

University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

**DoD Cyber Response**

CS 4950/5950  
Homeland Security &  
Cybersecurity


**Lesson 35**  
**DoD Cyber Response**

Rick White, Ph.D.  
University of Colorado, Colorado  
Springs



<sup>1</sup> Esc

1



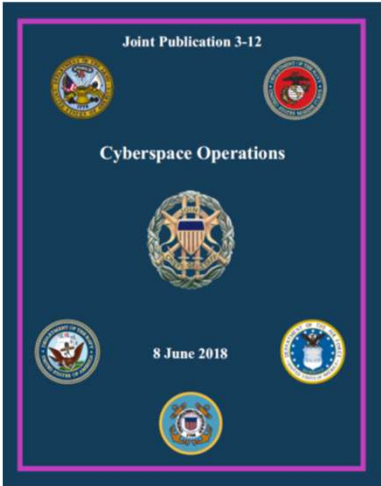
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**DoD Cyber Response**

DoD Joint Publication 3-12,  
Cyberspace Operations was  
updated in June 2018.



<sup>2</sup> Esc

2



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### DoD Cyber Response


To begin, JP 3-12 **acknowledges that the Department of Homeland Security has responsibility for protecting US cyberspace**, but that DoD is prepared to lend support when directed by the President.

### JP3-12 Cyber Ops

- **DHS** has responsibility for protecting US cyberspace.
- **DoD** is prepared to lend support when directed by President.

3  
Esc

3




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### DoD Cyber Response

- DoD cyber forces operate under the direction of **United States Cyber Command**, a functional military command capable of conducting offensive and defensive cyber operations.
- USCYBERCOM is headquartered at Fort Meade, MD, in proximity to the National Security Agency.



Service Secretaries

Service Departments

Army Cyber Command

Fleet Cyber Command

Air Force Cyber Command

Marine Corps Cyberspace

**USCYBER**

**Cyber Mission Force**

Cyber Protection Force

National Mission Force

Combat Mission Force

4  
Esc

4

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### DoD Cyber Response

- **All four services have designated cyber career specialties**; for example, you can be assigned a 17X Cyber Warfare Officer in either the US Army or US Air Force.
- Cyber specialists are trained and equipped by their respective services, and **conduct operations as part of the Cyber Mission Force.**

5 Esc

5

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### DoD Cyber Response

- The **Cyber Mission Force** went operational 17 May 18.
- The CMF is comprised of 133 teams of about 46 people adept in cyber operations.
- Most teams are dedicated to military missions in cyber defense and cyber offense.
- **About 13 teams, 10% of the force, are dedicated to protecting the nation's infrastructure.**

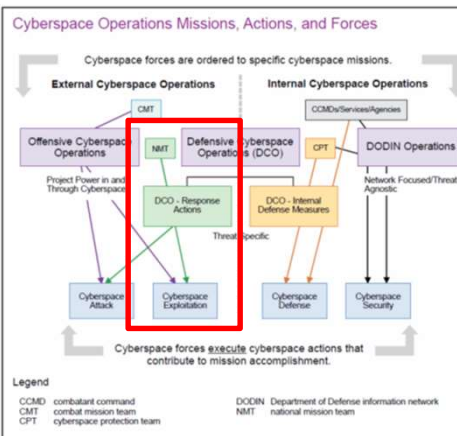
6 Esc

6



## DoD Cyber Response

1. **Cyber Protection Forces** defend DoD information networks, protect priority missions, & prepare cyber forces for combat
2. **Combat Mission Forces** conduct cyber ops in support of combatant commanders
3. **National Mission Forces** identify, block, and defeat foreign cyber-attack against US infrastructure



7

Esc

7




## DoD Cyber Response

- According to JP 3-12, cyber operations are categorized as either **offensive of defensive cyberspace operations**.
- **Defensive Cyberspace Operations** consist of both passive and active measures necessary to preserve friendly cyberspace capabilities and their data.
- **Offensive Cyberspace Operations** are clearly designed to infiltrate, subvert, or neutralize targeted systems, apparently under the same legal provisions that might be invoked to authorize conventional military action.
- JP 3-12 hints that “**active**” **defense measures** may entail some form of **counterattack** against a hostile system, but also stresses that all actions must remain legal, both at home and abroad.

8

Esc

8



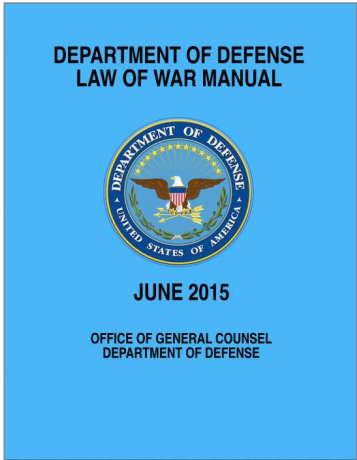
University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**DoD Cyber Response**

Cyber actions are required to conform with international conventions collectively known as the **Law of War** which are essentially **designed to prevent indiscriminate or unnecessary suffering.**



9  
Esc

9




University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**DoD Cyber Response**

**Would such restrictions prevent the US from shutting down an adversary's electric grid?**

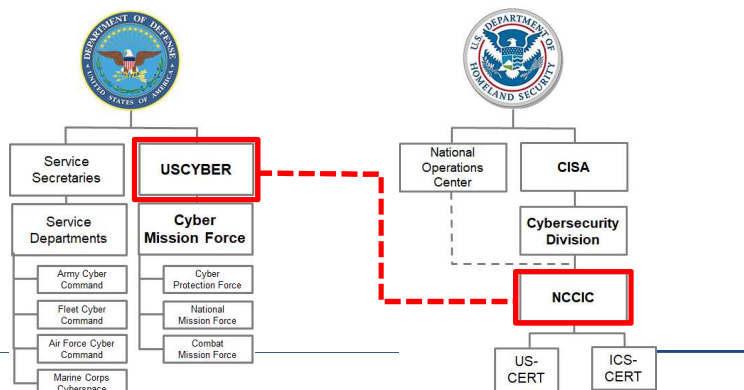


10  
Esc

10

### DoD Cyber Response

Coordination between DHS and USCYBERCOM takes place in the **National Cybersecurity and Communications Integration Center** operated by the Cybersecurity Division under the DHS Cybersecurity & Infrastructure Security Agency.



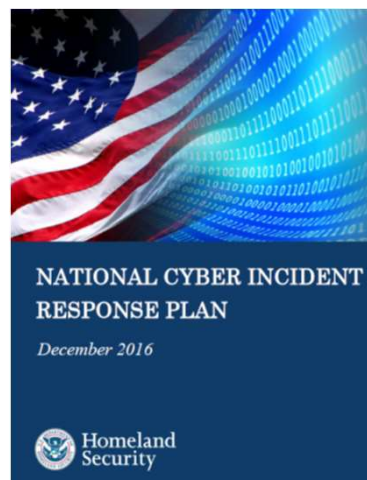
11

Esc

11

### DoD Cyber Response

According to the **2016 National Cyber Incident Response Plan**, USCYBERCOM support might be requested in response or anticipation of a **Significant Cyber Incident**.



12

Esc

12

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### DoD Cyber Response

In the case of a Significant Cyber Incident, the **Assistant Secretary for Cybersecurity and Communications** will convene a **Unified Coordination Group** to develop and execute a cyber Incident Action Plan.

General Definition	
Level 5 Emergency (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 Baseline (White)	Unsubstantiated or inconsequential event.

13 Esc

13

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### DoD Cyber Response

Of course the Unified Coordination Group Incident Management Team would be assisted by **playbooks** and other **operational plans** developed by the **NCCIC Planning Group**.

```

graph TD
    DHS[U.S. Department of Homeland Security] --> NOC[National Operations Center]
    DHS --> CISA[CISA]
    CISA --> CD[Cybersecurity Division]
    CD --> NCCIC[NCCIC]
    NCCIC --> USCERT[US-CERT]
    NCCIC --> ICSCERT[ICS-CERT]
    NOC -.- CD
  
```

14 Esc

14

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

**DoD Cyber Response**

Actions would be directed and executed by the **NCCIC Operations Group** working together with the **NCCIC Liaison Group**.

```

graph TD
    DHS[U.S. DEPARTMENT OF HOMELAND SECURITY] --> NOC[National Operations Center]
    DHS --> CISA[CISA]
    CISA --> CD[Cybersecurity Division]
    CD --> NCCIC[NCCIC]
    NCCIC --> USCERT[US-CERT]
    NCCIC --> ICS-CERT[ICS-CERT]
    NOC -.- NCCIC
  
```

Esc

15

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

**DoD Cyber Response**

**This is all a very complicated choreography that remains limited by ownership rights.**

```

graph TD
    DHS[U.S. DEPARTMENT OF HOMELAND SECURITY] --> NOC[National Operations Center]
    DHS --> CISA[CISA]
    CISA --> CD[Cybersecurity Division]
    CD --> NCCIC[NCCIC]
    NCCIC --> USCERT[US-CERT]
    NCCIC --> ICS-CERT[ICS-CERT]
    NOC -.- NCCIC
  
```

Esc

16



**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### DoD Cyber Response

Remember, DHS does not have its hands on the lever of critical infrastructure, therefore **all actions must be taken through the permission and support of owners and operators.**

```

graph TD
    DHS[U.S. Department of Homeland Security] --> NOC[National Operations Center]
    DHS --> CISA[CISA]
    CISA --> CD[Cybersecurity Division]
    CD --> NCCIC[NCCIC]
    NCCIC --> USCERT[US-CERT]
    NCCIC --> ICS-CERT[ICS-CERT]
  
```

Esc

17

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

### WTF?

**“When a cyber incident affects a private entity, the Federal Government will typically not play a direct role in the affected entities’ response activities but will remain cognizant of their activities and coordinate appropriately with the affected entity.”**

Esc

18

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**DoD Cyber Response**

Presumably, however, **IF** the attacks can be traced to a foreign country, **AND** the source can be confirmed, then USCYBER **National Mission Teams** **CAN** take action to thwart the attack.

19  
Esc

19

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

**Conclusion**

Questions?

20  
Esc

20