Cyber Threat Trends and US Network Security

Statement for the Record to the Joint Economic Committee

Lawrence K. Gershwin
National Intelligence Officer for Science and Technology
21 June 2001

(as prepared for delivery)

Mr. Chairman, thank you for the opportunity to provide a statement on cyber threat and critical infrastructure issues. Late last year the NIC published a report called *Global Trends 2015* which presented the results of a close collaboration between US Government specialists and a wide range of experts outside the government, on our best judgments of major drivers and trends that will shape the world of 2015.

In *2015* we anticipate that the world will almost certainly experience quantum leaps in information technology (IT) and in other areas of science and technology. IT will be the major building block for international commerce and for empowering nonstate actors. Most experts agree that the IT revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid-eighteenth century.

- The integration—or fusion—of continuing revolutions in information technology, biotechnology, materials science, and nanotechnology will generate dramatic increases in technology investments, which will further stimulate innovation in the more advanced countries.

The networked global economy will be driven by rapid and largely unrestricted flows of information, ideas, cultural values, capital, goods and services, and people: that is, globalization. This globalized economy will be a net contributor to increased political stability in the world in 2015, although its reach and benefits will not be universal. In contrast to the Industrial Revolution, the process of globalization will be more compressed. Its evolution will be rocky, marked by chronic financial volatility and a widening economic divide.

Cyber Threat Concerns

As the Director of Central Intelligence testified to the Congress earlier this year, no country in the world rivals the US in its reliance, dependence, and dominance of information systems. The great advantage we derive from this also presents us with unique vulnerabilities.

- Indeed, computer-based information operations could provide our

adversaries with an asymmetric response to US military superiority by giving them the potential to degrade or circumvent our advantage in conventional military power.

- Attacks on our military, economic, or telecommunications infrastructure can be launched from anywhere in the world, and they can be used to transport the problems of a distant conflict directly to America's heartland.

Hostile cyber activity today is ballooning. The number of FBI computer network intrusion cases has doubled during each of the past two years. Information derived from the Internet indicates that since last September the number of hacker defacements on the Web have increased over tenfold.

Meanwhile, several highly publicized intrusions and computer virus incidents such as the recent intrusion into the California Independent System Operator—the non-profit corporation that controls the distribution of 75 percent of the state's power—have fed a public—and perhaps foreign government—perception that the networks upon which US national security and economic well-being depend are vulnerable to attack by almost anyone with a computer, a modem, and a modicum of skill. This impression, of course, overstates the case.

US Networks as Targets

Information from industry security experts suggests that US national information networks have become more vulnerable—and therefore more attractive as targets of foreign cyber attack. An independent group of security professionals created the "Honeynet Project," placing virtual computers on the Internet to evaluate threats and vulnerabilities that currently exist. The results were stunning: the average computer placed on the Internet will be hacked in about 8 hours. University networks are even worse, with an unsecured computer system being hacked in only about 45 minutes.

- The growing connectivity among secure and insecure networks creates new opportunities for unauthorized intrusions into sensitive or proprietary computer systems within critical US infrastructures, such as the nation's telephone system.

- The complexity of computer networks is growing faster than the ability to understand and protect them by identifying critical nodes, verifying security, and monitoring activity.

- Firms are dedicating growing, but still insufficient, resources to the defense of critical US infrastructures against foreign cyber attack —perceived as a low likelihood threat compared to routine disruptions such as accidental damage to telecommunications lines.

Mainstream commercial software—whose vulnerabilities are widely known—is replacing relatively secure proprietary network systems by US telecommunications providers and other operators of critical infrastructure. Such commercial software includes imported products that provide

opportunities for foreign implantation of exploitation or attack tools.

- US government and defense networks similarly are increasing their reliance on commercial software.

Opportunities for foreign placement or recruitment of insiders have become legion. As part of an unprecedented churning of the global information technology work force, US firms are drawing on pools of computer expertise that reside in a number of potential threat countries.

- Access to US proprietary networks by subcontractors of foreign partners is creating “virtual” insiders whose identity and nationality often remain unknown to US network operators.

- Foreign or US insiders were responsible for 71 percent of the unauthorized entries into US corporate computer networks reported to an FBI-sponsored survey last year.

- Despite growing interconnectivity, control networks—whose compromise could disrupt critical US infrastructures such as power or transportation—are designed to be less accessible from outside networks, according to industry experts. In addition, many control networks use unique, proprietary, or archaic programming languages thought to be—and clearly intended to be—poorly understood by hackers. Nonetheless, we remain concerned that increasing use of the Internet by critical infrastructures and the US military combined with increasing convergence to just a few software systems could leave the US open to more damaging attacks.

Growing Foreign Capabilities

Advanced technologies and tools for computer network operations are becoming more widely available, resulting in a basic, but operationally significant, technical cyber capability for US adversaries.

Most US adversaries have access to the technology needed to pursue computer network operations. Computers are almost globally available, and Internet connectivity is both widespread and increasing. Both the technology and access to the Internet are inexpensive, relative to traditional weapons, and require no large industrial infrastructure.

- The tradecraft needed to employ technology and tools effectively however—particularly against more difficult targets such as classified networks or critical infrastructures—remains an important limiting factor for many of our adversaries.

Hackers since the mid-1990s have shared increasingly sophisticated and easy-to-use software on the Internet, providing tools that any computer-literate adversary could obtain and use for computer network reconnaissance, probing, penetration, exploitation, or attack. Moreover, programming aids are making it possible to develop sophisticated tools with only basic programming skills.

- Globally available tools are particularly effective against the mechanisms of the Internet, but specialized tools would be needed

against more difficult targets, such as many of the networks that control critical infrastructures.

Even with technology and tools, considerable tradecraft also is required to penetrate network security perimeters and defeat intrusion detection systems—particularly against defensive reactions by network security administrators. Tradecraft also will determine how well an adversary can achieve a targeted and reliable outcome, and how likely the perpetrator is to remain anonymous. Attackers must tailor strategies to specific target networks—requiring advanced and continued reconnaissance to characterize targets and ensure that exploitation tools remain effective in the face of subtle changes to computer systems and networks.

- Cyber attacks against less well-defended networks still would require prior identification of critical nodes and a preplanned campaign, if the attacks were to achieve a strategic impact.

Potential Actors and Threats

Let me talk about some of the groups that will challenge us on the cyber front.

Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, such hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical US networks—and even fewer would have a motive to do so.

Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack.

- In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

Hacktivists

A smaller foreign population of politically active hackers—which includes individuals and groups with anti-US motives—poses a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures.

Pro-Beijing Chinese hackers over the past two years have conducted mass cyber protests in response to events such as the 1999 NATO bombing of China’s embassy in Belgrade. Pro-Serbian hacktivists attacked a NATOwebsite during Operation Allied Force. Similar hacktivism accompanied the rise in Israeli-Palestinian clashes last year and several

thousand web page defacements and some successful denial-of-service attacks were associated with the recent EP-3 incident.

Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft, respectively, and through their ability to hire or develop hacker talent.

- Japanese syndicates used Russian hackers to gain access to law nforcement databases, evidently to monitor police investigations of their operations and members, according to a press report last year.

- According to press reports, a Mafia-led syndicate this year used banking and telecommunications insiders to break into an Italian bank's computer network. The syndicate diverted the equivalent of $115 million in European Union aid, to Mafia-controlled bank accounts overseas before Italian authorities detected the activity.

Foreign corporations also could use computer intrusions to tamper with competitors' business proposals, in order to defeat competing bids or unfairly position products in the marketplace.

- Computer network espionage or sabotage can affect US economic competitiveness and result in technology transfer—directly through roduct sales, or indirectly—to US adversaries.

Because cyber criminals' central objectives are to steal, and to do so with as little attention from law enforcement as possible, they are not apt to undertake operations leading to high-profile network disruptions, such as damage to US critical infrastructures.

- Major drug trafficking groups, however, could turn to computer network attacks in an attempt to disrupt US law enforcement or local government counternarcotics efforts.

- Organized crime groups with cyber capabilities conceivably could threaten attacks against critical infrastructure for purposes of extortion.

Moreover, rampant criminal access to critical financial databases and networks could undermine the public trust essential to the commercial health of US banking institutions and to the operation of the financial infrastructure itself.

- In addition, criminal computer network exploitation could inadvertently disrupt other infrastructures.

Terrorists

Traditional terrorist adversaries of the United States, despite their intentions to damage US interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited

cyber threat. In the near term, terrorists are likely to stay focused on traditional attack methods—bombs still work better than bytes—but we anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.

National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life, to extensive infrastructure disruption. Among the array of cyber threats, as we see them today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to US critical infrastructures.

- The tradecraft needed to employ technology and tools effectively remains an important limiting factor—particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years or so, only nation states appear to have the discipline, commitment and resources to fully develop capabilities to attack critical infrastructures.

Future Tools and Technology

New cyber tools and technologies are on the way for both the offense and defense. For example, because networks—and their vulnerabilities—are evolving so rapidly, new tools for network mapping, scanning, and probing will become increasingly critical to both attackers and defenders. Either side could apply research in autonomous software “agents”—intelligent, mobile, and self-replicating software intended to roam a network gathering data or to reconnoiter other computer network operations.

Incremental deployment of new or improved security tools will help protect against both remote and to some extent inside threats. Technologies include better intrusion detection systems, better methods for correlating data from multiple defensive tools, automated deployment of security patches, biometric user authentication, wider use of encryption, and public key infrastructures to assure the authenticity and integrity of e-mail, electronic documents, and downloaded software. However, the defense will be at some disadvantage until more fundamental changes are made to computer and network architectures—changes for which improved security has equal billing with increased functionality.

For attackers, viruses and worms are likely to become more controllable, precise, and predictable—making them more suitable for weaponization. Advanced modeling and simulation technologies are likely to assist in identifying critical nodes for an attack and conducting battle damage assessments afterward.

- In addition, tools for distributed hacking or denial of service—the coordinated use of multiple, compromised computers or of independent and mobile software agents—will mature as network connectivity and bandwidth increase.

The rapid pace of change in information technology suggests that the appearance of new and unforeseen computer and network technologies and tools could provide advantages in cyber warfare to either the defender or the attacker. Wildcards for the years beyond 2005 include the possibility of fundamental shifts in the nature of computers and networking, driven, for example, by emerging optical technologies. These changes could improve processing power, information storage, and bandwidth enough to make possible application of advanced software technologies—such as artificial intelligence—to cyber warfare.

- Such technologies could provide the defender with improved capabilities for detecting and attributing subtle malicious activity, or could enable computer networks to respond to attacks automatically.

- They could provide the attacker with planning aids to develop an optimal strategy against a potential target and to more accurately predict effects.

Implications

Despite the fundamental and global impact of the information revolution, the reliance of critical US activities on computer networks, and the attention being devoted to information operations, uncertainty remains whether computer network operations will evolve into a decisive military weapon for US adversaries.

- To a degree that we cannot estimate, emergency measures to compensate for computer network disruptions will be available to maintain some basic level of services—as demonstrated during the Y2K rollover. Adversaries, therefore, may never overcome the planning uncertainties that derive from a US potential to work around even severe degradations in network performance.

Nonetheless, a recent CIA report “Preserving National Security in an Increasingly Borderless World” suggests that the information age and advanced technology will embolden our adversaries to target what they perceive as our vulnerabilities rather than to engage US forces directly:

- Weapons of “mass effect,” such as denial-of-service attacks, are likely to proliferate in the coming decade.

- As the technology revolution accelerates, civilian technology will increasingly drive military technology, and the civilian sector will increasingly become the point of attack for enemies of the United States.

Whether or not foreign computer network operations mature into a major combat arm, however, they will offer an increasing number of adversaries new options for exerting leverage over the United States—including selection of either nonlethal or lethal damage and the prospect of anonymity.

- Adversaries will be able to use cyber attacks to attempt to deny the United States its traditional continental sanctuary with attacks on

critical infrastructures. They could exploit US legal and conceptual controversies relating to defending privately operated networks with US Government resources and the separation of the US domestic and foreign security establishments.

Adversaries also could use cyber attacks to attempt to slow or disrupt the mobilization, deployment, combat operations, or resupply of US military forces. Attacks on logistic and other defense networks would be likely to exploit heightened network vulnerabilities during US deployment operations—complicating US power projection in an era of decreasing permanent US military presence abroad.

Whatever direction the cyberthreat takes, the United States will be confronting an increasingly interconnected world in the years ahead. As the CIA report points out, a major drawback of the global diffusion of information technology is our heightened vulnerability. Our “wired” society puts all of us—US business, in particular, because they must maintain an open exchange with customers—at higher risk from enemies. In general, IT’s spread and the growth of worldwide digital networks mean that we are challenged to think more broadly about national security. We should think in terms of global security, to include the dawning reality that freedom and prosperity in other parts of the world are inextricably bound to US domestic interests.

TOP