Address by John C. Gannon
Assistant Director of Central Intelligence for Analysis and Production
to
The National Security Telecommunications and Information Systems Security Committee
3 April 2001

(as prepared for delivery)

Thank you. It is a special pleasure to be among such distinguished speakers today to address such an important organization as the NSTISSC. Your conference organizers asked me to share our perspective on the cyberthreat, over the next several years. I'll be happy to do that this morning.

To assist in my discussion of this important topic, I will draw from the work the National Intelligence Council has done on **Global Trends 2015**, with which I hope you are familiar, and on other estimative work undertaken by the NIC over the past year, especially by our National Intelligence Officer for Science and Technology, Larry Gershwin. It is useful, I think, to put the cyber threat into the context of a major S&T revolution over the next fifteen years.

In **Global Trends 2015** we anticipate that the world will almost certainly experience quantum leaps in information technology (IT) and in other areas of science and technology. The continuing diffusion of IT and new applications of biotechnology will be at the crest of the wave. Information Technology 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.

- Older technologies will continue lateral “sidewise development” into new markets and applications through 2015, benefiting US allies and adversaries around the world who are interested in acquiring early generation ballistic missile and weapons of mass destruction (WMD) technologies.

- Biotechnology will generate medical breakthroughs that will enable the world’s wealthiest people to improve their health and increase their longevity dramatically. At the same time, genetically modified crops will offer the potential to improve nutrition among the billions of malnourished people in the world.

- Breakthroughs in materials technology will generate widely available products that are multi-functional,environmentally safe, longer lasting, and easily adapted to particular consumer requirements.

- On the downside, disaffected states, terrorists, proliferators, narcotraffickers, and organized criminals will take advantage of the new high-speed information environment and other advances in technology to integrate their illegal activities and compound their threat to stability and security around the world.

Globalization

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 and timelines of globalization will be more compressed. Its evolution will be rocky, marked by chronic financial volatility and a widening economic divide.

- Regions, countries, and groups left behind will face deepening economic stagnation, political instability, and cultural alienation. These entities will foster political, ethnic, ideological, and religious extremism, along with the violence that often accompanies these phenomena . These disaffected entities will force the United States and other developed countries to remain focused on “old-world” challenges while simultaneously concentrating on the implications of “new-world” technologies.

GT2015 “Bottom Line”

We do make an effort in GT2015 to cut through the scary scenarios to a broad judgment about the cyber threat:

- Increasing reliance on computer networks is making critical US infrastructures more attractive as targets. Computer network operations today offer new options for attacking the United States within its traditional continental sanctuary—potentially anonymously and with selective effects. Nevertheless, we do not know how quickly or effectively adversaries such as terrorists, proliferators, narcotraffickers or disaffected states will develop the tradecraft to use cyber warfare tools and technology, or, in fact, whether cyber warfare will ever evolve into a decisive combat arm.

- We need, therefore, to assess carefully the capabilities of these varied groups in a continuing integrated threat assessment rather than panic and run. The cyber threat is a call to action—collaborative and concerted action across NSTISSIC agencies—not a cry to surrender. For those nations with a decisive technological advantage, like the United States, we need to remind ourselves that keeping that technological advantage will be our best line of both defense and offense.

Which is to say, we need to do a lot more work on this and to keep you all in the loop as we go along.

Perspective from 2001

Let's jump back from 2015 for a few moments and talk more concretely about the threats we face today.

Hostile cyber activity today is ballooning. The number of FBI computer network intrusion cases has doubled during each of the past two years. Meanwhile, several highly publicized intrusions and computer virus incidents since 1998 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

It is true that information from industry security experts suggests that US national information networks have become more vulnerable—and therefore more attractive as a target of foreign cyber attack.

- 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. The prospects for a cascade of failures across US infrastructures are largely known and understood.

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

Nonetheless, 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. US government and defense networks similarly are increasing their reliance on commercial software. Such commercial software includes imported products that provide opportunities for foreign implantation of exploitation or attack tools.

Finally, 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, such as Russia.

- 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.

Despite these growing vulnerabilities, however, the most important US targets remain difficult to compromise. Compromising such targets requires more advanced tools and tradecraft, such as recruiting an insider.

- 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 the growing interconnectivity I've stressed this morning, 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.

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 information 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 the networks that control many 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 military networks, such as logistics for example, still would require prior identification of critical nodes and a preplanned campaign, if the attacks were to achieve a strategic impact such as delaying a US force deployment.

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 NATO Website during Operation Allied Force. Similar hacktivism accompanied the rise in Israeli-Palestinian clashes last year.

Hackers for Hire

Government and criminal organizations have the resources to recruit hacker talent and the motivation to guide that technical talent with sophisticated tradecraft in order to turn it toward long-term objectives that could threaten the United States.

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 enforcement 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 last 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.

- Computer network espionage or sabotage can affect US economic competitiveness and result in technology transfer--directly through product 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. (Nonetheless, we will be on the alert for new information that could alter this judgment. We anticipate that 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. Among the array of cyber threats, as we see them today, only government-sponsored programs are developing capabilities with the prospect of causing widespread, long-duration damage to US critical infrastructures.

China (to name just one example) is expanding cyber related military training and is already incorporating cyber warfare into military exercises, according to press reporting.

- President Jiang last year stated that wars were passing from the stage of “mechanized warfare” to that of “information warfare.”

- A Chinese presidential decree last year established a military university whose mission includes training soldiers in information warfare, among other communications-related fields, according to a Chinese press report.

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.

For defenders, incremental deployment of new or improved security tools will help protect against both remote and 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.

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. Other capabilities likely by 2005 include self-modification to defeat signature recognition, remote control, stealthy propagation, and the ability of a single tool to affect multiple, mainstream operating systems.

- 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. Let us hope I am right in this judgment.

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.

Implications for Intelligence

Whatever direction the cyberthreat takes, the United States Government will be confronting an increasingly interconnected world in the years ahead. This is the core message of GT2015. We will have to develop, in response, greater communications and collaboration across the agencies of our own Government, with other governments, and with the corporate world. Interagency cooperation will be essential to understanding the cyberthreat, as well as other transnational threats that will crowd our agenda, and to responding effectively with

interdisciplinary strategies. Consequence management of a major attack on a critical US infrastructure would involve virtually all agencies of the Federal Government, State, and local governments, foreign governments, law enforcement, the military, the medical community, and the media. NSTISSC and the Intelligence Community clearly have a lot of work to do if we are to understand this evolving threat and to be prepared to deal with it.

This dramatic story has no definite ending today. Clearly, the Intelligence Community has a major challenge ahead to serve you and the American people.

Thank you.