Department of the Air Force
Scientific Advisory Board

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE
WASHINGTON DC

Enhancing Operational Cyber Security Study

Abstract

During times of global competition or high-end armed conflict, competitors and potential adversaries will continually seek to exploit U.S. forces' dependence on data and network technologies in weapons systems, platforms, and critical infrastructure. Malicious cyber and cyber-physical activities may be designed to disable U.S. surveillance or strike assets; gather intelligence information; corrupt sensor data and message content; or impair transport, energy, and communication networks. To ensure continued ability to operate in contested environments, the Department of the Air Force (DAF) must act decisively to secure and defend its networks, assets, and facilities against a wide range of malicious cyber activity from sophisticated competitors and potential adversaries.

Effective cyber deterrence, defense, resilience, and recovery will be essential to DAF operations in any future conflict with peer adversaries. Preparing for mission success in cyber-contested environments requires enterprise-wide consideration of policies, strategies, and technologies that will allow U.S. forces to fully leverage the advanced weapons systems, facilities, and infrastructure developed with decades worth of investment. In view of the fast-evolving cyber landscape, the DAF would benefit from a review of its cybersecurity governance, processes, capabilities, and technologies.

The goal of this study is to provide actionable, specific, and justifiable recommendations for enhancing operational cybersecurity. An important emphasis of this study is to raise awareness of the large role cybersecurity makes for operational mission systems and overall readiness and to consider recommendations that will begin to have impact within the next 3-5 years.

The EOC panel visited stakeholders across the DAF, the wider Department of Defense (DoD), the US Government, and technical sector. These hosting organizations provided the team with topical briefings and panel discussions, detailed technical and programmatic documentations, and compelling tours of relevant facilities.

The study panel recommends five courses of action that will help prepare the DAF within the next 3-5 years to operate in a potential conflict:

1. Train all personnel to operate in environments that have been degraded by cyber effects

2. Increase surge capacity for cyber operations by leveraging the Air National Guard and the private sector

3. In pre-conflict, focus cyber security forces on prioritizing and mitigating the vulnerabilities that are most likely to threaten mission execution

SAF PA Approval: 2025-0634

4. Elevate the informal CROCS (Cyber Resilience Office for Operational Control Systems) working group to a CROWS (Cyber Resilience Office for Weapons Systems) – equivalent framework for cybersecurity

5. Automate analytics for near-real-time and forensic-cyber threat detection and response.