Department of the Air Force
Scientific Advisory Board

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE
WASHINGTON DC

Implications Cyber Warfare Study

Abstract

Cyber warfare is becoming more and more a reality. Today, what was viewed as science fiction in the 1960s is becoming the reality of the 2000s, as our currently fielded information and computing systems are widely vulnerable to malicious attack. Challenges to be managed include: defining terminology, assigning organizational responsibilities; incorporating safe processes; educating participants; establishing strategies; defining tactics, techniques, and processes; working within the legal system; etc. Of course, identifying, developing, and applying suitable technologies is a critical component of cyber defense.

This past year, the USAF initiated a new organization within the 8th Air Force to pursue these challenges. Meanwhile, the USAF Scientific Advisory Board (SAB) was also asked to conduct a summer study into the implications of cyber warfare. A summary of our recommendations is relatively simple to express; however, understanding the subtleties of our recommendations will be important for anyone attempting to execute our recommendations.

This report summarizes the deliberations and conclusions of the 2007 SAB Summer Study Implications of Cyber Warfare. The Board was asked to assess vulnerabilities of USAF systems to disruption from cyber attack, identify scenarios for attack, and make recommendations for technology investment that might mitigate risks associated with such attacks.

Volume 1 of the report contains the viewgraphs and notes associated with the outbriefing of the study.

Volume 2 presents an overview of the study activities, the study findings, and major recommendations.

Volume 3 contains classified information and supporting rationale relevant to the derivation of our recommendations.

SAF PA Approval: 2025-0617