Defending and Operating in a Contested Cyber Domain

Abstract

The Air Force Scientific Advisory Board (SAB) Study, entitled *Defending and Operating in a Contested Cyber Domain*, addresses the Air Force's readiness to defend itself and operate in a contested cyber domain. This study continues the investigation started with the FY07 SAB Study, entitled *Implications of Cyber Warfare*, which pointed out the need for our forces to be able to "fight through" and continue to operate in the presence of attacks on our cyberspace infrastructure. The current study examines three major areas influencing fight through capability: *operational readiness*, the *defense industrial base (DIB)*, and *science and technology (S&T)*. Each area is characterized by a number of unique issues that lead to several distinct recommendations, but an important realization is that the areas are inter-related. Operational readiness poses challenges to the S&T community to conduct research and develop technologies that will enable the desired capabilities in current and future systems. These S&T products drive the DIB to upgrade and develop cyber enabled systems that, in turn, support operational readiness. This inter-relatedness, while essential for providing the superiority of the Air Force, can also produce new vulnerabilities that can be exploited by our adversaries.

The study team undertook a substantial number of visits to and received input from key stakeholders including: most of the MAJCOMs ultimately responsible for operational readiness; Strategic Command; the acquisition community responsible for developing and accrediting mission systems; US government agencies and departments that have essential roles in protecting the nation's critical infrastructure; contractors that are members of the defense industrial base; commercial vendors of IT capabilities and tools; venture capitalists who fund the development of cyber technologies; FFRDCs and research institutions that develop and assess new cyber technologies; and academic institutions that are at the forefront of cyber research.

The study investigated the nature of the cyber contested domain and concluded the following: (1) While there is evidence of extensive Air Force information and network exploitation today, it is expected that adversary effort will shift to direct attacks on mission system capabilities during conflict. Consequently, the driving concern needs to be Mission Assurance (MA) – a broader concept than Information Assurance (IA). (2) Attacks can occur and their effects can propagate across all cyber system layers (physical, software, mission and human organizational layers). (3) Attack trajectories are dynamic and may skip over layers in reaction to defensive actions.

The study has concluded that the Air Force will continue to face challenges to maintaining Mission Assurance in the face of potential cyber attack. The study made specific recommendations in all three areas and emphasized that coordinated, aggressive steps need to be taken to further improve fight through capabilities in a contested Cyber Domain.