

Fact Sheet:  
**2018 DoD Cyber Strategy and Cyber Posture Review**  
*Sharpening our Competitive Edge in Cyberspace*

## Purpose

The *2018 Department of Defense (DoD) Cyber Strategy* articulates how the Department will implement the priorities of the *National Defense Strategy* in and through cyberspace. It supersedes the *2015 DoD Cyber Strategy*. The first-ever *DoD Cyber Posture Review* provided a comprehensive assessment of the Department's ability to successfully execute the Strategy.

---

## Central Challenge

U.S. prosperity and security depend on open and reliable access to information. Nations that are deterred from directly confronting U.S. military strength are using cyberspace operations in day-to-day competition to exploit a perceived advantage and harm our interests. China and Russia are engaging in great power competition via persistent, aggressive cyberspace campaigns that pose strategic, long-term risks to the Nation, our allies, and partners.

---

## Key Themes

- Using cyberspace to amplify military lethality and effectiveness;
  - Defending forward, confronting threats before they reach U.S. networks;
  - Proactively engaging in the day-to-day great power competition in cyberspace;
  - Protecting military advantage and national prosperity;
  - Recognizing partnerships are key to shared success in protecting cyberspace;
  - Actively contesting the exfiltration of sensitive DoD information;
  - Embracing technology, automation, and innovation to act at scale and speed;
  - Supporting the defense of critical infrastructure;
  - Recruiting, developing, and managing critical cyber talent.
- 

## DoD Objectives for Cyberspace

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace domain;
2. Enhancing Joint Force military advantages through the integration of cyber capabilities into planning and operations;
3. Deterring, preempting, or defeating malicious cyber activity targeting U.S. critical infrastructure that is likely to cause a significant cyber incident;
4. Securing DoD information and systems, including on non-DoD-owned networks, against cyber espionage and malicious cyber activity;
5. Expanding DoD cyber cooperation with allies, partners, and private sector entities.

## Cyber Posture Review

- As directed by the FY18 National Defense Authorization Act, the Department conducted a comprehensive review of the Department’s cyber posture and ability to execute the Strategy. The Review included extensive background research, data collection, and expert interviews.
  - This classified Review identified that we must continue investments in our people, capabilities, and processes to meet fully the objectives set forth in the Strategy.
  - The Review also included workshops, modeling, and wargames to further develop the Department’s approach to deterring, disrupting, and defeating malicious cyber activity and successfully competing in cyberspace.
- 

## Implementation

- The Department has begun to address these challenges, but it is an enduring effort and significant work remains.
- The Department will continually monitor specific Strategy implementation tasks through the Principal Cyber Advisor.
- The Department is identifying budget and resource impacts for the Fiscal Year 2019 and 2020 budgets.

