Telecommunications Vulnerability and Survivability Assessments

Issue Background

One of the primary functions of the President's National Security Telecommunications Advisory Committee (NSTAC) is to provide technical information and advice in the identification and solution of problems that impact national security and emergency preparedness (NS/EP) telecommunications. Assessing the vulnerabilities of the telecommunications infrastructure and its survivability has been an important part of the NSTAC mission since its inception.

History of NSTAC Actions

The NSTAC has addressed the issue of telecommunications survivability from numerous perspectives. In 1986, the Telecommunications Systems Survivability (TSS) Task Force was directed to determine whether NSTAC recommendations had inconsistencies, whether the recommendations met the Government's NS/EP telecommunications policy requirements, and whether the Government effectively responded to the recommendations. The TSS Task Force was later tasked to assess the impact of new technologies on telecommunications survivability. The TSS Task Force completed reports on Government actions taken in response to NSTAC recommendations on commercial network survivability, commercial satellite survivability, electromagnetic pulse, automated information processing, and the national coordinating mechanism. The TSS Task Force also completed an assessment of the applicability of network management technology to NS/EP telecommunications survivability.

In 1990, the NSTAC completed an initial assessment of physical security of the public switched telephone network (PSTN) in response to a National Research Council report, concluding that industry and the Government were demonstrating substantial progress in addressing physical security vulnerabilities. Beginning in September 2000, the NSTAC Convergence Task Force analyzed potential security and reliability vulnerabilities of converged PSTN with Internet protocol (IP) networks. It noted that malicious attacks on PSTN and IP network gateways could impact overall network availability and reliability. In 2001, the Network Security/Vulnerability Assessments Task Force addressed public network security and made recommendations on: coordinating assistance related to preventing, mitigating, and responding to physical threats to the public network (PN); enhancing security of the control space of the PN; and wireless security issues.

Recent NSTAC Activities

During the NSTAC XXVI Cycle (March 2002-April 2003) the NSTAC remained active in evaluating vulnerabilities of telecommunications infrastructure. The Vulnerabilities Task Force assessed vulnerabilities associated with the concentration of critical telecommunications assets in telecom hotels and Internet peering points; the task force findings and recommendations were designed to help mitigate the overall risk for widespread impacts to the telecommunications infrastructure resulting from physical attacks. The Internet Security/Architecture Task Force studied vulnerabilities in pervasive software and protocols critical to the operation of the Internet; it recognized the need for industry and the Government to effectively and efficiently share information so that they can remain ahead of the threat as much as possible. The Wireless Task Force identified wireless security requirements and recommended methods to address wireless security challenges. As NS/EP users employ a greater variety of communications technologies during their missions, these types of assessments are increasingly important.