Cyber Situational Awareness
Abstract

The USAF Scientific Advisory Board's (SAB) Cyber Situational Awareness (CSA) Study was chartered to assess how well the Air Force understands what information systems will be employed in a given operation, how it monitors their condition, and how it reports that information to critical operational users. Awareness of the readiness of these systems is essential for an operational commander to ensure successful execution of the mission just as it is for aircraft, space systems, and munitions.

The Study conducted a comprehensive assessment of CSA with a primary focus on the needs of the Joint Force Air Component Commander (JFACC). The SAB interacted with and gathered extensive data from a wide cross-section of commercial and defense industry, military operational users, and military and commercial information systems providers to assess the state of practice in cyber situational awareness. The end result was a recommended path to meeting the threats and opportunities of synchronized warfighting across the Air-Space-Cyber domains.

Strong linkages and dependences exist between the air and space domains and the cyber domain. This creates substantial opportunities and threats from coordination of operational effects in the cyber domain with effects in the air and space domains. But, this requires a level of situational awareness in the cyber domain that enables synchronization of: (1) Mission assurance in the air, space, and cyber domains, (2) Supporting offensive cyber operations, and (3) Coordinated defensive cyber operations. The SAB found that the USAF is not on a path to reaching the level of CSA needed to meet the threats and opportunities presented by synchronized air-space-cyber operations. Also, the assessed current state of CSA is that the JFACC today has extremely limited access to real cyber situational awareness. However, recommended actions can bring CSA to a comparable level as SA in air and space. The Air Force should:

1. Develop and/or implement technologies to allow real-time assessment of confidentiality and integrity of cyber and mission systems beyond emphasis on availability. Technology development is required, but near-term insertion opportunities exist.

2. Ensure USCYBERCOM and the broader Intelligence Community provide actionable and timely threat intelligence and vulnerabilities to all JFACCs and other commanders to support improved CSA. Greater timeliness and responsiveness of intelligence products are key to CSA.

3. Develop technologies and processes to enable near-, mid- and far-term capabilities for dynamic mission mapping to support mission-aware cyber asset allocation. Near-real-time dynamic mission mapping is needed to achieve broad CSA.

4. Build and test an instantiation of the CSA-enabling architecture for the Air Operations Centers based on mission-critical functional partitions and out-of-band monitoring with deep data-analytic capabilities. A robust CSA-enabling architecture can be implemented for numerous missions.

5. Utilize automation to augment human decisions across the CSA hierarchy, allowing better use of limited manpower and enabling analyses of increasingly complex cyber activity. Appropriate uses of automation will lead to substantially improved CSA.

6. Address the human component of human-systems integration to provide an effective operational solution that meets the most urgent CSA needs of the Air Force. Appropriately skilled and experienced cyber personnel are essential for CSA.