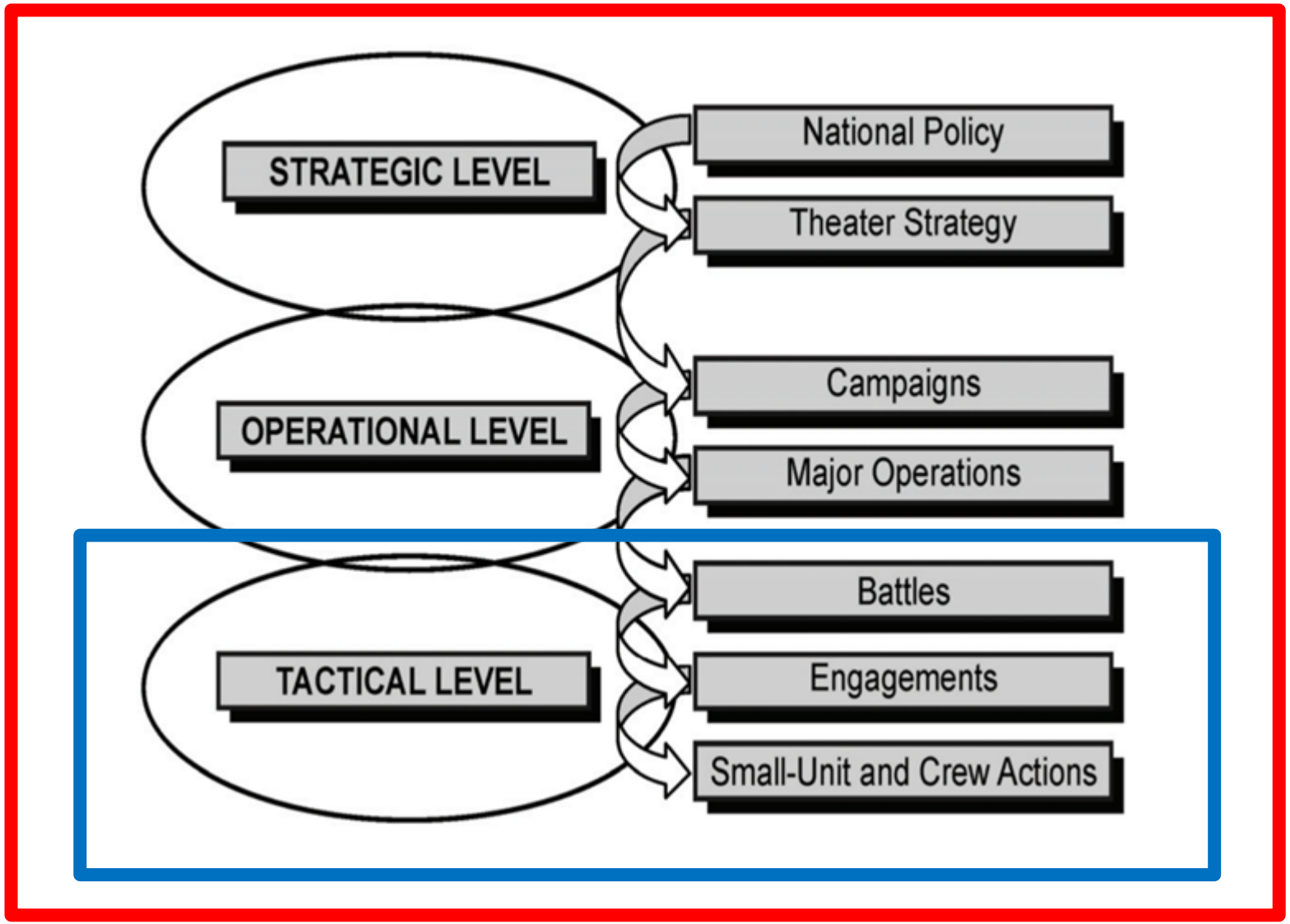


Levels of War



Much of InfoSec

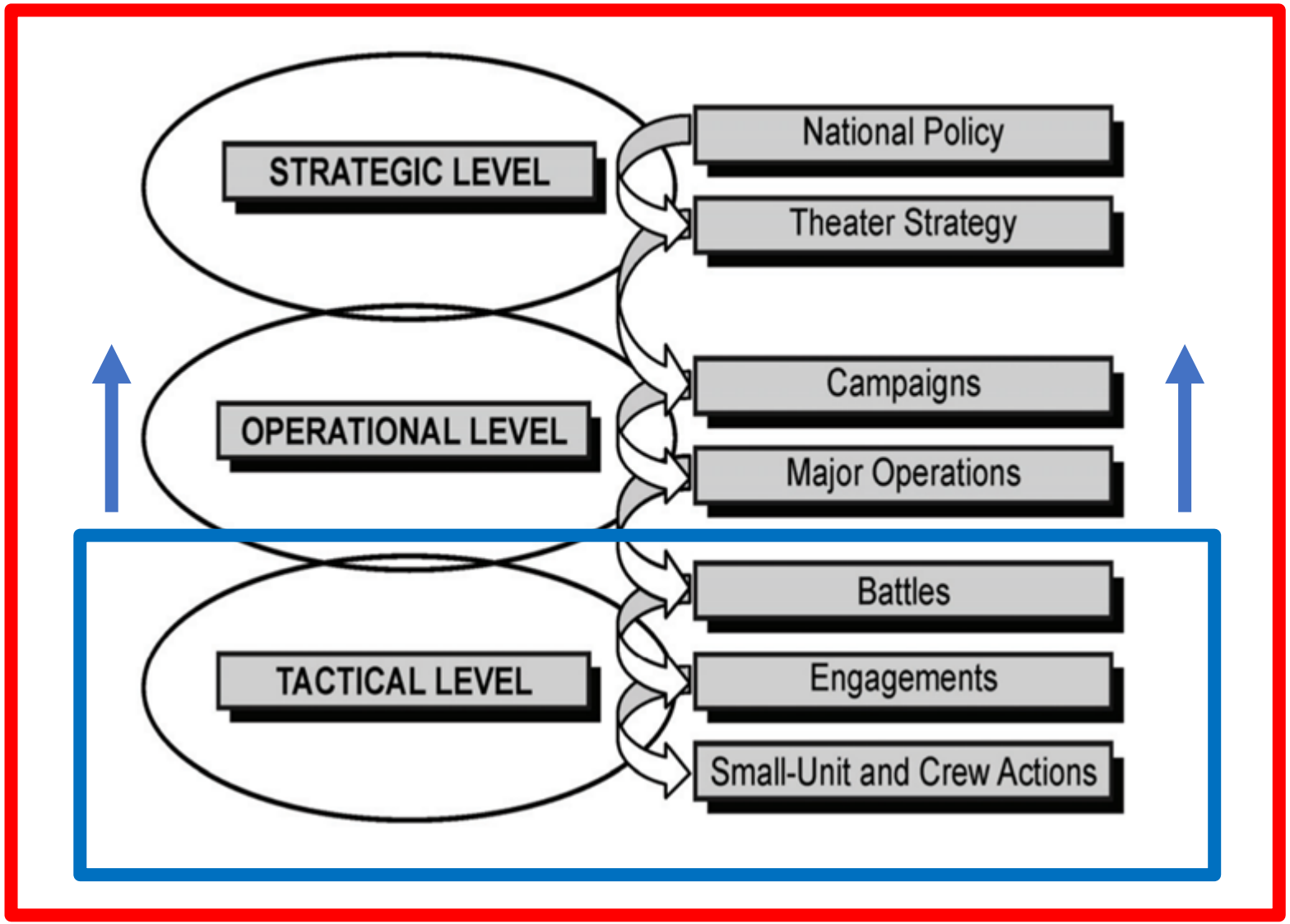
Levels of War



Nation-States

Much of InfoSec

Levels of War



Nation-States

Much of InfoSec

A Cyber Army of Today

United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

http://www.arcyber.army.mil/Pages/ArcyberHome.aspx

A Cyber Army of Today

United States Army Cyber Command directs and conducts integrated **electronic warfare, information and cyberspace operations** as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

http://www.arcyber.army.mil/Pages/ArcyberHome.aspx

A Cyber Army of Today

United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to **ensure freedom of action in and through cyberspace and the information environment**, and to deny the same to our adversaries.

http://www.arcyber.army.mil/Pages/ArcyberHome.aspx

A Cyber Army of Today

United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, **and to deny the same to our adversaries**.

http://www.arcyber.army.mil/Pages/ArcyberHome.aspx

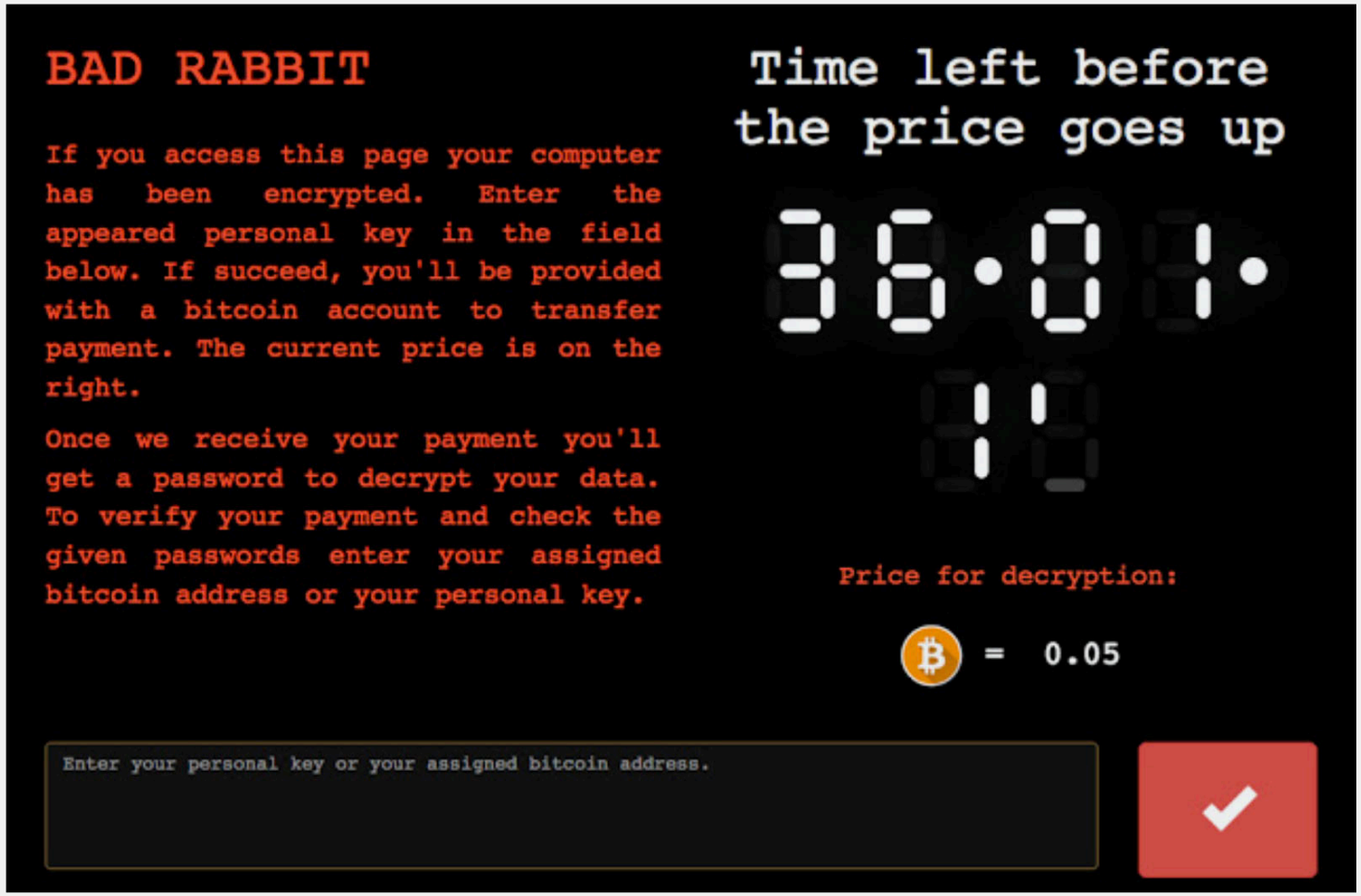
And We See the Effects…

http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Bad Rabbit used NSA “EternalRomance” exploit to spread, researchers say

EternalRomance exploit was used to move across networks after initial attack.

SEAN GALLAGHER - 10/26/2017, 11:37 AM




EQUIFAX®

Heart of Texas
Page Liked · 12 hrs ·

155th anniversary of Virginia secession from the U.S.

The Virginia Convention of 1861, also known later as the Secession Convention, convened on February 13, 1861, on the eve of the American Civil War (1861–1865), to consider whether Virginia should secede from the United States.

Its 152 delegates, a majority of whom were Unionist, had been elected at the behest of the Virginia General Assembly. Eventually the momentum turned toward secession, and the convention voted on April 17 to leave the Union. Virginians expressed their agreement at the polls on May 23. The state had joined the Confederacy.

The secession initiative, first and foremost, was perfectly legal and Constitutional. Technically, Viriginia had no other choice as the state couldn't put up with the lawlessness of the federal authorities. Both back then and today many southern states have enough reasons for secession. Feds don't protect states from illegal immigrants, they try to rob Americans of their Constitutional right to bear arms, don't hesitate to stick to land grabbing (Red River issue), impose gay marriages and...well, the list goes on.

What we all are facing are 4 years of Hillary's presidency. I guess it's about time Texans did realize secession is the only option left. We should leave the Union of lies and show the way for the other Southern states.
Let's do that until it's still legal to say "secession" and "Confederacy" and fly the Texas flag. Come and take it, Washington.

Like Comment Share

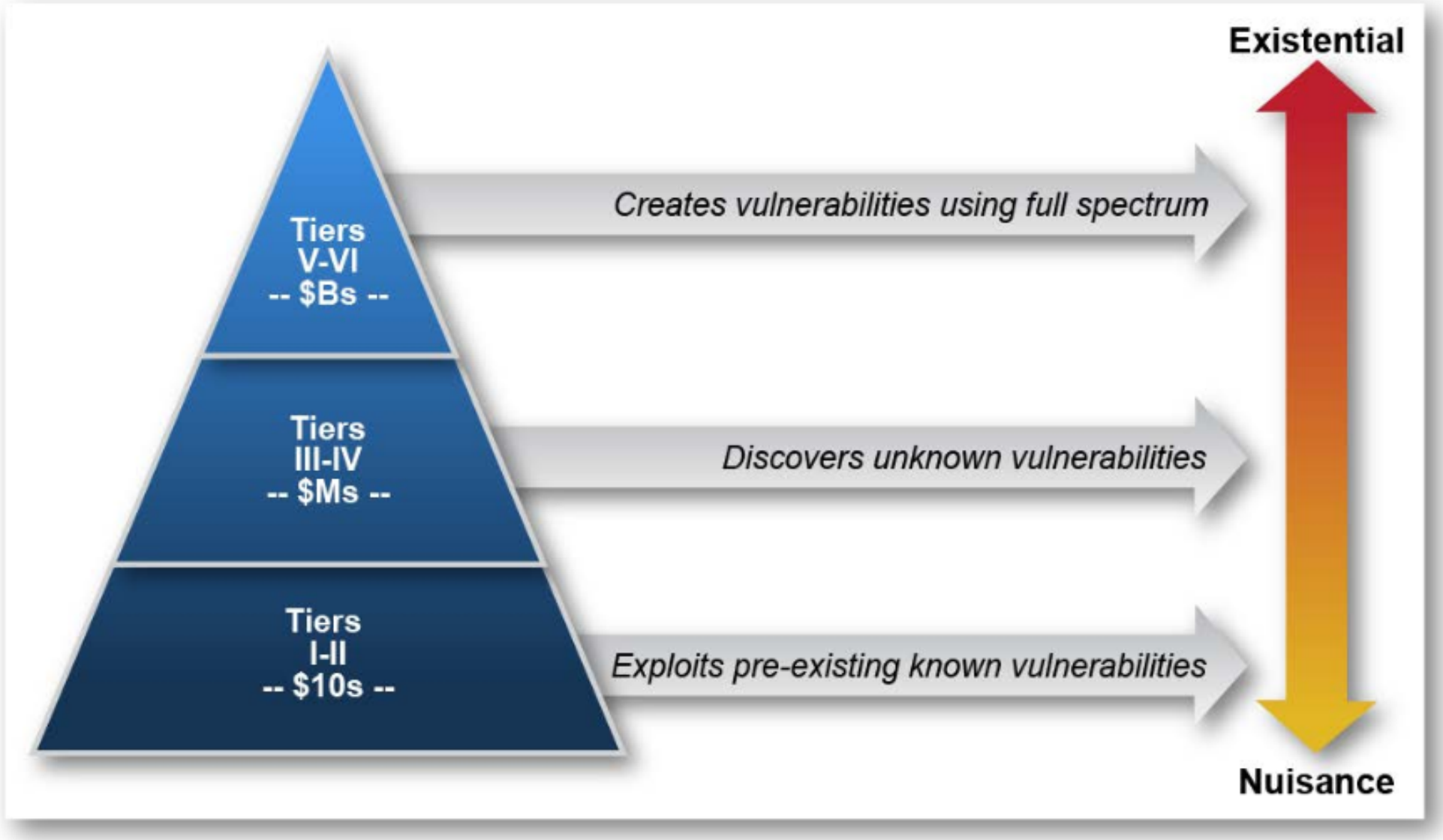
861 Top Comments

315 shares 48 comments

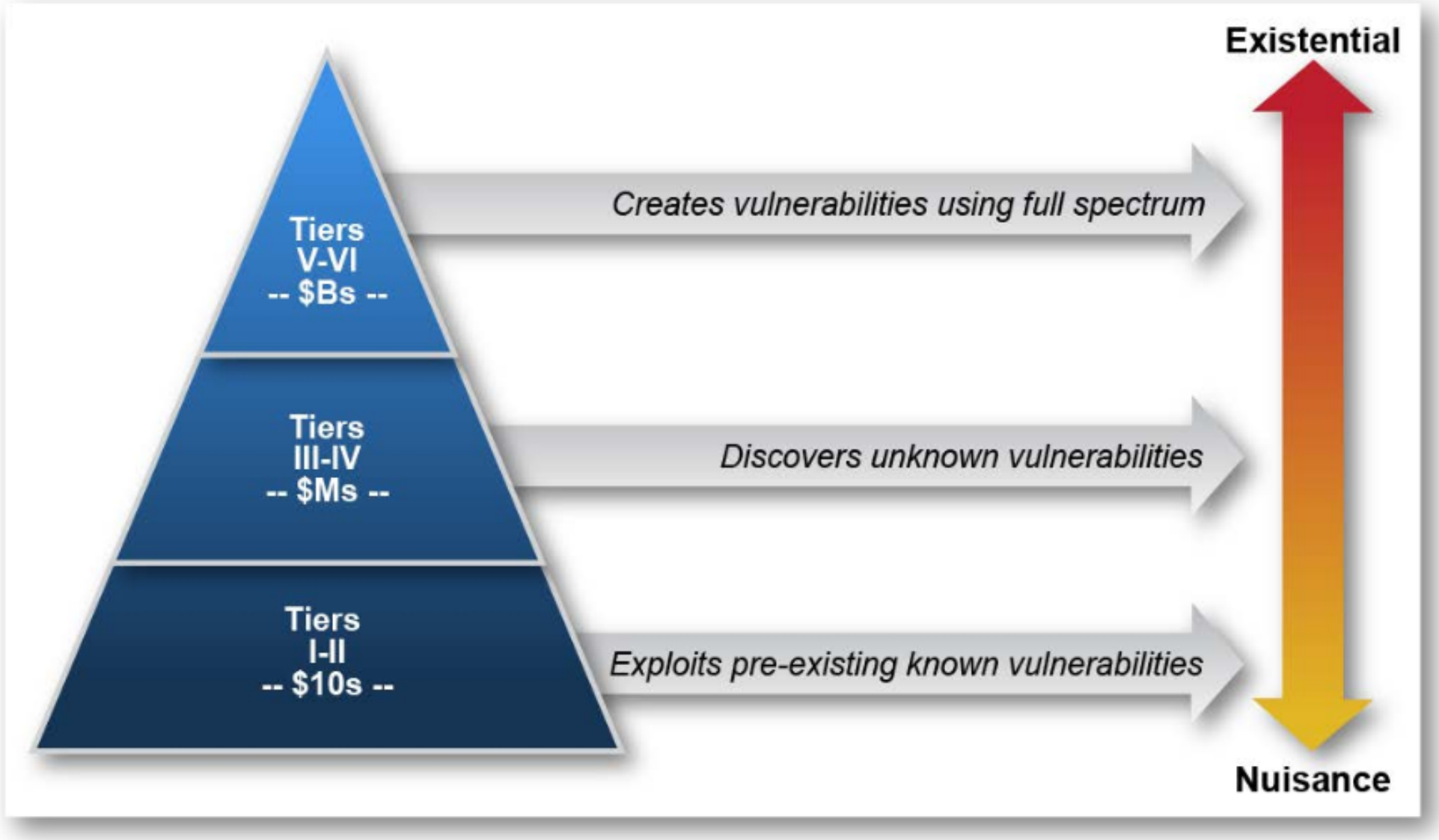
Stephen W Peel The Civil War wasn't about slavery it was about States rights. Slavery was already on

http://www.philly.com/philly/news/politics/presidential/facebook-russia-fake-posts-trump-election-clinton-20171006.html

https://www.nps.gov/feha/planyourvisit/images/Donald_Trump_swearing_in_ceremony.jpg



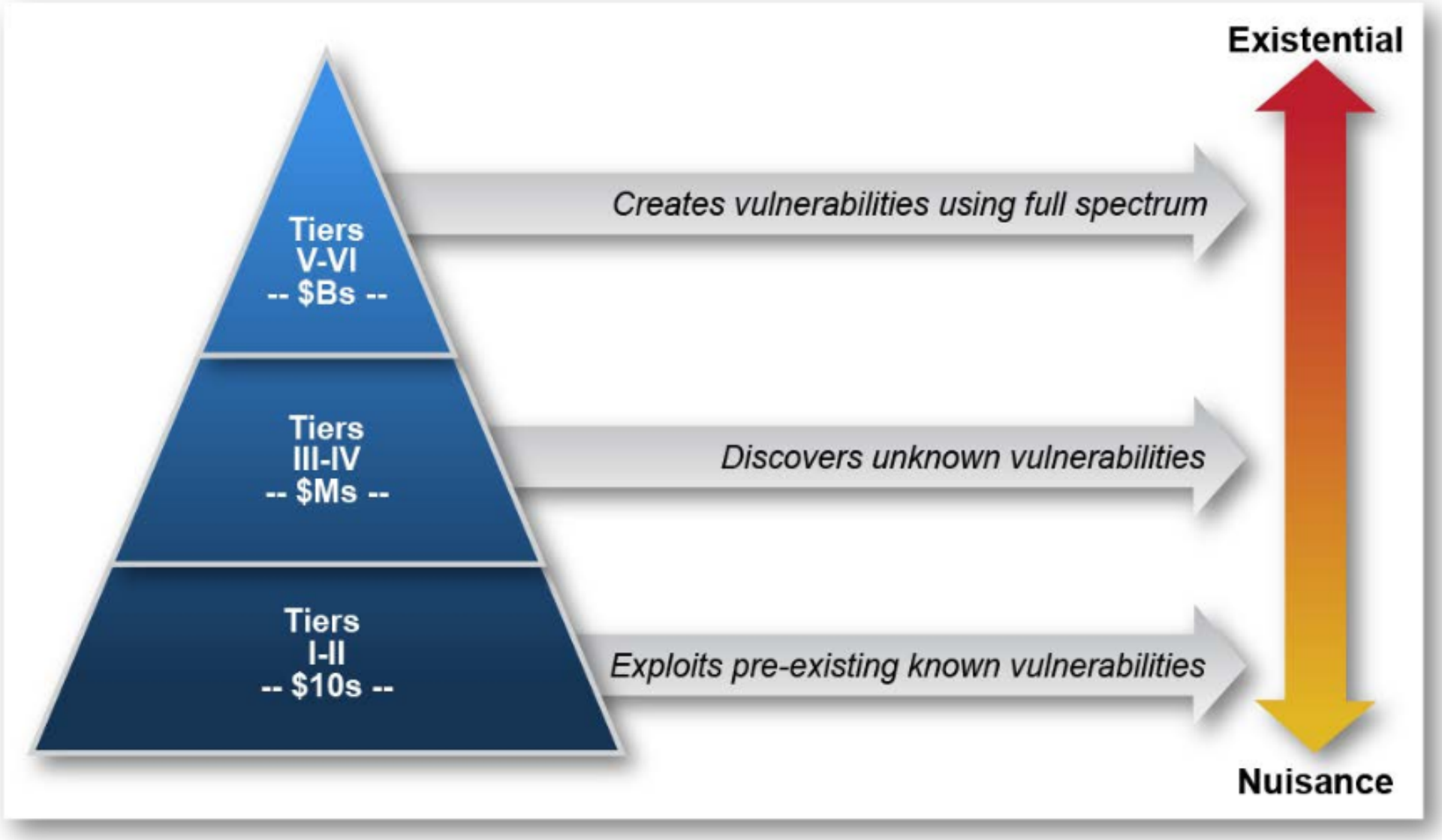
"Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, January 2013.



Much of InfoSec

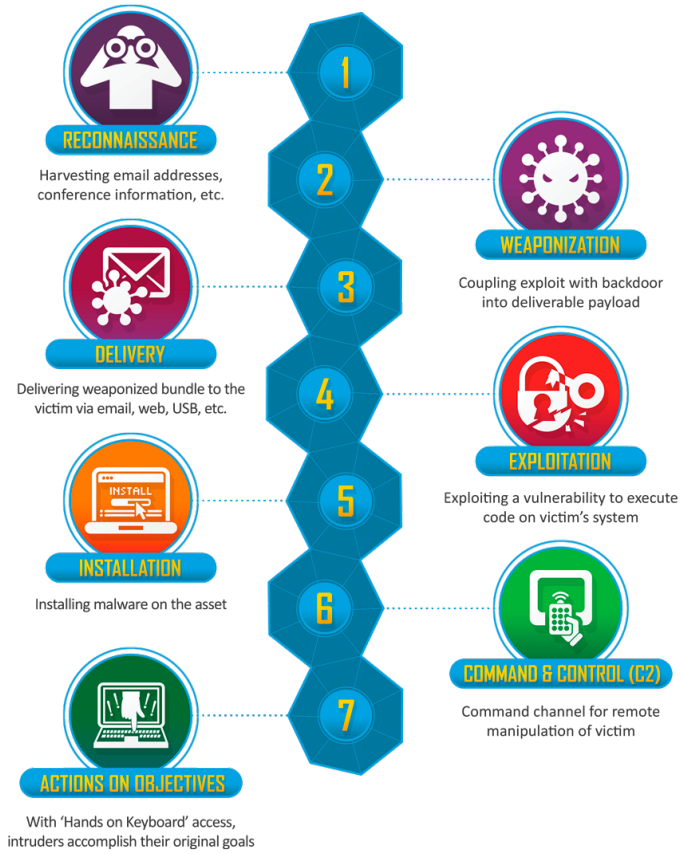
"Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, January 2013.

Nation-state Cyber Forces

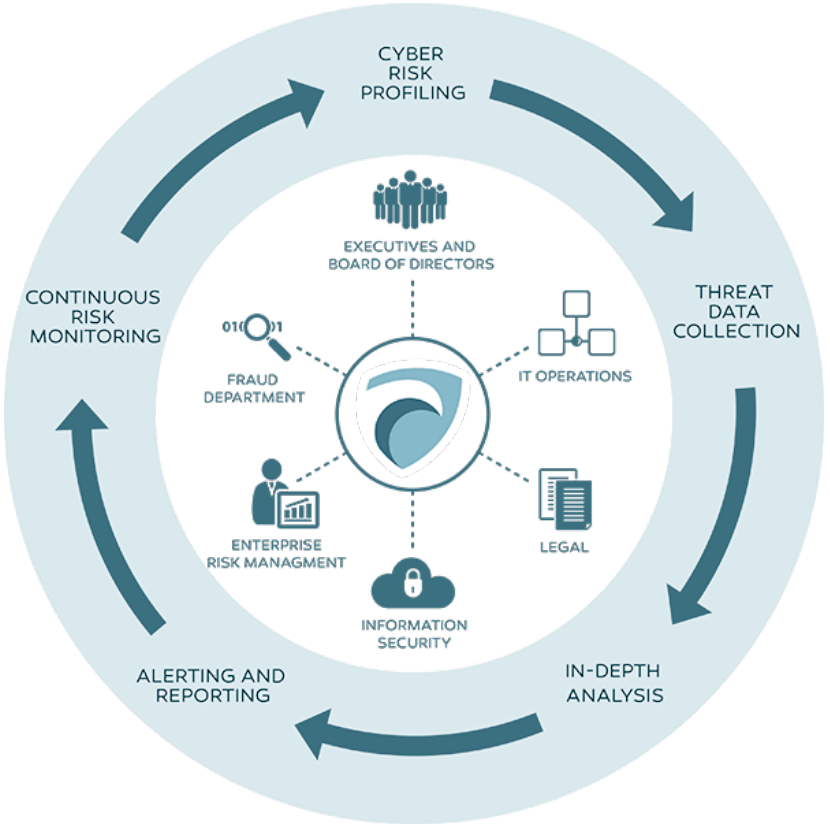


"Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, January 2013.

Military Thinking Adopted in Cybersecurity

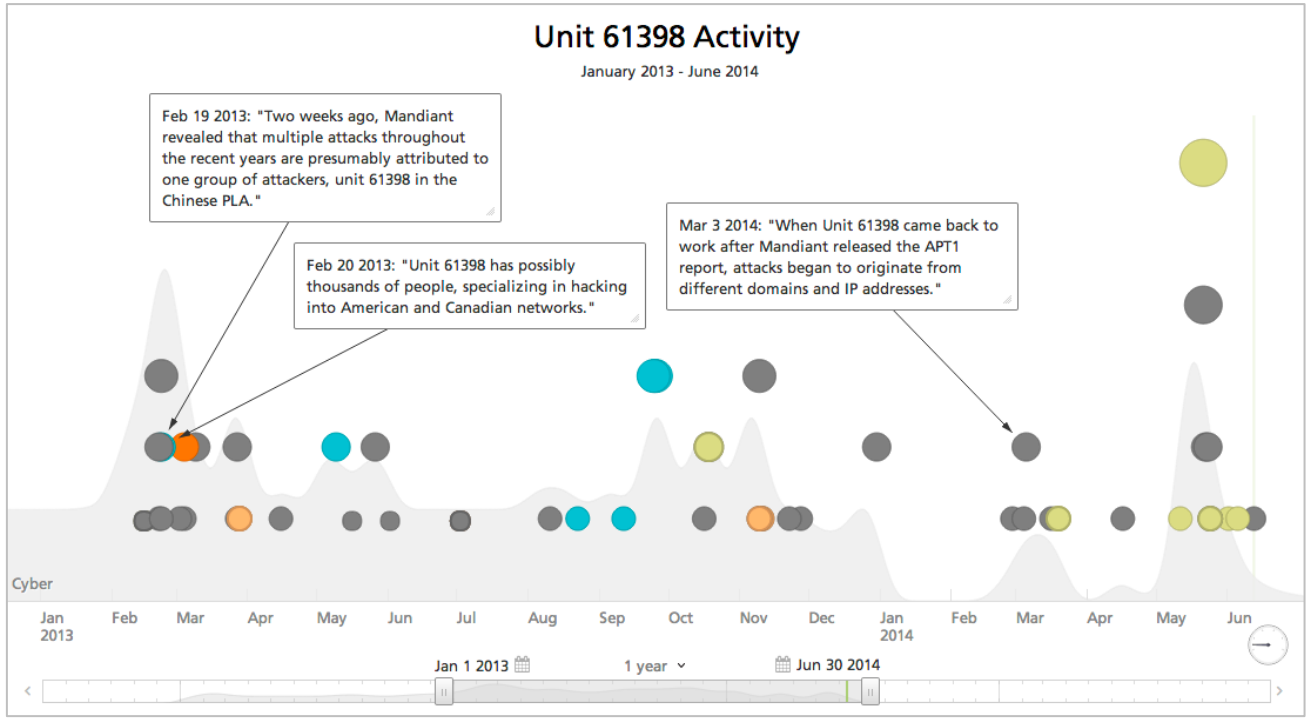


Kill Chain



Threat Intelligence

https://www.surfwatchlabs.com/threat-intelligence-products/purchase
https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html



Campaigns

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.

42

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

TTPs

https://www.recordedfuture.com/assets/attacker-landscape-61398-timeline.png
http://slideplayer.com/slide/4255725/14/images/43/Risk+Analysis+Intel+Gain/Loss+Calculus+@%25.jpg

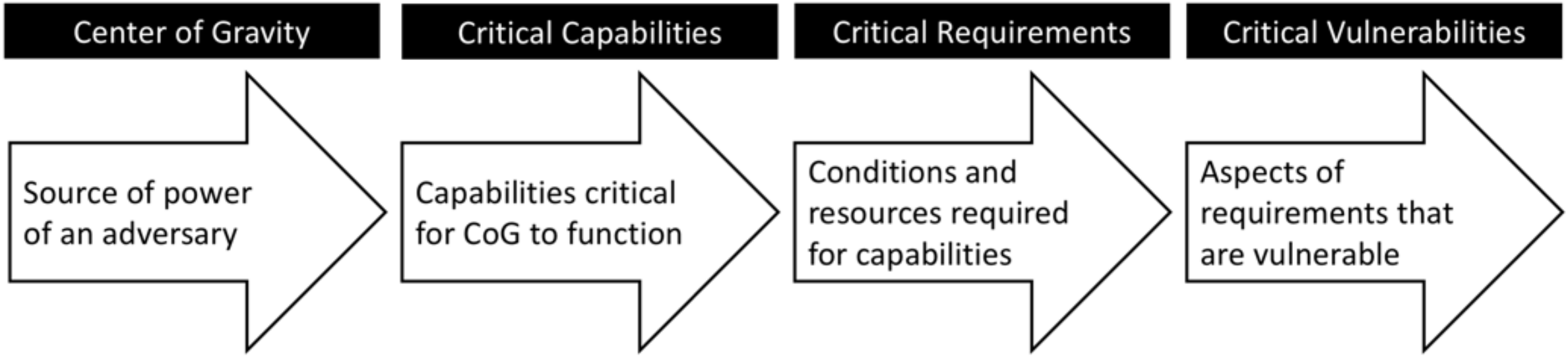
Two-star: Every soldier must be a cyber defender

By: Kathleen Curthoys October 22

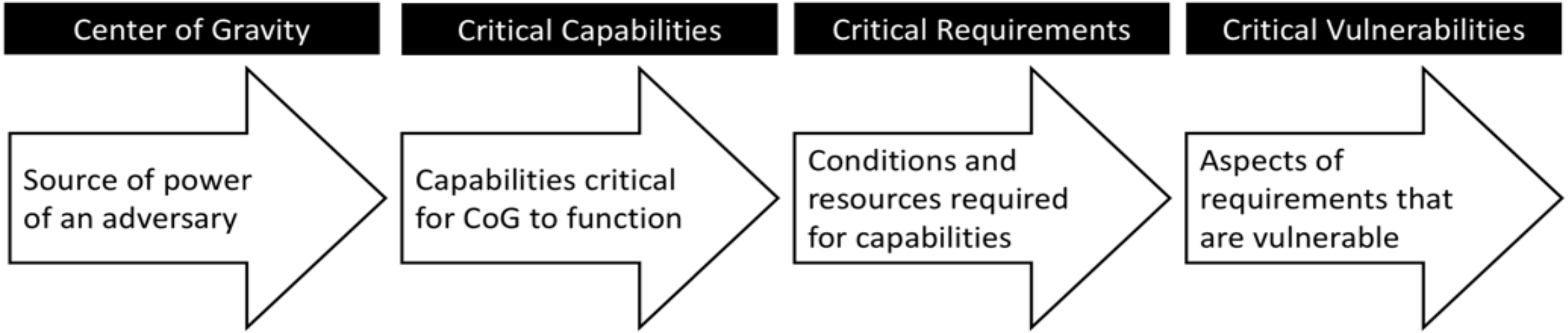
Maj. Gen. Patricia Frost leads the Army Cyber Directorate, which stood up last year to integrate cyber, electronic warfare and information operations. (Alan Lessig/Staff)

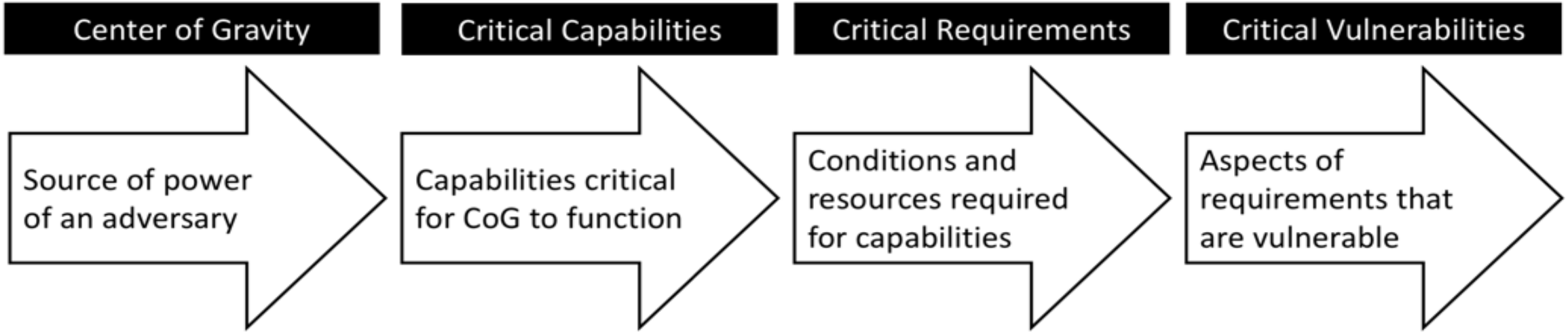
Examples…

Center of Gravity Analysis

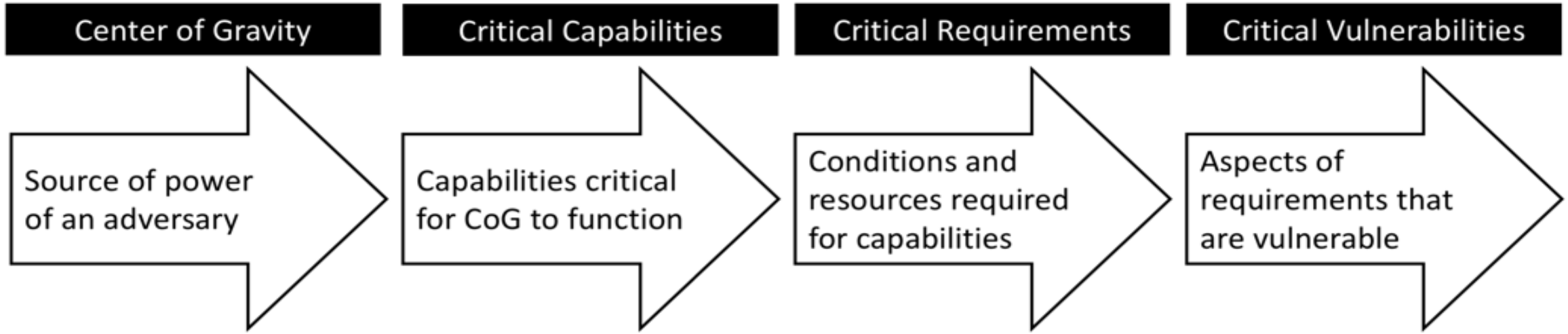


"a source of power that provides moral or physical strength, freedom of action, or will to act."


Center of Gravity
Critical Capabilities
Critical Requirements
Critical Vulnerabilities
Source of power of an adversary
Capabilities critical for CoG to function
Conditions and resources required for capabilities
Aspects of requirements that are vulnerable

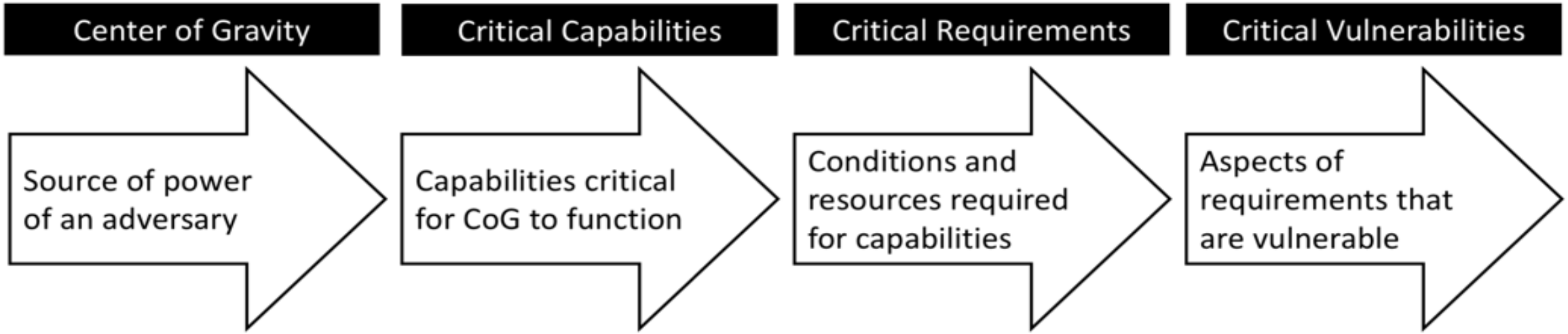

Center of Gravity
Critical Capabilities
Critical Requirements
Critical Vulnerabilities
Source of power of an adversary
Capabilities critical for CoG to function
Conditions and resources required for capabilities
Aspects of requirements that are vulnerable

Internet



Internet

Search
Hardware Supply Chain
Software Supply Chain
Internet Governance
WWW
Email
Protocols
Telecom Infrastructure



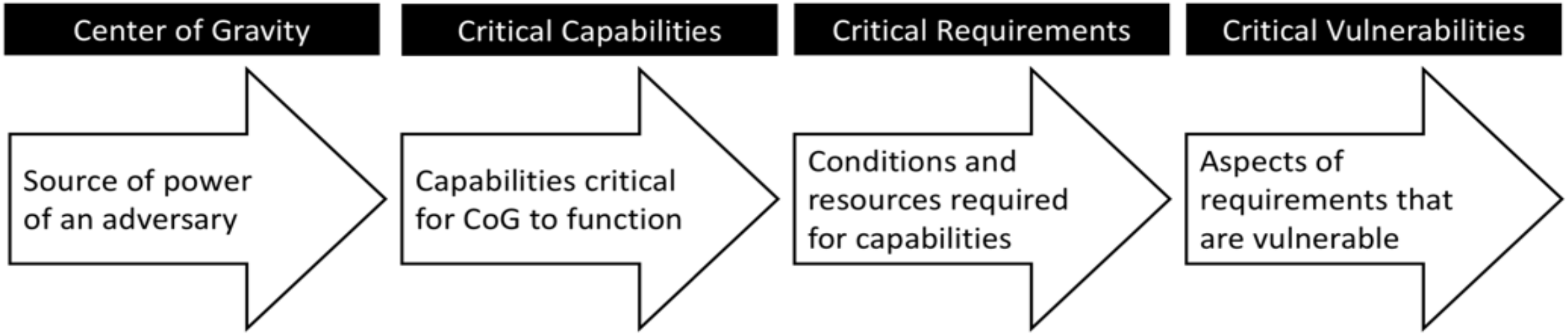
Internet

Search
Hardware Supply Chain
Software Supply Chain
Internet Governance
WWW
Email
Protocols
Telecom Infrastructure

Chip foundries
Chip design firms
Transportation
Warehousing

OS companies
Open source repositories
Open source developer communities
Software update mechanisms
App stores

Undersea cables
Communications satellites
EM spectrum



Internet

Search
Hardware Supply Chain
Software Supply Chain
Internet Governance
WWW
Email
Protocols
Telecom Infrastructure

Chip foundries
Chip design firms
Transportation
Warehousing

- Opaque nature of chip logic
- Warehouse physical security

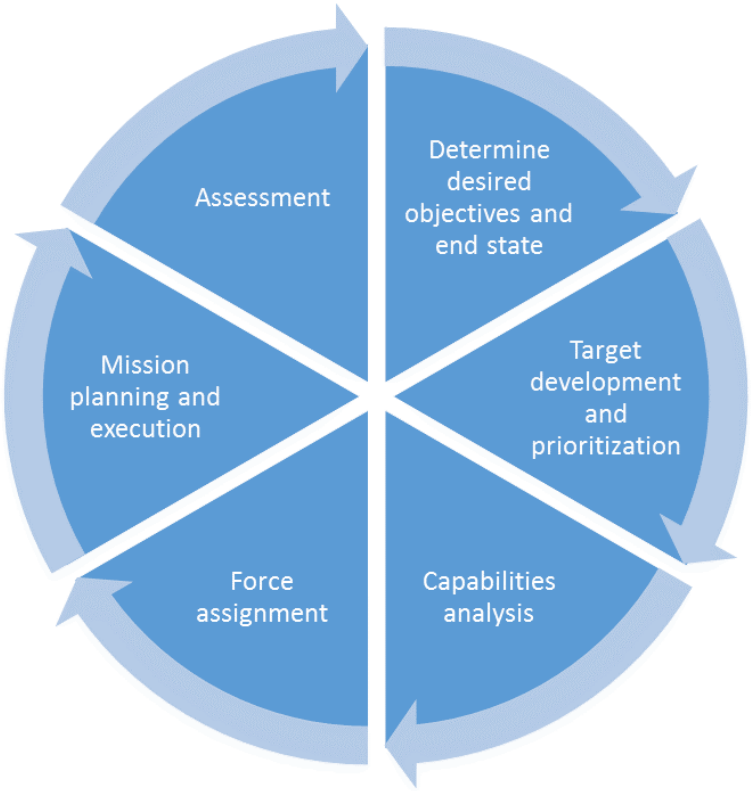
OS companies
Open source repositories
Open source developer communities
Software update mechanisms
App stores

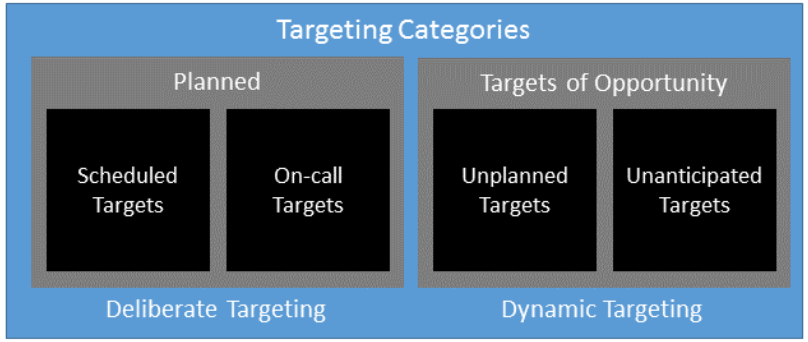
- Version control software
- Outdated hashing algorithms
- OS source code access
- App store code reviews

Undersea cables
Communications satellites
EM spectrum

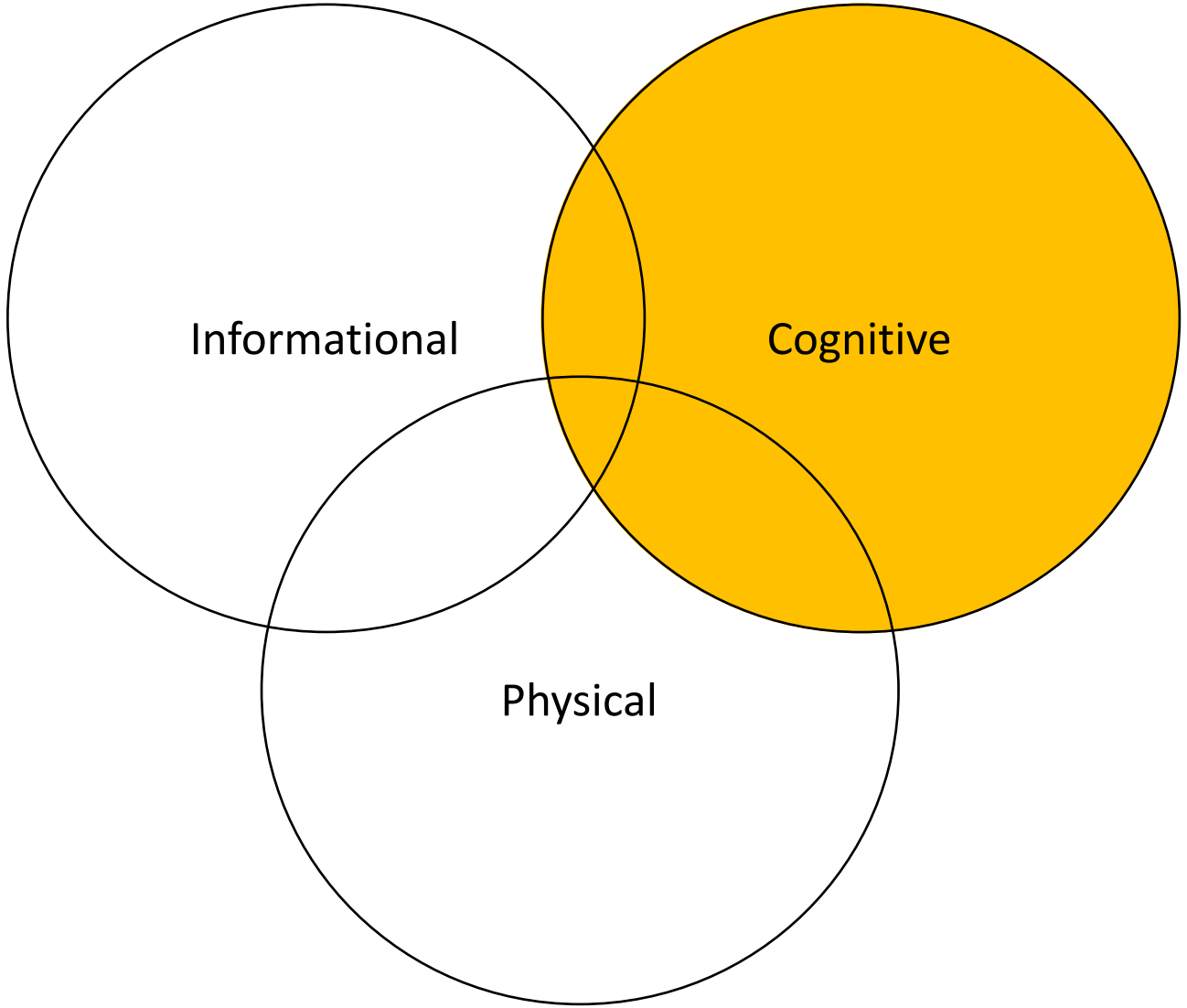
- Submarine access to undersea cables
- GPS jamming and spoofing

Fires and Targeting

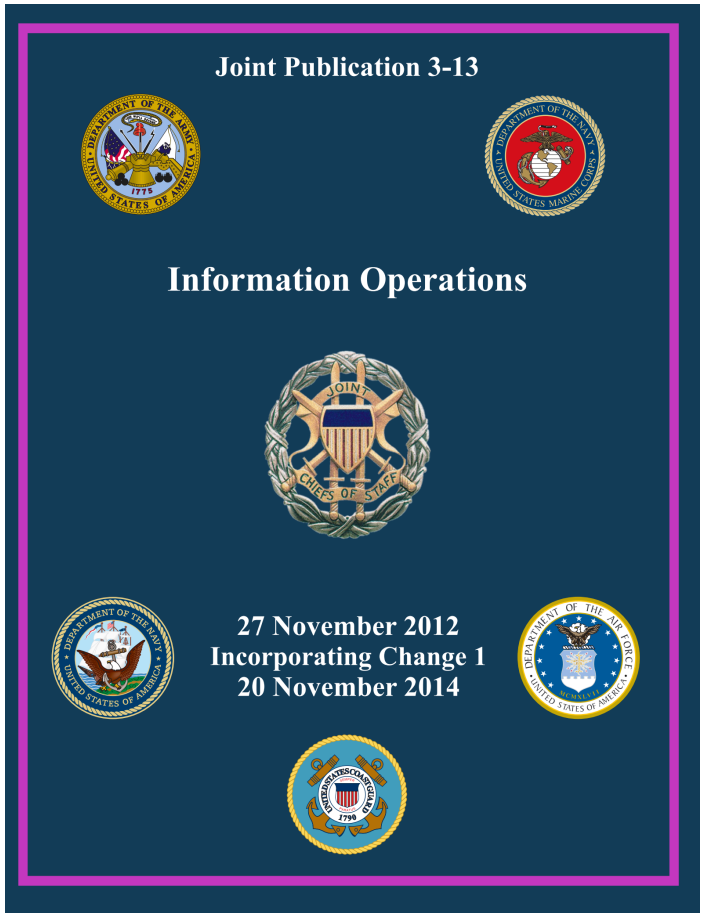




Domains



IO Defined



IO employs psychological operations (PSYOP), cyber operations, electronic warfare techniques, deception, and operations security (OPSEC) **to defend information and information systems, and to influence decision making.** Occurs in both peace and war.

Cyber Enabled IO

See…

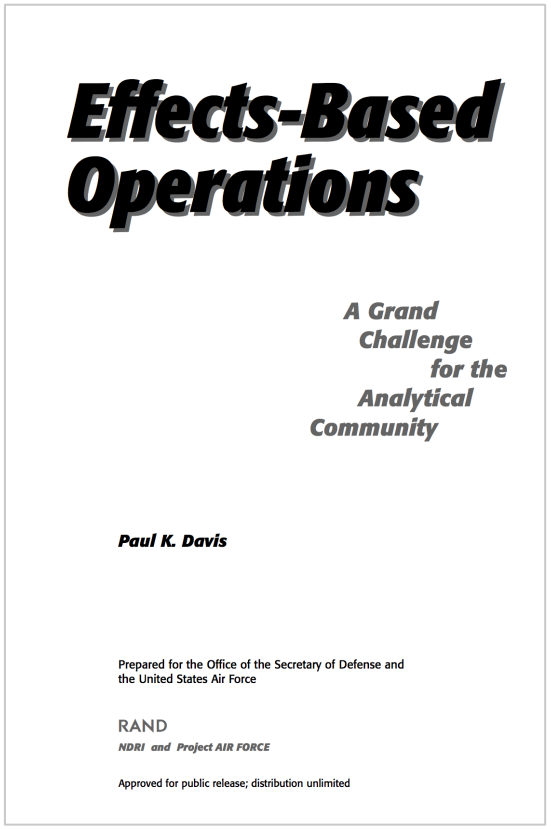
Herb Lin “On Cyber-Enabled Information/Influence Warfare and Manipulation,” Oxford Handbook of Cybersecurity, 2018 (Forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680

http://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-us-forces-evacuation-fake-message-trump-kim-jong-un-latest-a7961766.html

Intelligence Process

Derived from: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Effects Based Operations

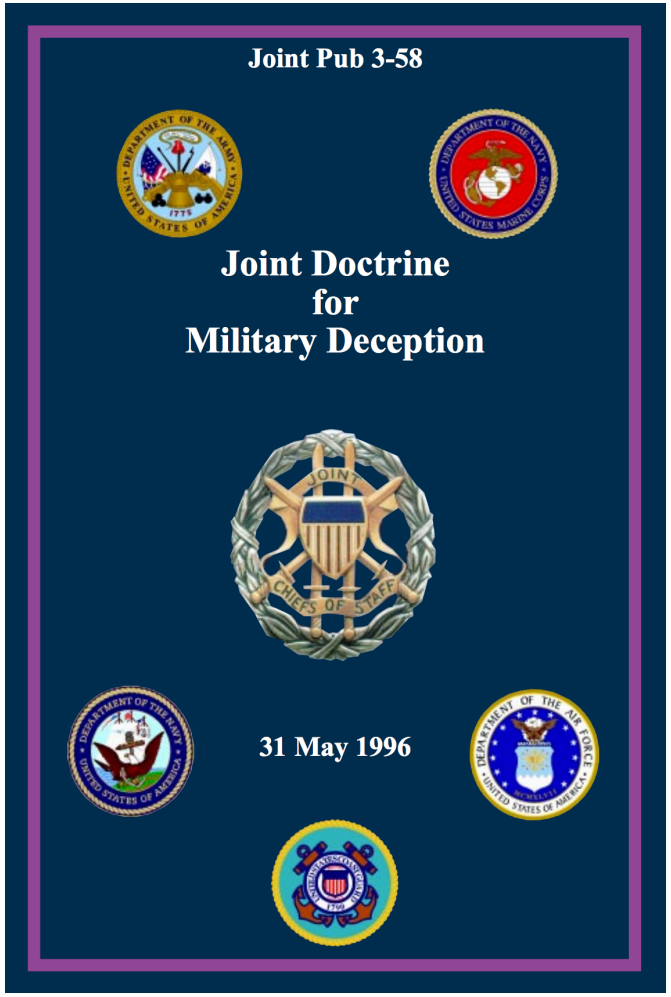


A military concept for planning and executing operations designed to achieve a desired effect.

- **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

https://en.wikipedia.org/wiki/Effects-based_operations
http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_60.pdf
http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_09.pdf
https://openclipart.org/image/800px/svg_to_png/191794/william-morris-letter-d.png

Deception

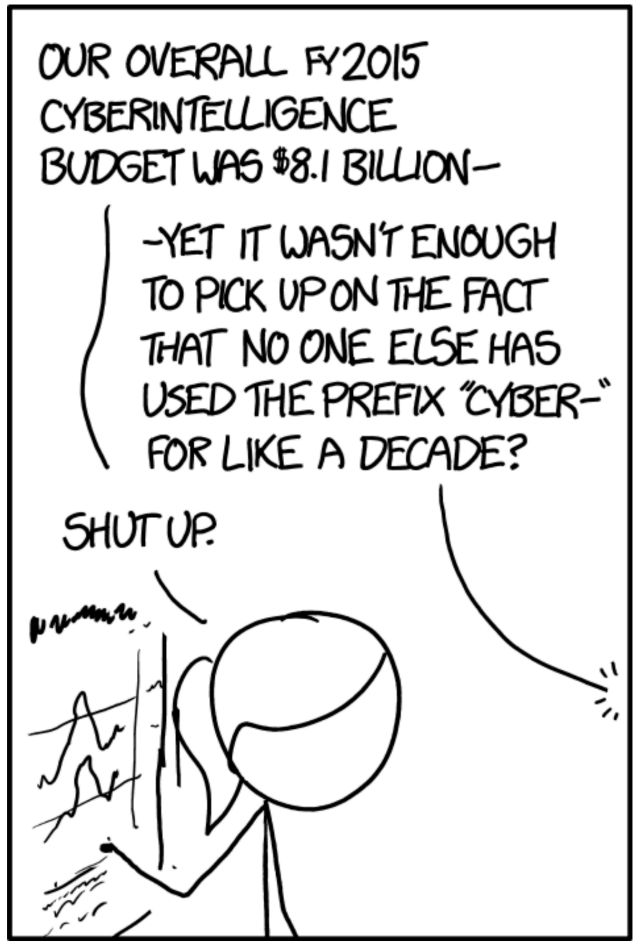


	Attacker	Defender
Human	Providing decoy web page	Convincing IT Help Desk to reset password Phishing
Code / Machine	Analysis VM environment convinces malware it is “real” Spoofed network service banners	Spoofing browser user agent Spoofing IP address

The Future of Cyber Armies

- Every major power and most minor powers
- United States Cyber Academy
- Separate military service for cyber
- 30 year veterans of continuous offensive and defensive operations
- Robust Legal Authorities
- Cyber-enabled IO
- AI and Human Teaming

Takeaways…



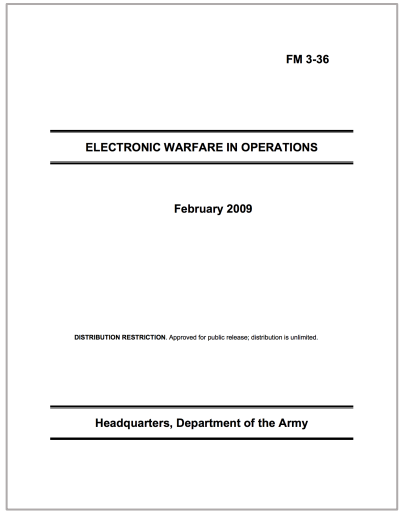
- When assessing your threat, **think like a nation-state cyber army**
- There is **much to mined** here for both researchers and practitioners
- **Read a manual or book** on the subject and look for intersections with infosec

https://xkcd.com/1573/

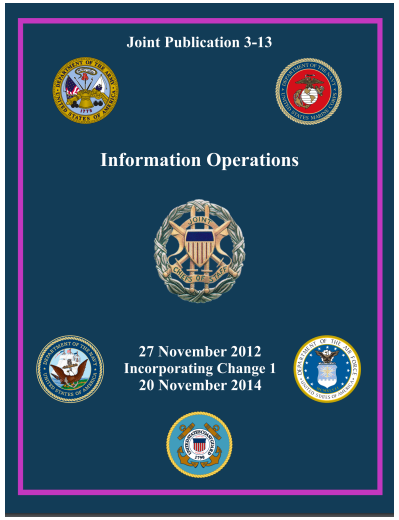
Where to Go for More Information…

Deception
JP 3-13.4

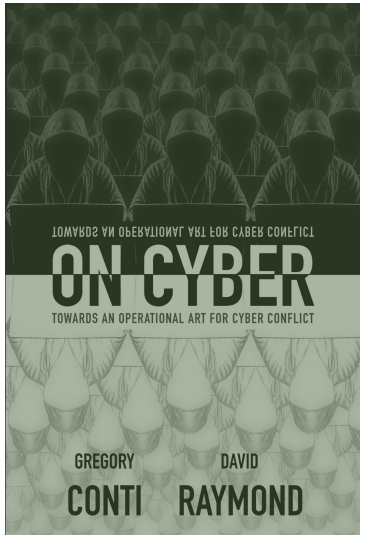
EW
FM 3-36



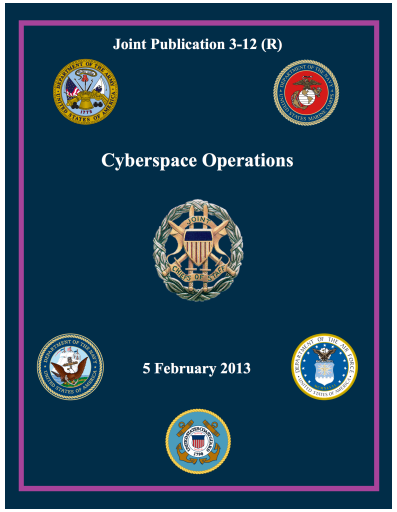
IO
JP 3-13



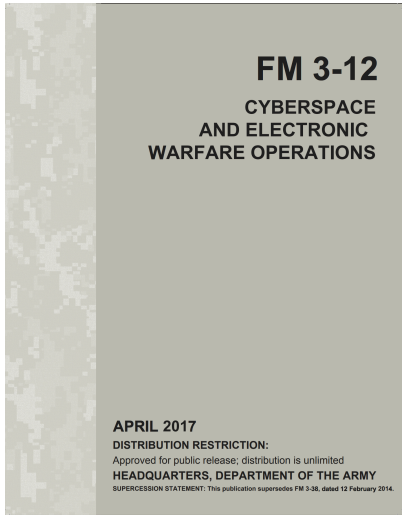
On Cyber



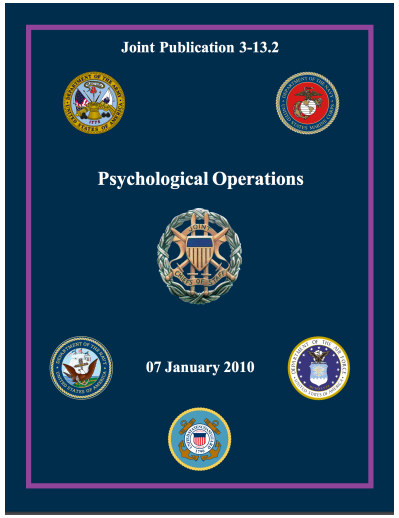
Cyber
Operations
JP 3-12



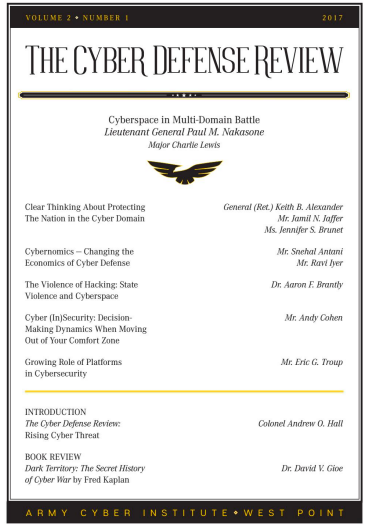
Cyber
Operations
FM 3-12



PSYOP
JP 3-13.2



Cyber
Defense
Review



Questions???

Tom Cross @_decius_ · 6 Aug 2016

Years from now I'll remember that I was close enough to crush **skynet**'s circuits before the war began. #regrets

1 3 22

"Years from now I'll remember that I was close enough to crush Skynet's circuits before the war began. #regrets"

- @_decius_

Gregory Conti / Director of Research / IronNet Cybersecurity / @cyberbgone