

# *The* NATIONAL STRATEGY FORUM REVIEW

An Online National Security Journal Published by the National Strategy Forum

## **Chapter 7: Cyber Security**

Cyber security is a rapidly growing, critical threat to U.S. national security because it affects our national economy, communications, business and commerce, academia and education, and society. A distinction is made between physical threats of the real world and the less well understood threats emanating from the cyber domain. Not only do cyber attacks threaten the U.S. critical infrastructure, but cyber information security lags far behind counter-threat measures and technology.

These issues were examined at a recent conference titled, “National Security Threats in Cyberspace” conducted by the American Bar Association Standing Committee on Law and National Security and the National Strategy Forum. The conference was underwritten as part of the McCormick Foundation Conference Series.

The U.S. is nearing total reliance on the integrity of cyberspace. This trend is irreversible. A small number of people, states, and organizations can manipulate cyberspace with devastating effect. The expense of cyber intrusion prevention systems is very high and can never be completely effective because the identity of the threat cannot be determined with a high degree of certainty.

For the immediate future, unless there is a technological breakthrough, society must adapt to the new reality—that cyber threats are inevitable and pervasive. The new phenomenon is that nefarious actors can cloak their identities in virtual worlds and operate freely with relative impunity.

Intrusive events could cause serious consequences, such as taking down the U.S. electrical grid, interfering with wire transfers of funds, and disrupting air traffic control systems, all of which could be deemed acts of war. The problem is that America would be unable to identify the enemy quickly and respond appropriately. Cyber intrusion is a shadow problem: it is difficult to anticipate the intrusion; it is difficult to determine when the crisis is over; and there is uncertainty as to when and if the problem has been resolved.

The U.S. response to cyber threat and cyber security is a work in progress with dual tracks: organizational/leadership and legal doctrine. The magnitude of the problem has been adequately defined by the government and the private sector. Unfortunately, response lags far behind increasing vulnerability. One of the barriers to resolving the problem is the reluctance of private sector organizations to report intrusions because of their concern that acknowledging vulnerability would adversely affect their stock value. The ideal approach is widespread international information sharing. However, privacy concerns arise because of fear of governmental intrusion. Any approaches that the government might take to cure the problem must consider privacy concerns.

There is a need for a coherent legal doctrine that enables law enforcement officials to investigate, prosecute, and sanction intruders. There are two problems in this regard: one, identification of the intruder; and two, many or most of the intrusions originate abroad, and there is no unified international legal regime to facilitate investigation, prosecution, and imposition of sanctions.

The first step is to overcome inertia. Until the recent creation of U.S. Cyber Command, headed by the director of the National Security Agency, there was no suitable governmental structure in place to address the problem. It remains to be seen how well it will work in practice, but it is a step in the right direction. Government communications are routed through privately owned communication networks, but inter-private sector coordination and government/private liaison and cooperation is lacking. At a minimum there is an urgent need for interagency cooperation. This would be imposed by Congress and a presidential leadership initiative. Although the challenge is technological, an effective bureaucratic organization coupled with an urgent plan will be needed to address and resolve the problem.

A relatively simple objective would be the recognition that a plethora of the information collected and stored is redundant. For example, retailers need only to authenticate purchasers—they do not need the bulk of financial and personal information that accompanies transactions.

Two decades ago, the U.S. was the leader of the new information age. Today, the world still looks to the U.S. for leadership in this area. For the moment, determined adversaries are in control; they have anonymity and skills that enable them to intrude successfully on relatively soft targets. A rapid and robust national response could significantly impede the ability of cyber threats to affect U.S. national security.

The U.S. needs a clear objective that is articulated with a high degree of precision. A unified strategy to address the threat has not been developed. While *ad hoc* tactics are in place, they are neither comprehensive nor do they implement a developed strategy. Time is of the essence because the intruders are acquiring skills that exceed development of countermeasures.