## Cyber Security: Recovery and Reconstitution of Critical Networks

## July 28, 2006

Richard C. Schaeffer, Director of Information Assurance, NSA

Answers to Questions for Response, 11/01/06

**1. Please identify for the Committee the greatest threats to the Internet in terms of foreign intelligence services, terrorist organizations and organized crime and their capabilities to disrupt, attack, or misuse the network in ways which would be detrimental to the nation.**

In a networked world, the barriers for entry into the technical exploitation and attack business are negligible compared to what they were when dedicated systems and point-to-point communications were the rule. Today, any nation state, terrorist organization, criminal enterprise, or disaffected individual needs only Internet access and modest computer science talent to remotely reconnoiter and attempt to manipulate computers and computer-controlled systems with ties to American economic and security interests. As the daily headlines attest, vulnerabilities in commodity information technology (IT) and unfortunate choices on the part of network operators and users routinely invite and enable such mischief. We will always have to guard against the high-end threats posed by the few unusually able and determined adversaries who are willing to mount complex, long-term operations to infiltrate critical networks. However, the greatest threat today though arises from the many low cost, low risk opportunities for adversaries to remotely search for network weaknesses and, sooner or later, parlay a meager investment into disproportionately potent political, financial, or military effects.

Foreign intelligence services are judged to pose the serious threat to the U.S. networks connected to the Internet. Also, sophisticated foreign intelligence services can leverage their traditional intelligence tradecraft, bringing multifaceted capabilities to support their Computer Network Operations.

Terrorist organizations have come to appreciate the value of the Internet and make great use of it for their own communications, research and propaganda purposes. Islamic extremists have been involved in Web page defacement/denial of service attacks, as in their response to the controversial cartoons published in Danish newspapers in early 2006. Some groups do have computer-literate personnel who could be used to conduct such operations.

**2. Hypothetically speaking and given NSA's limited authority, what role can/should or does NSA play or wish to play in bringing to bear the significant capabilities it has on improving the security of the network? In other words, what therefore can NSA do to provide enhanced security to all users of the network throughout the nation?**

The NSA has unique insight into the vulnerabilities of information systems and the components that comprise those systems, how adversaries can and do operate against them, and how various adversaries and attacks might be best countered. In the days when the national security systems that NSA is explicitly charged to help protect consisted mostly of government-specific components, the NSA had little reason or ability to contribute to the security of unclassified systems or commercial technology. Today, national security systems often rely on commercial products or infrastructure, or interact with systems that do. This has created important common ground between defense and broader homeland security needs and drives the NSA to work with others to raise the information assurance level of IT products and services generally. Accordingly, we've built, and continue to expand, partnerships with other U.S. government entities, private industry and academia. (Our Statement for the Record gives a few examples). In addition to continuing to produce security solutions for the U.S. national security community as we have in the past for many years, we also aim to translate our unique insight (including knowledge derived from classified activities and other sensitive sources) into design guidance for IT suppliers; acquisition and architectural guidance for IT buyers; best practices and situational awareness for system users and operators; recommended doctrine for security authorities; and tools, techniques, and training for fellow (or, in the case of our academic excellence program, future) security practitioners. Such efforts will continue to grow.

**3. Does NSA believe it is possible to provide requisite protection for users (defined as all users: personal, business and government) of the network to assure that they can maintain the confidentiality, integrity, and availability of their communications and data and business transactions? If not, what are the most significant things users can do to resist most of the attacks and reduce the vulnerabilities inherent in the system?**

"Perfect security" wasn't attainable even within the narrow and relatively easily protected confines of the national security community in the days before the network revolution. It surely isn't within the reach of all network users today, and won't be tomorrow either. With that said, the situation needn't be as bleak as it often is. Frustratingly, the same networks are often found vulnerable to, or even, actually victimized by, the same attack over and over again, and more frustratingly, even when the attack is well known and adequate protective measures are readily available. This is one area where the NSA's insight is not unique. Any number of public and private entities publish lists of powerful computer security basics – things like using strong passwords, promptly installing all software patches, encrypting data at rest, disabling unused computer processes, and allowing users only those privileges which are essential for the work they need to do. It's analogous to the simple precautions we take to protect our homes, like locking doors and windows and installing deadbolts. For most users and system administrators, disciplined attention to just a few basics can be the difference between inviting trouble and actively discouraging it. Users need to understand the added security risk of self-published information in aggregation on the Internet. They must resist unknown eye-catching applications claiming to bring a diversion to its readers.

**4. GAO has reported that critical infrastructures extensively rely on information systems and electronic data to carry out their missions. Could a significant Internet disruption pose a threat to national security by interfering with these critical infrastructures?**

Many systems that are critical to the nation's security have some connectivity to the Internet or to utilities, communications services, or other infrastructure that make some use of the Internet. In theory, essential national security operations are designed to not wholly depend on the Internet or any uncontrolled external infrastructure, and to be able to function adequately, although perhaps with some degradation, despite modest outages. The complexity of modern operations and networks, however, probably precludes saying that this is always true in practice. It's not unreasonable to think that a significant and sustained Internet disruption might affect at least a few critical functions immediately, and perhaps impact some more over time as unanticipated "ripple" effects emerged.

**5. It seems that nation states and disciplined transnational organizations can employ a high level of tradecraft to hide attacks or create successful attacks that do not cause an operational impact on a government agency or commercial enterprise. How concerned are you that the U/S. is being victimized by such attacks and what if anything can be done to develop tools for detecting, analyzing, and stopping these covert attacks?**

It is indeed possible for certain types of network intrusions to go undetected for quite some time, and such attacks are of great concern across and beyond the national security community. The threat is being addressed on three fronts. First, both the public and private sectors continue to invest in improving intrusion detection technology. No one pretends that this alone will solve the problem, but progress is being made and every step forward raises our adversaries' operational costs and risks. Second, the public and private sectors also continue to invest in making information technology less vulnerable to unauthorized remote access. Again, we're not going to make attacks impossible, but we can push potential adversaries towards fewer and more demanding attack vectors, and this makes the detection problem more tractable. Finally, it's important to remember that although the problem is tied to technology, the solution need not be. Our efforts to spot and stop attackers at our cyber perimeters must be augmented with aggressive intelligence collection and all source analysis aimed at uncovering our adversaries' plans and capabilities and compromising their operations. Intelligence has long been used in this way to bolster the nation's counterespionage capabilities and to help warn of conventional military attack. It must similarly be a component of our cyber defense.