Visions of the Information Society

Network security: Protecting our critical infrastructures[1]

EXECUTIVE SUMMARY

Cyberspace—the Internet and other computer-based networks—is becoming one of the most important infrastructures that characterize modern societies. Among the networks of cyberspace are systems that control and manage other infrastructures such as banking, emergency services, energy delivery, and many transportation and military systems. Thus, many regions' economic and social stability may depend on these networks. The computer-communications networks of cyberspace are the underlying technological bases that will enable all "visions of the information society."

Dependencies on networks for communication and business operations continue to grow along with the growth of cyberspace. Today, the Internet in particular, which has grown without any planning or central organization, is a vast network of networks. As of 1989, the Internet interconnected around 20 countries and 100,000 hosts. The majority of those hosts were located in the United States. As of early 2002, there were hundreds of millions of host computers[2] and perhaps at least a half billion users worldwide[3]. More than half of the users are now located outside the U.S. and perhaps a quarter outside of the OECD countries. It is increasingly beyond the scope of single nations to control users who would inflict damage to or via the systems of cyberspace.

 This paper was written by Professor Seymour Goodman, Pamela B. Hassebroek and Professor Hans Klein of the Georgia Institute of Technology, and is one of six ITU *Visions of the Information Society* papers. For more information, go to www.itu.int/visions. The full paper will be made available in the spring of 2003.

2 Source: Network Wizards Survey, http://www.isc.org/ds/WWW-200207/index.html

3 Source: NUA Survey, http://www.nua.ie/surveys/how_many_online/

Destructive acts using computer networks have cost billions of dollars and increasingly threaten the resources of network-connected critical infrastructures. Threats[4] to network infrastructures are potentially extensive not only as their value increases in terms of the infrastructures themselves, the value of hosted services, and the value of what is located on them, but also because of their widespread and low-cost access. These infrastructures of cyberspace are vulnerable due to three kinds of failure: complexity, accident, and hostile intent. However, we lack a comprehensive understanding of these vulnerabilities—largely because of the extraordinary complexities of many of the problems, and perhaps from too little effort to acquire this understanding. But there is ample evidence that vulnerabilities are there: examples of all three kinds of failure abound, and vulnerabilities are found almost every time people seriously look for them.

Within this vast, complex cyberspace system, it is so simple to connect that users of today's systems require few skills and little understanding of the underpinnings. Thus, we require not only technical protections but also an awareness and alertness on the part of all users to the dangers inherent in the use of any system connected to a network. Attacks so far have been limited. However, many believe that it is only a matter of time before prolonged, multifaceted, coordinated attacks are going to find those network vulnerabilities and exploit them to produce serious consequences. Prudence dictates better protection against accidents and attacks before things get much worse. All realizations of "visions of the information society" are going to be severely limited if the people in that society do not trust or feel secure with the underlying infrastructures.

Alertness to the dangers requires protections that can stay abreast of changing attack modes. An essential part of a defence strategy is continual network monitoring and innovation in monitoring techniques to minimize the potential for damage from the actions of cybercriminals. However, there are multiple stages of defence and a cycle of understanding, which is a complex system in itself. The overlapping stages of prevention and/or thwarting an attack, incident management, reconstituting after an attack, and improving defender performance by analysis and redesign are essential to understanding the elements of each network intrusion attempt. Invariably, gaining this understanding involves some ability to trace the route of attack to the source so that the attacker can be identified. International cooperation can help to bring about success in this effort, in situations where it would be impossible otherwise.

Faced with the possibility of disruption of critical infrastructures in ways that could have serious consequences, governments should be expected to implement prudent defence plans. Each country should first identify those infrastructures and their interdependencies that are critical to its survival and to its social

4 "Vulnerabilities" are weaknesses that can be exploited. "Threats" do the exploiting. Threats are most often human and hostile, but could also be natural or accidental, e.g., a weather-induced power outage that exploits the vulnerability of no back-up power supply.

and economic well-being. Planning for specific defences of these identified infrastructures may usefully include both passive[5] and active defence forms.

Since an infrastructure system is typically a mix of public and private ownership, the various owners are likely to have different motivations for and roles in such planning for its protection. Private owners will seek solutions that maintain revenues and the confidence of their markets. Governments will pursue policies that focus on longer-term aspects of protection, seeking to protect their economies and national security, to maintain law and order, and to reduce cumulative losses.

The combination of diversity in its users and its international dimension contributes much to the promise of cyberspace networks and, at the same time, creates the most difficult problems. Its international character is central to the "vision" for many of the network's visionaries. And this characteristic creates a requirement of international cooperation for increasing the security of the network's infrastructures. Defence policies and practices must apply globally to be effective. The ways in which cooperation can help to increase security are numerous, but in this paper, we focus on some of the most clear and expedient avenues to curtailment of criminal activity. These activities include: standardization, information sharing, halting attacks in progress, legal coordination, and providing aid to developing nations.

In many aspects of network connection, the issue of standards offers both an opportunity for improvement in security and an opportunity for clearer avenues to abuse. Standard protocols, applications, workstation and server configurations all play a role in providing either a system of trust or a platform for criminals. Security as a clear and present priority for network operation needs to be a prime focus for future development standards and remedial activity.

Information sharing is required in order to develop security standards for successful product development and effective standard security practices. International collaboration in all aspects of network operations can help to ensure the best possible protection for the valuable assets of its users. A cyberattack in progress can be minimized by the widespread communication of such an event to users and system operators. Information sharing is also essential in order to locate and prosecute cyber criminals.

One form of international cooperation that has been much discussed is the potential for harmonization of laws among countries that can help to prevent cybercrime and provide a deterrent to cybercriminals. Criminals may currently circumvent jurisdictions and places with strong technical and legal barriers in order to find the cracks in the system where it is safe to create problems. We need to close these cracks.

5 Passive defence is essentially target hardening. Examples include internal use of various technologies and products, such as firewalls and cryptography, and procedures to protect the assets owned by an individual or organization. Active defence, in contrast, imposes serious risk or penalty to the attacker.

All of these forms of cooperation work better, when all nations are equally capable of carrying their share of responsibilities. At present, this is not the case. There are many countries where people with high-level technical skills are not present in adequate numbers. A cooperative effort among nations can assist with these needs for training and equipment.

Achieving global coordination in these areas is not an easy task. It requires legal and administrative policies in order to create a framework for global interaction. Policies include setting well-defined boundaries for legal actions, the creation of an international organization, and possibly a multilateral treaty. Cybercrime and the potential for cyberterrorism not only creates a requirement for intergovernmental machinery, but, given our growing dependencies on the networks, adds a sense of urgency to the task.

Given the urgency of the problem as well as the difficulty of constructing global frameworks, it is appealing to look for shortcuts. One attractive alternative would employ private coordination, perhaps based on the model of the Internet Engineering Task Force (IETF). However, private groups cannot contribute directly in active defence or in legal harmonization. In addition, privatization allows a policy process that may lack proper international representation and democratic participation. Such deficiencies in an international organization could create barriers to effectiveness in the process of addressing network security.

We believe that a necessary way to proceed is through international, intergovernmental coordination. The types of cooperation described above suggest a highly interactive partnership in pursuit of common goals. We present in this paper what we conceive as the ideal model for such a construction. We see four required features in this model: First, all cooperating countries would share a common baseline perception of what constitutes criminal behavior in cyberspace. Second, each of the governments of the world would have substantial competence to deal with the problem of preventing, thwarting, etc. and punishing attacks on cyber systems. This includes capabilities and policies in passive defence to provide effective security within each government's jurisdiction. Third, each would have substantial capability in active defence, and a competent national authority for engaging in active defence. Finally, international responses to transnational attacks would be covered under a near-universal umbrella convention that would permit timely action under established procedures. While initiatives exist in international cooperation to increase security, the present reality is still far from this ideal model.