Cyberspace Operations — Student Resource Guide

A compact, clickable resource pack for new military students of cyberspace operations. Organized: Fundamentals → Defensive Cyberspace Operations (DCO) → Offensive Cyberspace Operations (OCO). Includes direct links, examples, books, courses, and certification paths. (Public/unclassified resources only.)

1) Fundamentals — Core concepts & starting points

NIST guidance, networking, basic cyber hygiene, and introductory courses. Start here if you are new.

NIST SP 800■12: An Introduction to Information Security — baseline framing of security controls and risk. Link: nvlpubs.nist.gov - SP 800-12 Rev.1 (PDF)

DoD Cyber Workforce / DCWF — role definitions and KSAs for DoD cyber personnel. Link: DoD CIO - DCWF

Intro course — Cybrary: Introduction to IT & Cybersecurity — example lesson and labs. Link: Cybrary Course

Quick video example: "Introduction to IT & Cybersecurity | Lesson 01" — YouTube. Link: YouTube Intro Lesson

2) Defensive Cyberspace Operations (DCO)

Defensive fundamentals: detection, hardening, incident response, attack surface reduction, and resilience.

DoD Cyber Exchange — Policies & Guidance — official doctrine, policy, and guidance. Link: DoD Cyber Exchange Policies & Guidance

DC3 — Defense Cyber Crime Center — forensics, training, and lab references. Link: DC3

SIEM & IDS example: "Security Onion" — open-source network monitoring / IDS distro for training and labs. Link: Security Onion (use for packet capture / detection labs)

Practical lab platforms / CTFs: Try "OWASP Juice Shop" for web-app defensive testing and "Hack The Box" for network/host labs. Links: OWASP Juice Shop, Hack The Box

Incident case studies (examples): Search/report pages for SolarWinds, Colonial Pipeline, and Log4Shell analysis — these are excellent real-world studies. Example reading: "SolarWinds: Incident Summary and Lessons Learned" (public analysis articles available from Mandiant/CrowdStrike/Krebs).

DCO Courses & Tools (examples)

CISA — Cybersecurity Training & Exercises — free modules, exercises, and tabletop resources. Link: CISA Training

SANS / GIAC (selected defensive courses) — proactive monitoring, incident handling, DFIR. Link: SANS Institute

Free defensive tool examples: Wireshark (network capture), Suricata (IDS), OSSEC (HIDS). Links: Wireshark, Suricata, OSSEC

3) Offensive Cyberspace Operations (OCO)

OCO covers reconnaissance, exploitation, command-and-control, persistence, and OPSEC. Note: many offensive techniques are restricted or classified; use only in approved training/testbeds.

USCYBERCOM — Public materials & media — strategic statements and public video briefings. Link: USCYBERCOM

Red Team / Penetration test frameworks: MITRE ATT&CK; (adversary tactics & techniques) — essential for mapping attacker behavior. Link: MITRE ATT&CK;

Offensive toolkit examples for authorized labs: Metasploit (exploit framework), Burp Suite (web app proxy), and Cobalt Strike (commercial red team tool; restricted). Links: Metasploit, Burp Suite

Example OCO case studies: Stuxnet, NotPetya, and documented GRU campaigns — read public technical analyses (Symantec, Mandiant reports).

OCO Courses & Practice (examples)

EC-Council CEH — Certified Ethical Hacker (overview & public materials). Link: EC-Council CEH

Offensive labs / CTFs: HackTheBox "Pro Labs", Offensive Security's "Proving Grounds" and "OSCP" prep. Links: Hack The Box, Offensive Security

MITRE ATT&CK; Evaluations — public evaluations that show how vendors detect real adversary behaviors. Link: ATT&CK; Evaluations

4) Certifications — Paths & examples

Common military-relevant certs. Use official cert sites for exam objectives, training, and prerequisites.

CompTIA Security+ — vendor-neutral baseline cert. Link: CompTIA Security+

CISSP — (ISC)² — managerial/architect-level; requires experience. Link: (ISC)² CISSP

CEH — EC-Council — offensive-focused cert for authorized penetration testing. Link: CEH

GIAC / SANS — DFIR, intrusion detection, incident handling certs. Link: GIAC

5) Websites, Threat Intel & Communities

CISA — Alerts & Known Exploited Vulnerabilities: CISA News & Alerts

Krebs on Security — investigative journalism for major incidents: Krebs

CrowdStrike Blog — threat research & reports: CrowdStrike

arXiv — Security papers: arXiv - Cryptography & Security (recent)

CTF calendars & practice: CTFtime.org — CTFtime

6) Books & Media — examples with where to find

Hacking: The Art of Exploitation — Jon Erickson — practical low-level hacking and memory. (No Starch Press)

Practical Malware Analysis — Sikorski & Honig — malware reverse engineering lab guide. (No Starch Press)

@War: The Rise of the Military-Internet Complex — Shane Harris — narrative on cyber conflict.

The Web Application Hacker's Handbook — Stuttard & Pinto — web app exploitation and testing.

Sample video: "MITRE ATT&CK; Explained" — example YouTube overview: MITRE ATT&CK; Overview

7) How to use this guide (quick study plan)

1. Start with the Fundamentals links (NIST SP 800-12 + an intro course). 2. Deploy local lab VMs and practice with Security Onion, Wireshark, or OWASP Juice Shop. 3. Build toward a certification (Security+ recommended first). 4. Progress into defensive CTFs and then move into authorized offensive labs (HackTheBox Pro Labs, Offensive Security). 5. Keep reading incident reports and MITRE ATT&CK; mappings to connect tactics to real events.

Prepared for military students of cyberspace operations. This PDF contains public links and examples intended for training and unclassified learning. For classified or restricted materials, consult your command training officer or approved DoD training portals.