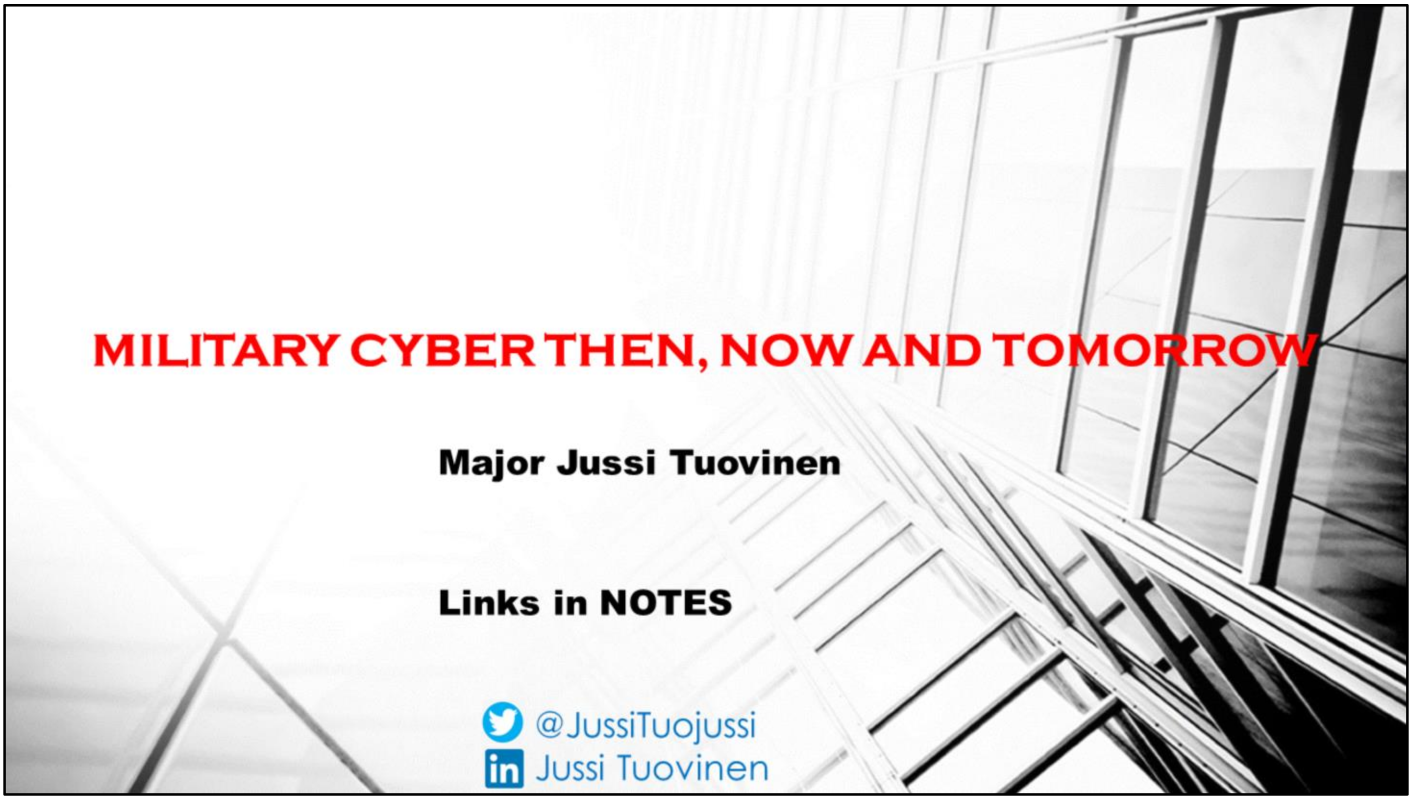


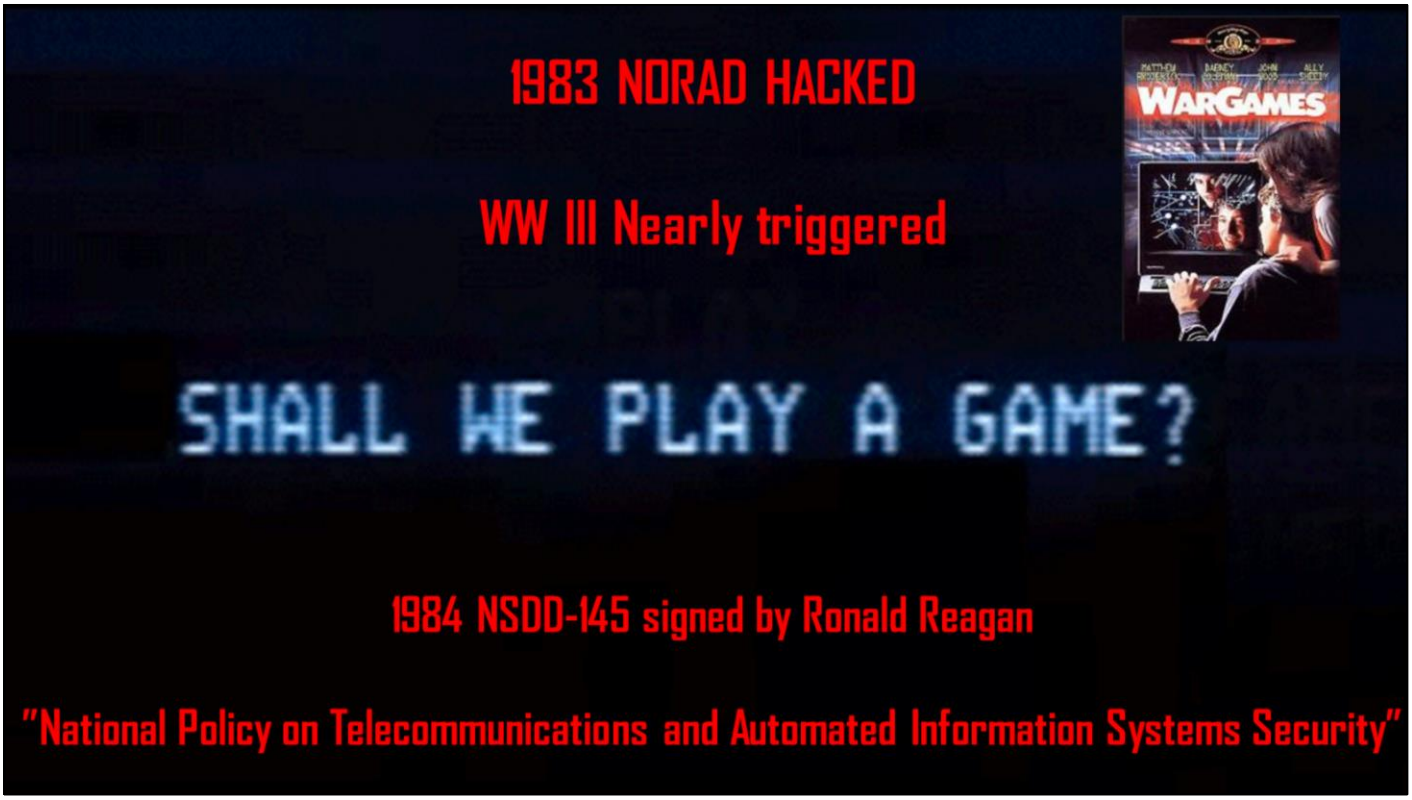
MILITARY CYBER THEN, NOW AND TOMORROW

Major Jussi Tuovinen

Links in NOTES

@JussiTuojussi

Jussi Tuovinen



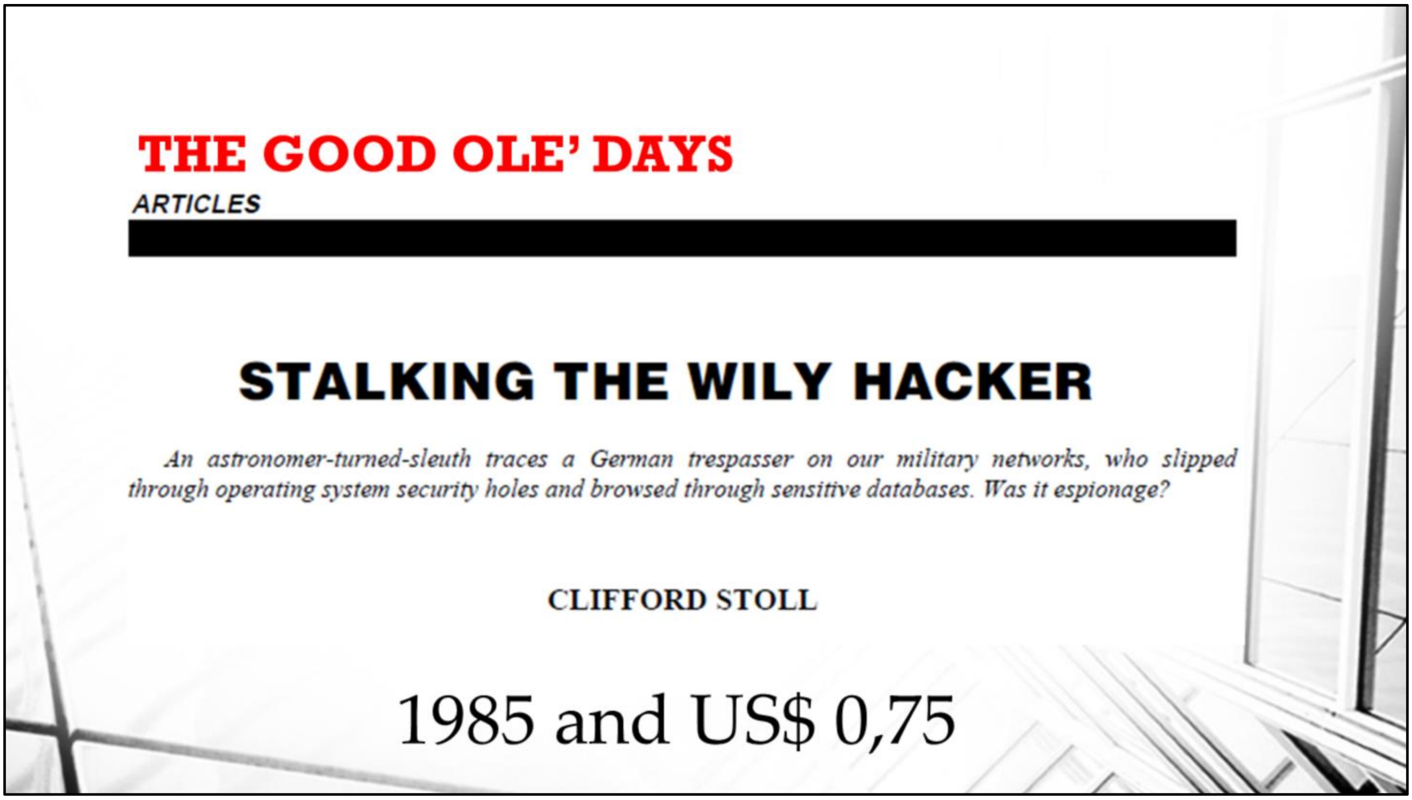
1983 NORAD HACKED

WW III Nearly triggered

SHALL WE PLAY A GAME?

1984 NSDD-145 signed by Ronald Reagan

"National Policy on Telecommunications and Automated Information Systems Security"



THE GOOD OLE' DAYS

ARTICLES

STALKING THE WILY HACKER

An astronomer-turned-sleuth traces a German trespasser on our military networks, who slipped through operating system security holes and browsed through sensitive databases. Was it espionage?

CLIFFORD STOLL

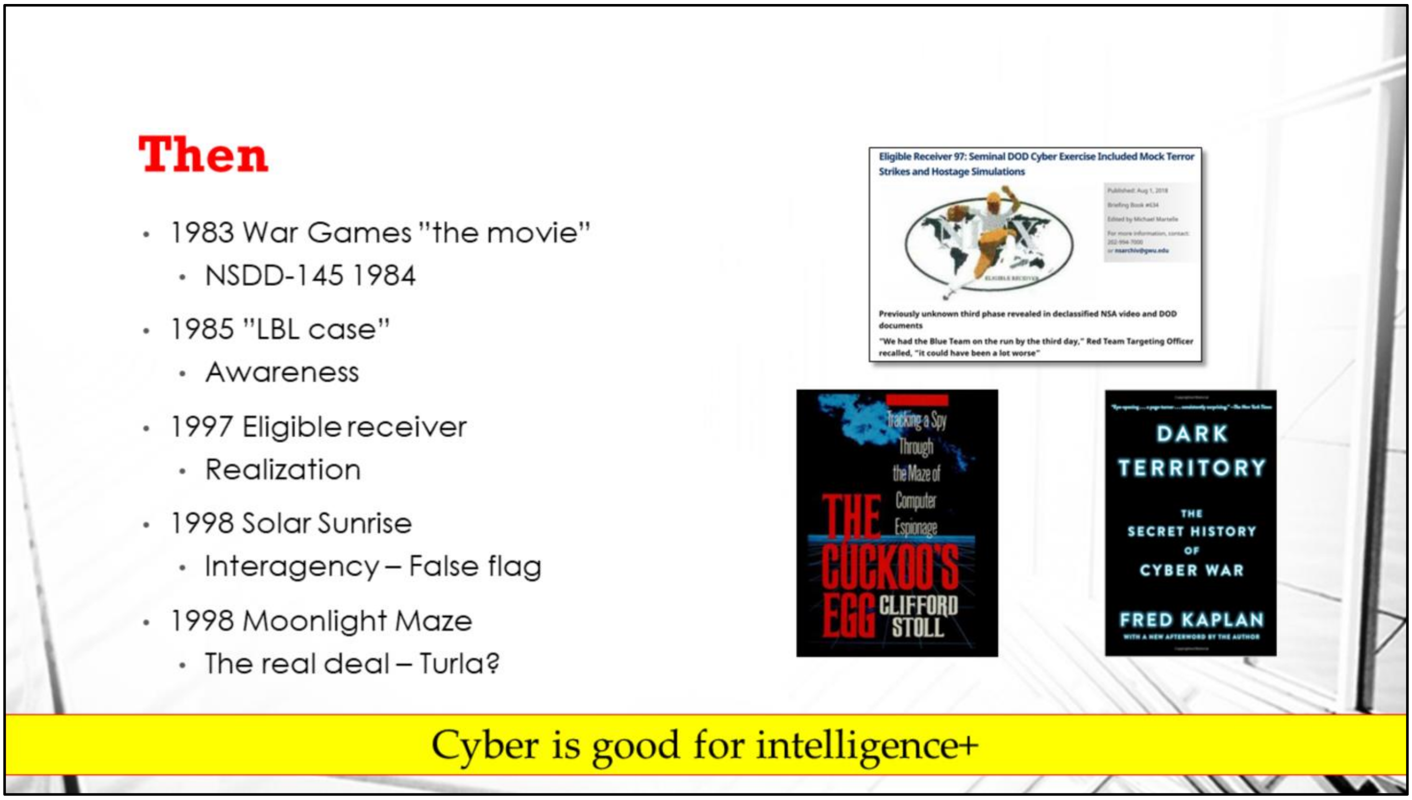
1985 and US$ 0,75

WILY HACKER
http://mars.umhb.edu/~wgt/cisc4370/wilyhacker.pdf

Markus Hess
https://en.wikipedia.org/wiki/Markus_Hess

Cuckoos egg
https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg

CCC
https://en.wikipedia.org/wiki/Chaos_Computer_Club



Then

- 1983 War Games "the movie"
  - NSDD-145 1984
- 1985 "LBL case"
  - Awareness
- 1997 Eligible receiver
  - Realization
- 1998 Solar Sunrise
  - Interagency – False flag
- 1998 Moonlight Maze
  - The real deal – Turla?

Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations

Published: Aug 1, 2018

Briefing Book #634

Edited by Michael Martelle

For more information, contact:
202-994-7000
or nsarchive@gwu.edu

Previously unknown third phase revealed in declassified NSA video and DOD documents

"We had the Blue Team on the run by the third day," Red Team Targeting Officer recalled, "it could have been a lot worse"

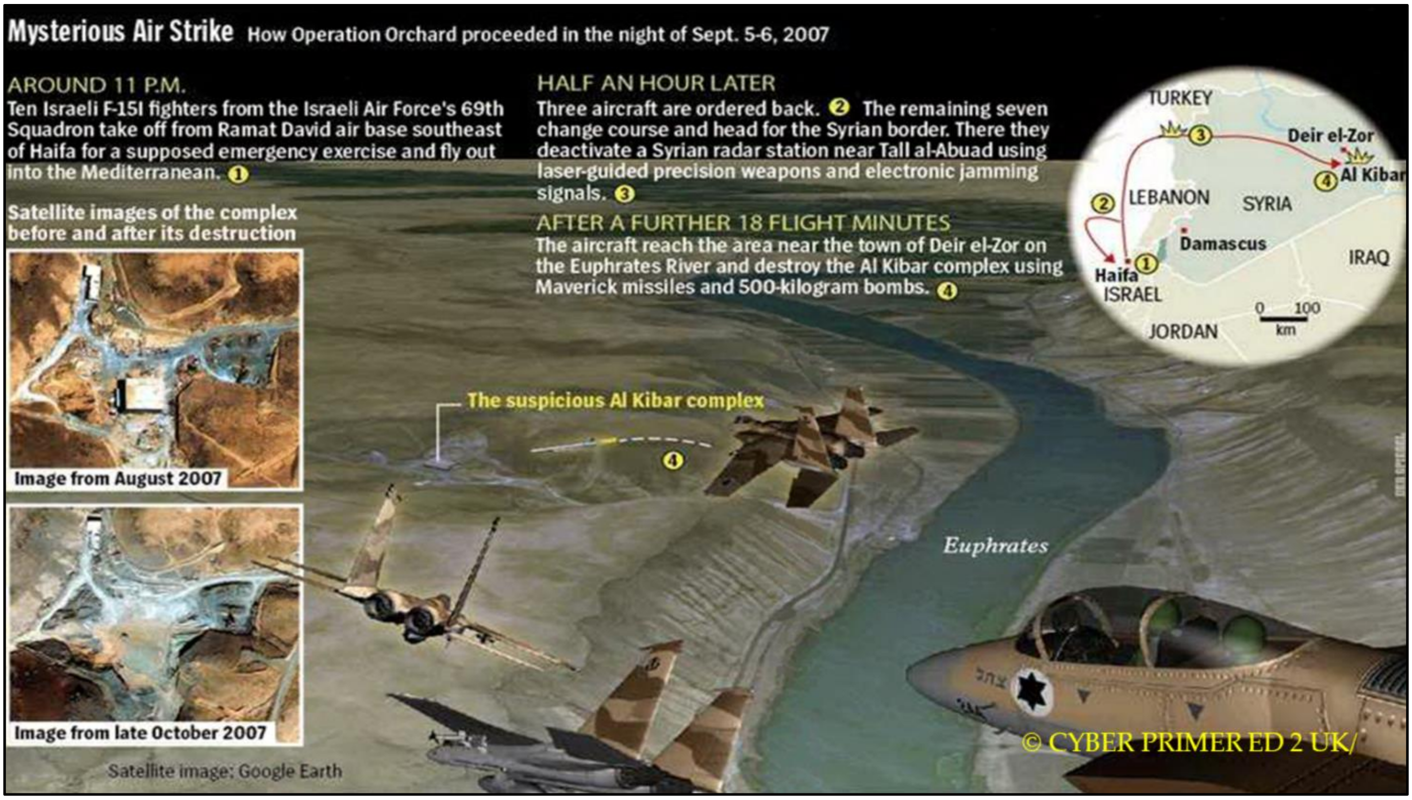
ELIGIBLE RECEIVER
Tracking a Spy Through the Maze of Computer Espionage
THE CUCKOO'S EGG
CLIFFORD STOLL
DARK TERRITORY
THE SECRET HISTORY OF CYBER WAR
FRED KAPLAN
WITH A NEW AFTERWORD BY THE AUTHOR

Cyber is good for intelligence+

ER97
https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations

Solar sunrise
https://www.globalsecurity.org/military/ops/solar-sunrise.htm
http://www.informit.com/articles/article.aspx?p=19603&seqNum=4

Moonlight Maze
https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7



Mysterious Air Strike How Operation Orchard proceeded in the night of Sept. 5-6, 2007

AROUND 11 P.M.

Ten Israeli F-15I fighters from the Israeli Air Force's 69th Squadron take off from Ramat David air base southeast of Haifa for a supposed emergency exercise and fly out into the Mediterranean. ①

HALF AN HOUR LATER

Three aircraft are ordered back. ② The remaining seven change course and head for the Syrian border. There they deactivate a Syrian radar station near Tall al-Abuad using laser-guided precision weapons and electronic jamming signals. ③

AFTER A FURTHER 18 FLIGHT MINUTES

The aircraft reach the area near the town of Deir el-Zor on the Euphrates River and destroy the Al Kibar complex using Maverick missiles and 500-kilogram bombs. ④

Satellite images of the complex before and after its destruction

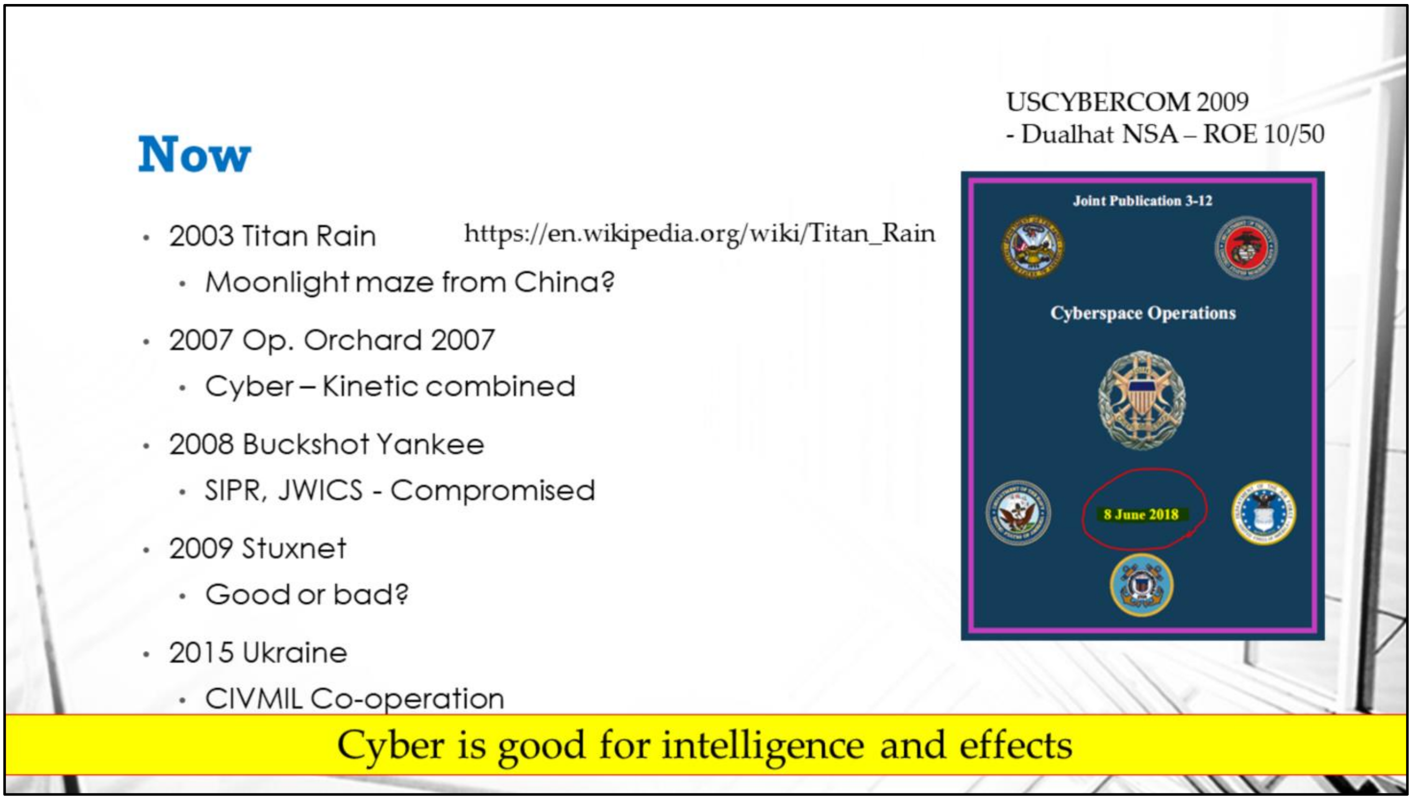
Image from August 2007

Image from late October 2007

Satellite image: Google Earth

© CYBER PRIMER ED 2 UK/

Operation Orchard:
https://www.wired.com/2009/11/mossad-hack/



Now

- 2003 Titan Rain https://en.wikipedia.org/wiki/Titan_Rain
  - Moonlight maze from China?
- 2007 Op. Orchard 2007
  - Cyber – Kinetic combined
- 2008 Buckshot Yankee
  - SIPR, JWICS - Compromised
- 2009 Stuxnet
  - Good or bad?
- 2015 Ukraine
  - CIVMIL Co-operation

USCYBERCOM 2009
- Dualhat NSA – ROE 10/50

Joint Publication 3-12

Cyberspace Operations

8 June 2018

Cyber is good for intelligence and effects

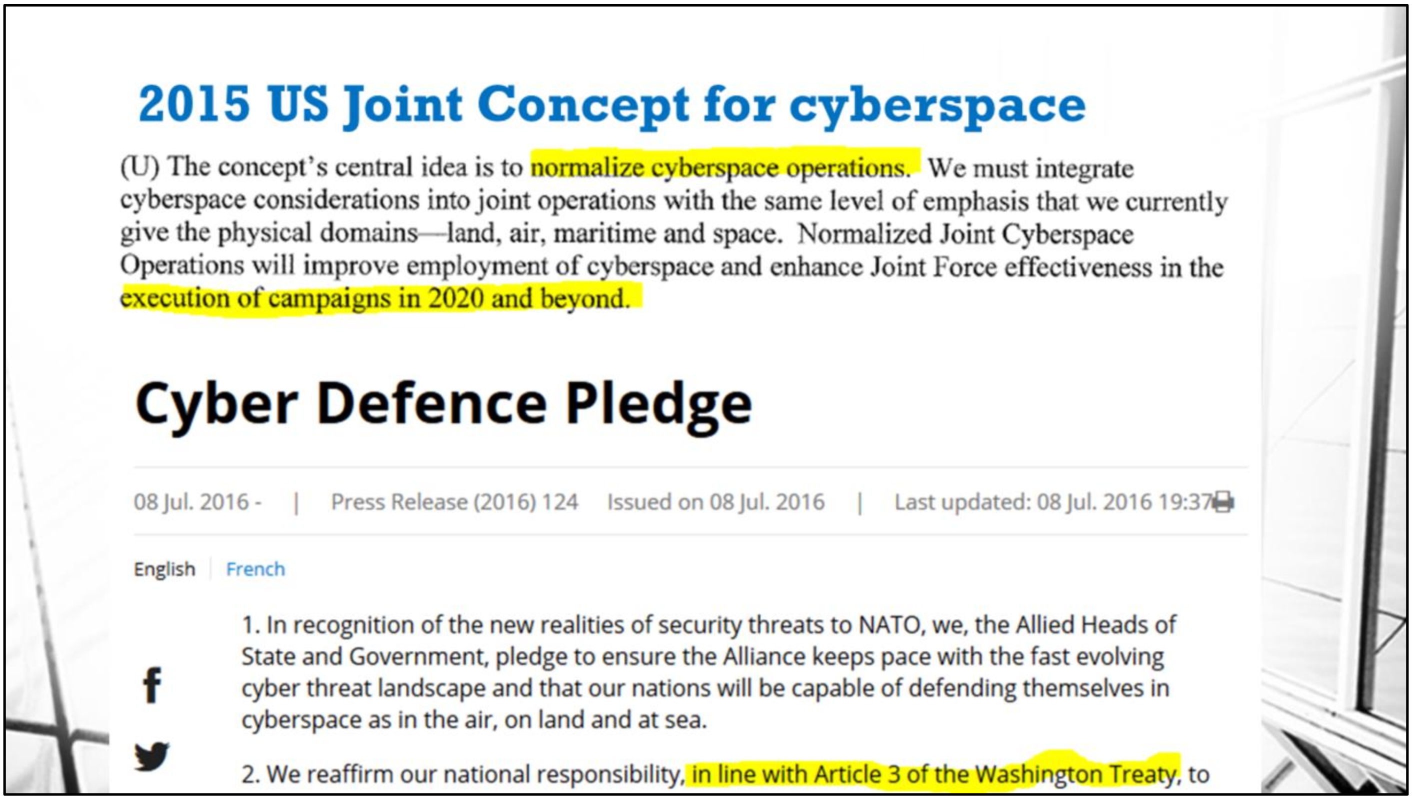
Titan rain
https://en.wikipedia.org/wiki/Titan_Rain

Buckshot Yankee:
https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?noredirect=on&utm_term=.d0f05586e648

Stuxnet:
https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Ukraine
https://www.wired.com/story/russian-hackers-attack-ukraine/

JP312:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150



2015 US Joint Concept for cyberspace

(U) The concept's central idea is to normalize cyberspace operations. We must integrate cyberspace considerations into joint operations with the same level of emphasis that we currently give the physical domains—land, air, maritime and space. Normalized Joint Cyberspace Operations will improve employment of cyberspace and enhance Joint Force effectiveness in the execution of campaigns in 2020 and beyond.

Cyber Defence Pledge

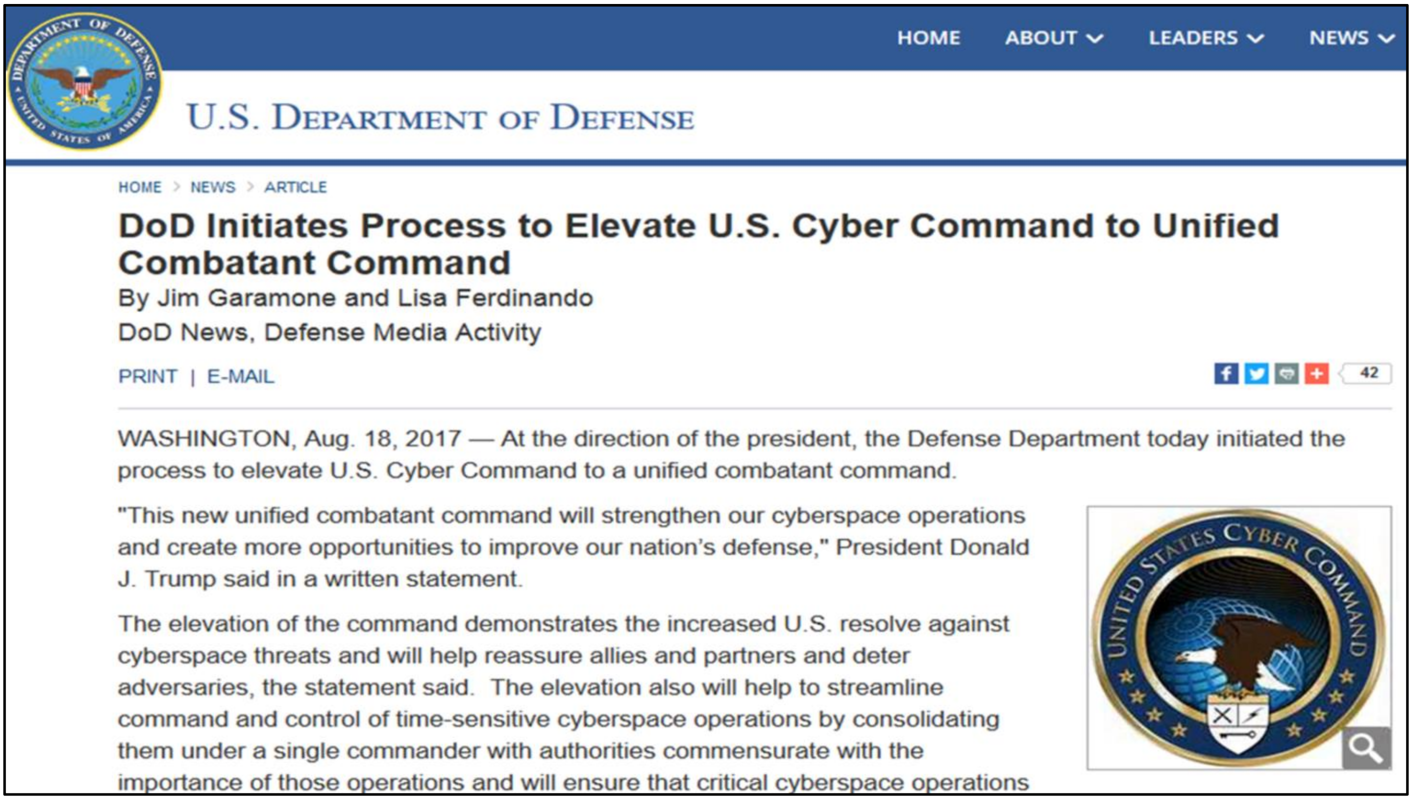
08 Jul. 2016 - | Press Release (2016) 124 Issued on 08 Jul. 2016 | Last updated: 08 Jul. 2016 19:37

English | French

1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.

2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to

NATO
https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
https://www.nato.int/cps/en/natohq/official_texts_133177.htm
https://www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=en



HOME ABOUT LEADERS NEWS

U.S. DEPARTMENT OF DEFENSE

HOME > NEWS > ARTICLE

DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command

By Jim Garamone and Lisa Ferdinando

DoD News, Defense Media Activity

PRINT | E-MAIL

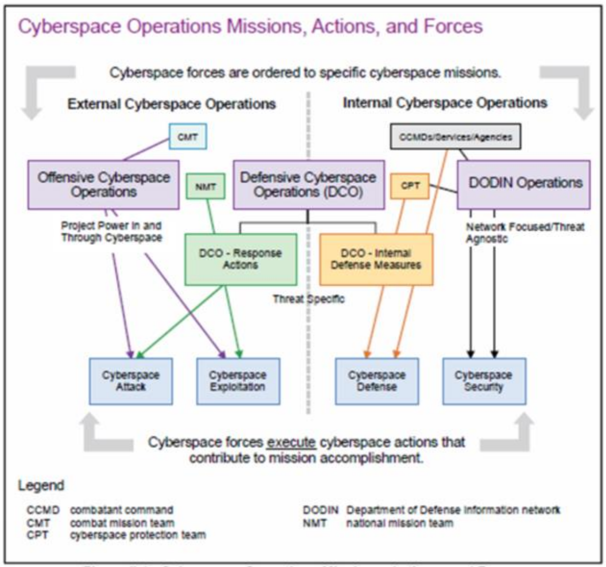
42

WASHINGTON, Aug. 18, 2017 — At the direction of the president, the Defense Department today initiated the process to elevate U.S. Cyber Command to a unified combatant command.

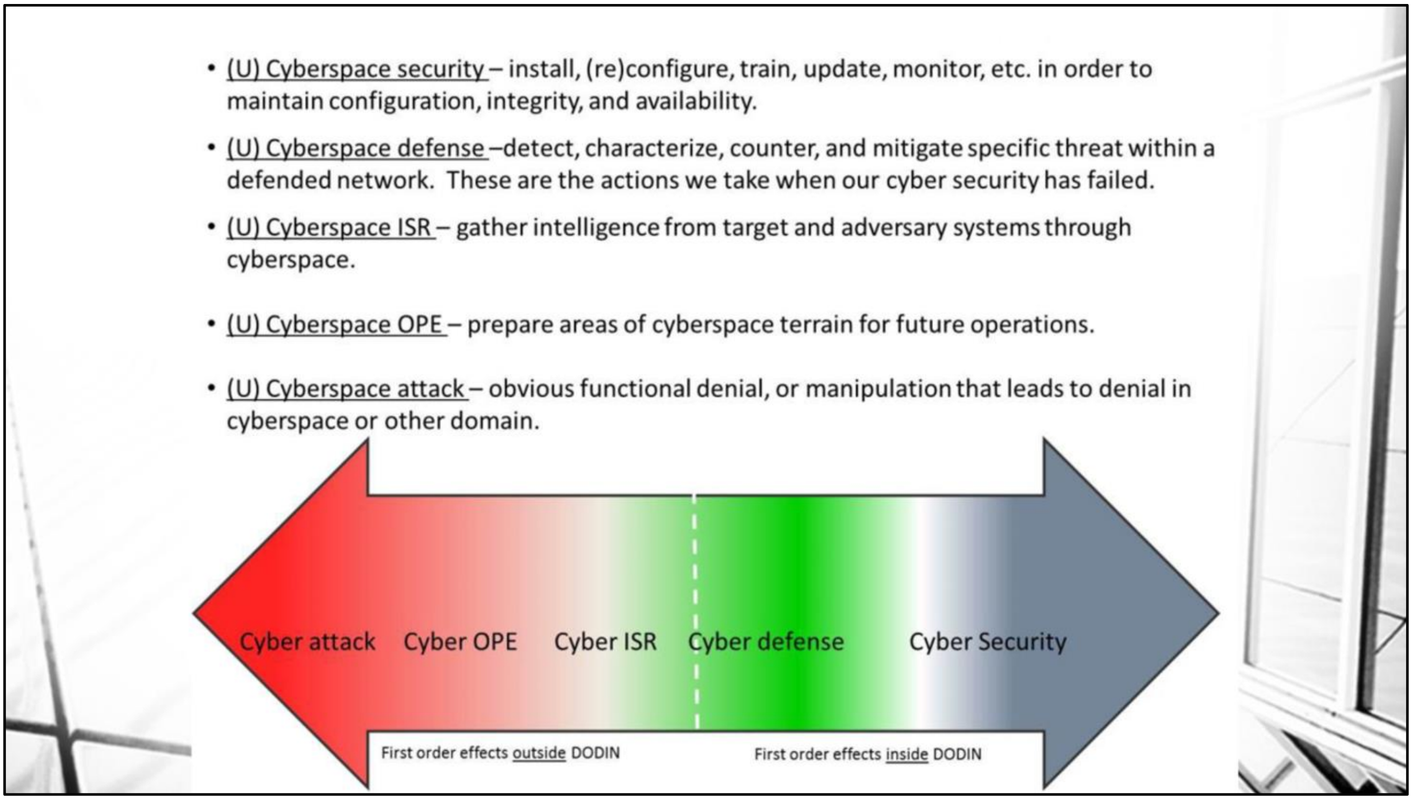
"This new unified combatant command will strengthen our cyberspace operations and create more opportunities to improve our nation's defense," President Donald J. Trump said in a written statement.

The elevation of the command demonstrates the increased U.S. resolve against cyberspace threats and will help reassure allies and partners and deter adversaries, the statement said. The elevation also will help to streamline command and control of time-sensitive cyberspace operations by consolidating them under a single commander with authorities commensurate with the importance of those operations and will ensure that critical cyberspace operations

CYBER OPERATIONS – DODIN → DCO → OCO


Cyberspace Operations Missions, Actions, and Forces
Cyberspace forces are ordered to specific cyberspace missions.
External Cyberspace Operations
Internal Cyberspace Operations
CMT
CCMDs/Services/Agencies
Offensive Cyberspace Operations
NMT
Defensive Cyberspace Operations (DCO)
CPT
DODIN Operations
Project Power in and Through Cyberspace
DCO - Response Actions
DCO - Internal Defense Measures
Network Focused/Threat Agnostic
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.
Legend
CCMD combatant command
CMT combat mission team
CPT cyberspace protection team
DODIN Department of Defense information network
NMT national mission team

JP312: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150



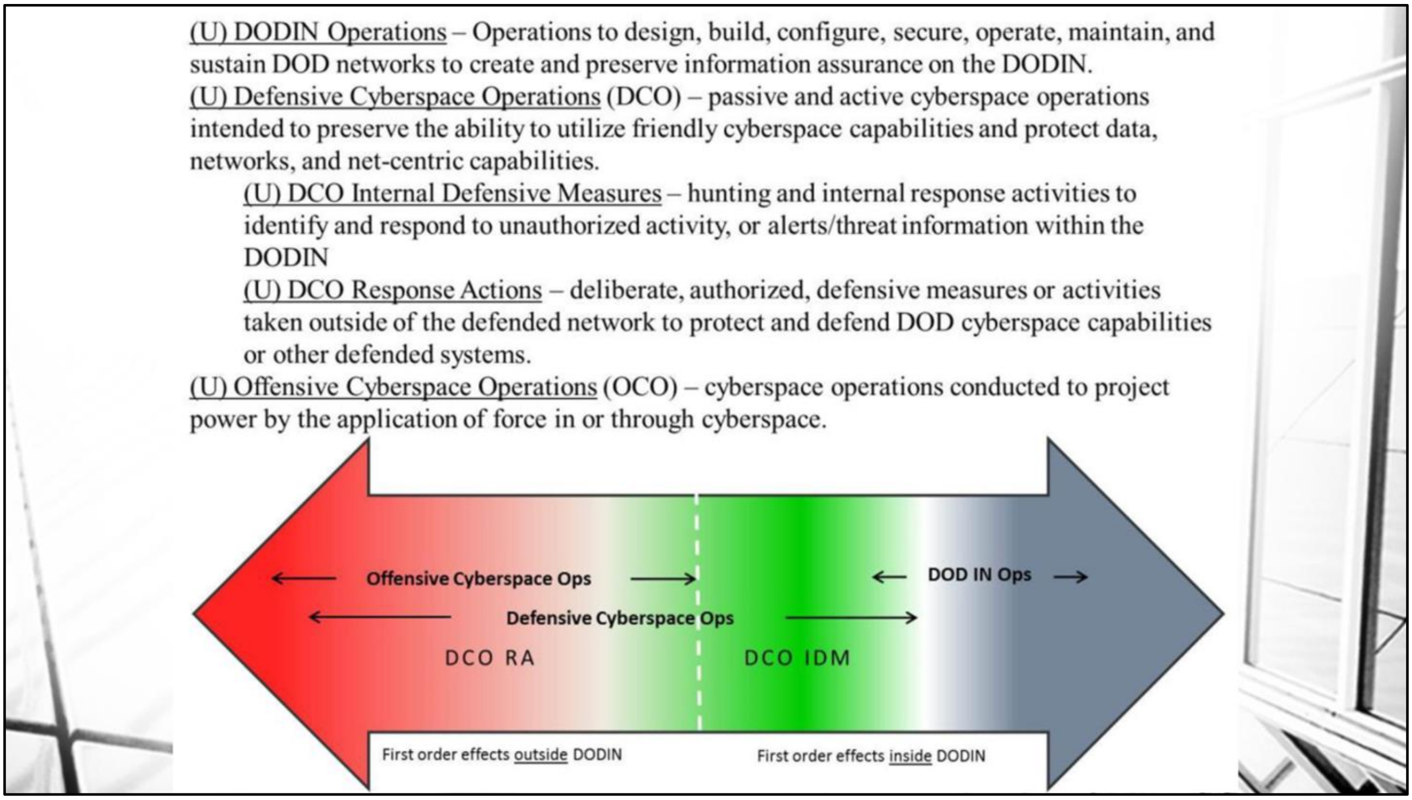
- (U) Cyberspace security – install, (re)configure, train, update, monitor, etc. in order to maintain configuration, integrity, and availability.
- (U) Cyberspace defense –detect, characterize, counter, and mitigate specific threat within a defended network. These are the actions we take when our cyber security has failed.
- (U) Cyberspace ISR – gather intelligence from target and adversary systems through cyberspace.
- (U) Cyberspace OPE – prepare areas of cyberspace terrain for future operations.
- (U) Cyberspace attack – obvious functional denial, or manipulation that leads to denial in cyberspace or other domain.

Cyber attack Cyber OPE Cyber ISR Cyber defense Cyber Security

First order effects outside DODIN

First order effects inside DODIN

JP312:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150



(U) DODIN Operations – Operations to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve information assurance on the DODIN.

(U) Defensive Cyberspace Operations (DCO) – passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities.

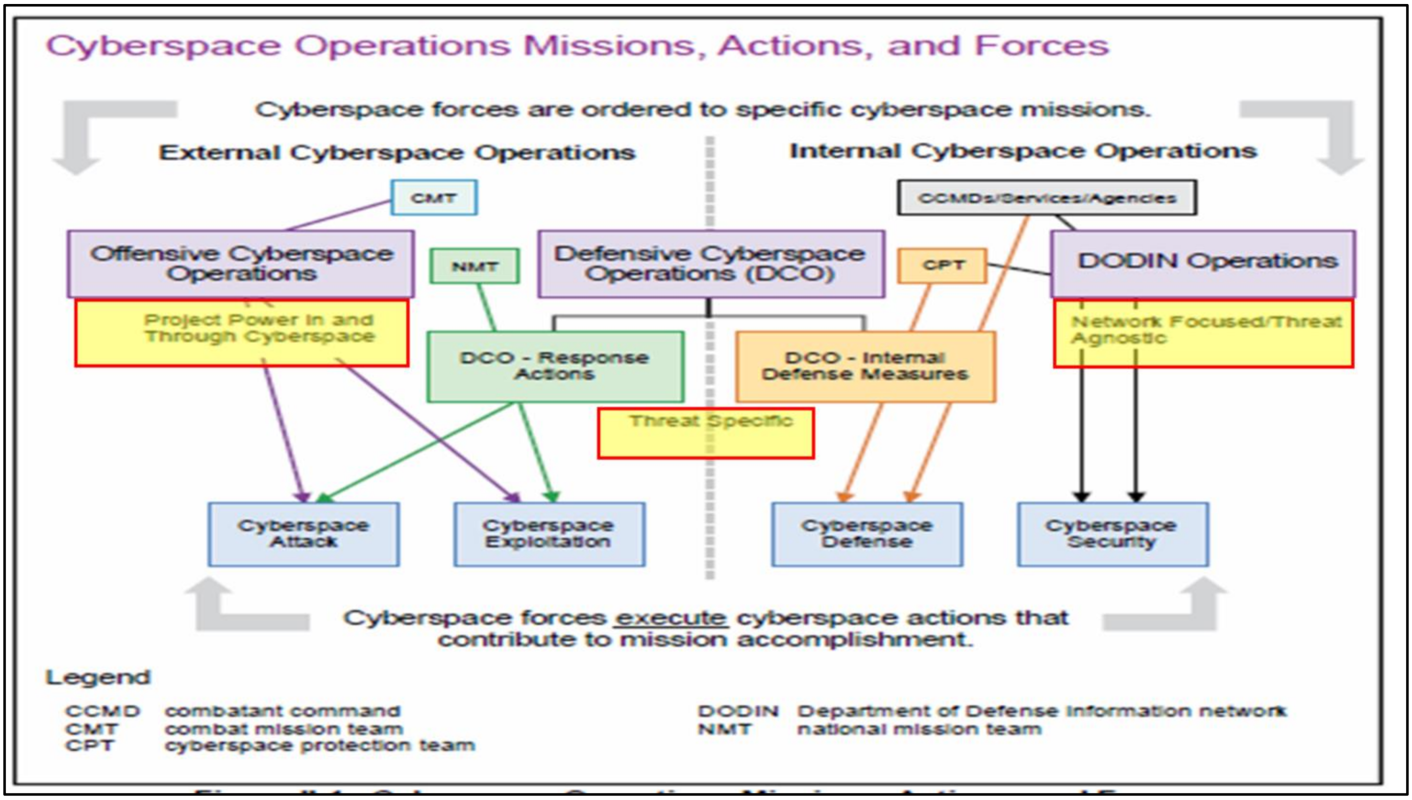
(U) DCO Internal Defensive Measures – hunting and internal response activities to identify and respond to unauthorized activity, or alerts/threat information within the DODIN

(U) DCO Response Actions – deliberate, authorized, defensive measures or activities taken outside of the defended network to protect and defend DOD cyberspace capabilities or other defended systems.

(U) Offensive Cyberspace Operations (OCO) – cyberspace operations conducted to project power by the application of force in or through cyberspace.

← Offensive Cyberspace Ops →
← DOD IN Ops →
← Defensive Cyberspace Ops →
DCO RA
DCO IDM
First order effects outside DODIN
First order effects inside DODIN

JP312: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150



Cyberspace Operations Missions, Actions, and Forces

Cyberspace forces are ordered to specific cyberspace missions.

External Cyberspace Operations
Internal Cyberspace Operations
CMT
CCMDs/Services/Agencies
Offensive Cyberspace Operations
NMT
Defensive Cyberspace Operations (DCO)
CPT
DODIN Operations
Project Power In and Through Cyberspace
DCO - Response Actions
DCO - Internal Defense Measures
Network Focused/Threat Agnostic
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security

Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.

Legend

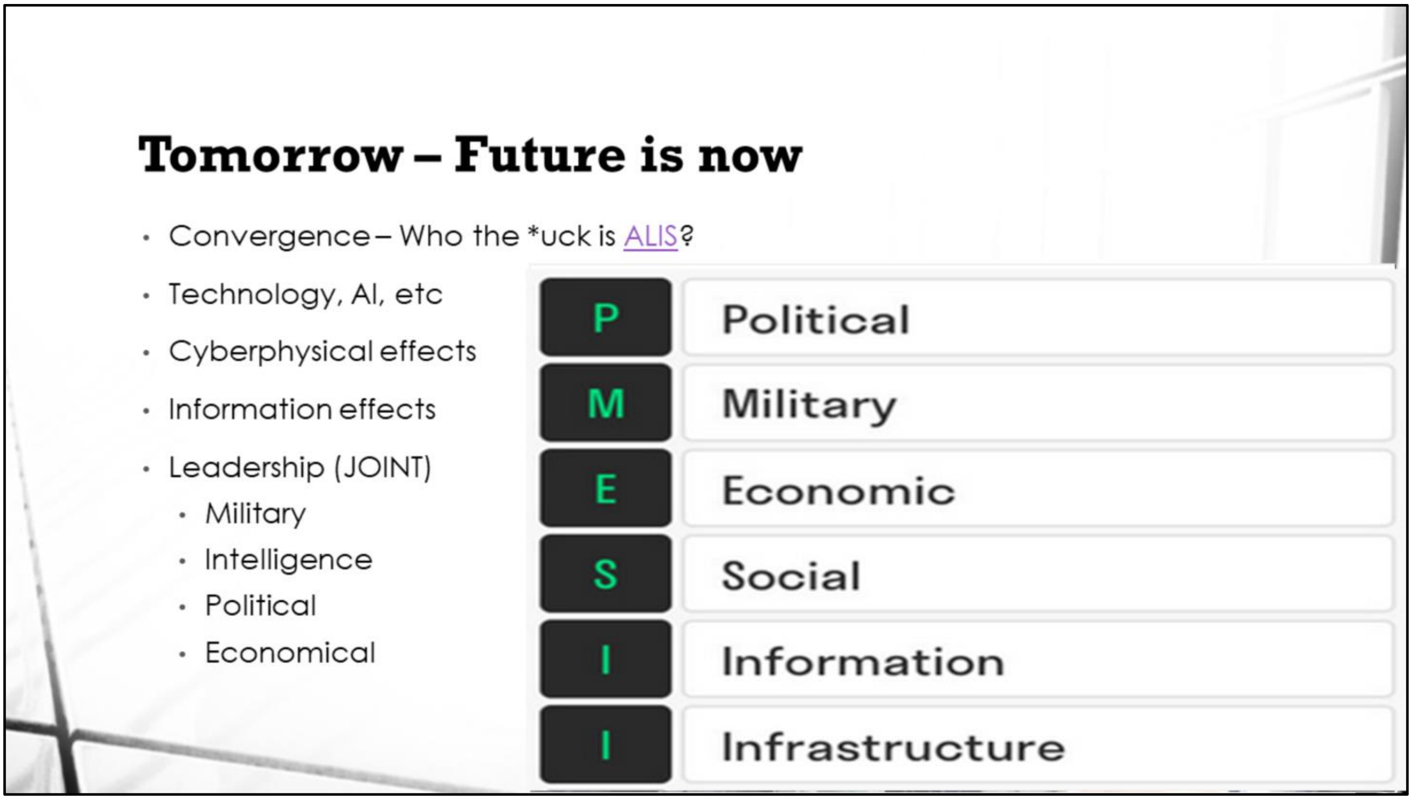
CCMD	combatant command
CMT	combat mission team
CPT	cyberspace protection team
DODIN	Department of Defense information network
NMT	national mission team

Threat agnostic – DODIN
Threat Spesific – DCO
Project power – OCO

JP312:
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

”The fifth military domain”

Protect our systems and create effects to adversary systems



Tomorrow – Future is now

- Convergence – Who the *uck is ALIS?
- Technology, AI, etc
- Cyberphysical effects
- Information effects
- Leadership (JOINT)
  - Military
  - Intelligence
  - Political
  - Economical

P	Political
M	Military
E	Economic
S	Social
I	Information
I	Infrastructure

ALIS – Autonomic Logistics and Information System
https://www.youtube.com/watch?v=yqShP6R5P6g
https://www.lockheedmartin.com/en-us/products/autonomic-logistics-information-system-alis.html

GAO REPORT
https://www.gao.gov/products/GAO-19-128

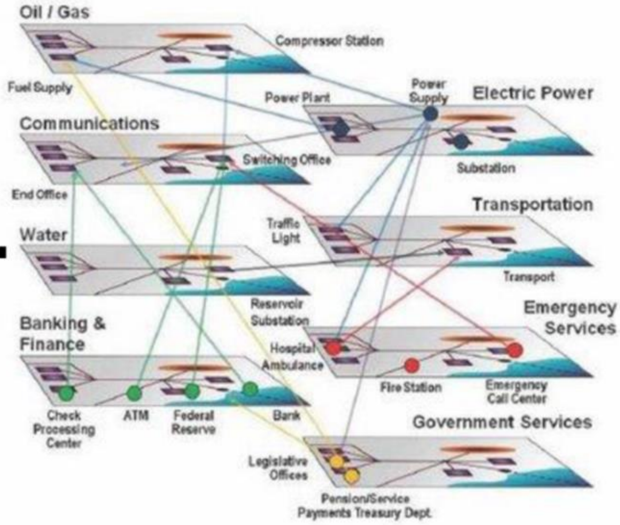
DARPA AI
https://www.darpa.mil/program/cyber-grand-challenge

INFO
https://taskandpurpose.com/researchers-track-nato-troops-internet

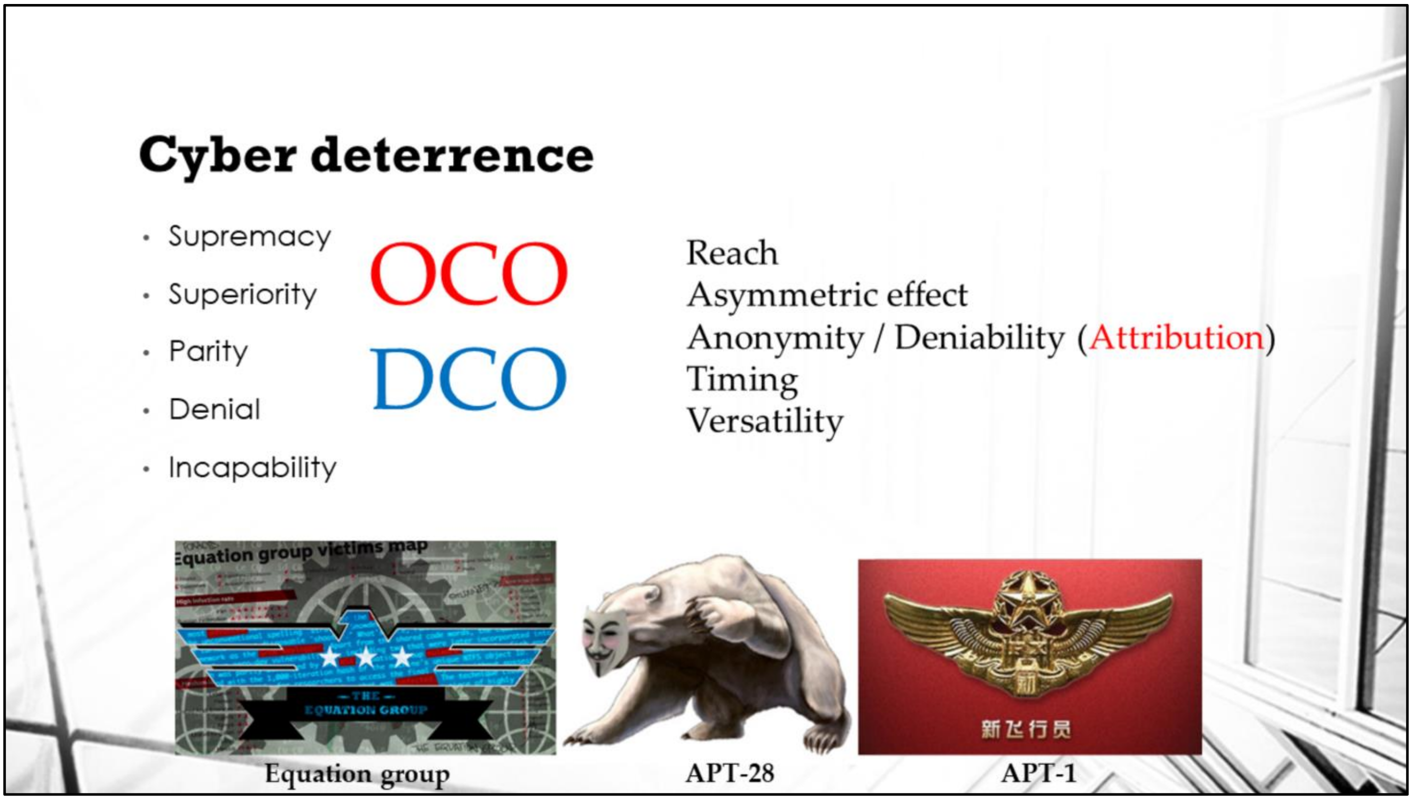
PMESIIPT
https://www.toolshero.com/strategy/pmesii-pt/

Fighting power + Support

+



Cyber is a team sport



Cyber deterrence

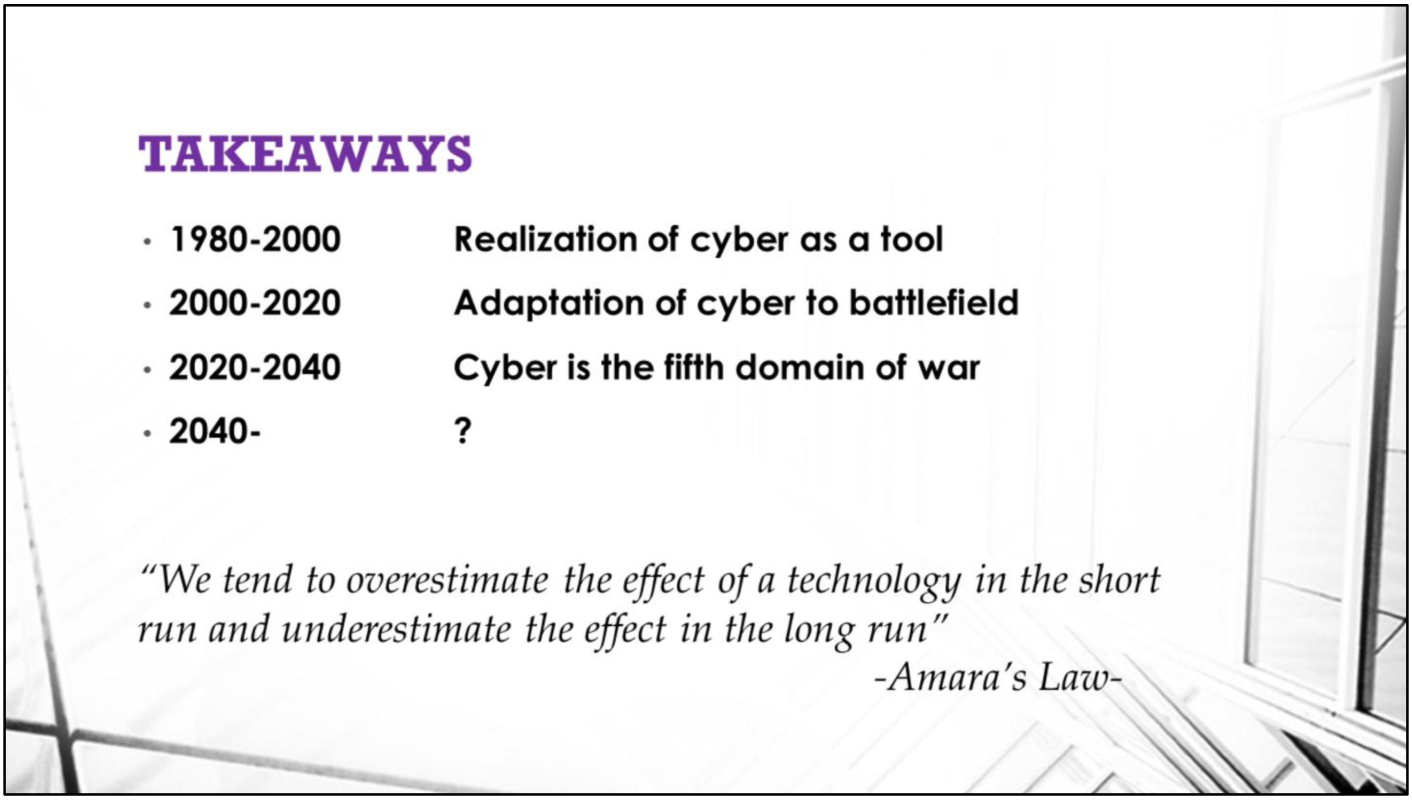
- Supremacy
- Superiority
- Parity
- Denial
- Incapability

OCO

DCO

Reach
Asymmetric effect
Anonymity / Deniability (Attribution)
Timing
Versatility

Equation group **APT-28** **APT-1**



TAKEAWAYS

1980-2000	Realization of cyber as a tool
2000-2020	Adaptation of cyber to battlefield
2020-2040	Cyber is the fifth domain of war
2040-	?

"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run"

-Amara's Law-