Protecting America's Critical Infrastructure--Preventing an Electronic Pearl Harbor
By Edward V. Badolato

Introduction

Following a Justice Department review of the nation's vulnerability to terrorism in the wake of the Oklahoma City bombing, and in recognition of comparable threats to our national infrastructures, President Clinton signed Executive Order 13010 on July 15, 1996, establishing a joint Government-industry Presidential Commission on Critical Infrastructure Protection.

There was concern that terrorists might now have access to the sophisticated technology and unconventional tools that would allow them to attack our economy and critical infrastructure using advanced computer technology. With this in mind, the Commission gathered top individuals from a variety of backgrounds in the private sector and Government to design a joint strategy to protect and assure the continued reliable operation of U.S. critical infrastructures--telecommunications, electric power, gas and oil (storage and transportation systems), banking and finance, transportation, water supply, and vital government services.

After 15 months of study, including public meetings, conferences, simulations, and over 6,000 contacts with associations and corporations, the Commission forwarded its report, "*Critical Foundations–Protecting America's Infrastructures*" to the President in October 1997. The Commission made six key findings in their comprehensive report:

- The critical infrastructures are at serious risk today; and the capability to do harm is now readily available.

- There is no single warning system to alert us about an impending attack.

- At present, Government and industry don't readily share information that might give warning of a cyber attack.

- Federal research and development budgets aren't funded to study threats and vulnerability to infrastructure systems.

- A new way of thinking about government and industry relations is needed as a result of our dependence on information systems, the astonishing rapid growth of automated systems and their pervasive impact on critical infrastructures.

- The eight critical infrastructures are so central to our national defense and our economic well being that it is time to lay the foundations for their future security on a new form of cooperative partnership between the private sector and government.

System Vulnerability--the Energy Industry

It was clear from the Commission report that the accelerating reliance on computers makes our infrastructures more vulnerable. Access to U.S. infrastructure's information systems can come from all over the world, blurring traditional boundaries and jurisdictions. U.S. security, economic

prosperity and social well being are increasingly relying on complex and interdependent infrastructures whose lifeblood is energy- oil, natural gas, and electric power. The incapacity of the oil, gas, or electric power industries due to vulnerabilities could to serious harm to U.S. national security. The US energy infrastructure is critical to our economy and our national defense, and is the key to all of the other infrastructures.

The U.S. energy infrastructure is the most reliable and robust in the world. Energy shortages and outages are rare. But today, the reliability of electricity is becoming more critical to the nation's competitiveness and standard of living in the Information Age. Without electrical power, other critical infrastructures such as telecommunications, banking, and finance cannot function. The transportation infrastructure would cease to operate because it relies almost exclusively on oil products for mobility and telecommunications for coordination.

The Range of Threats

The sources of potential threats to infrastructures can be physical threats to tangible property and cyber threats--electronic, radio-frequency, or computer-based attacks on information or communications components used in critical infrastructures' process control systems. For decades US companies have generally done an outstanding job protecting themselves against natural and physical threats. The cyber threat is not like physical security where you can post guards with guns behind fences. The cyber threat keeps changing so there is no end to it.

The threat has changed and new thinking is required. No longer does the U.S. face a Soviet military capability linked to a hostile intent. Today, an improper command, remotely sent over a network to a power generating station's control computer could be just as effective as a full scale explosive attack, and the perpetrators would be harder to identify and apprehend. A recent review of elements of our critical infrastructure by telecommunications experts pointed out that our current rudimentary control center protection methods eases the way for hacker penetration, and that weak cyber security could allow a relatively simple attack to cause major disruptions of our electric power system.

The threat to our national infrastructure is a potential threat based on existing cyber capabilities available to anyone with hostile intent---hackers, disgruntled insiders, ordinary criminals, organized crime groups, political dissidents, terrorists, foreign intelligence agencies, or nation states or sub-national entities that operate with or without their nations' support. They can enter information and process control systems to read, modify, and copy sensitive company information, block legitimate user access, scan and report the vulnerabilities of a company's computer systems, and make detection of computer intrusions difficult.

Foreigners could hire hackers to disrupt power transmission or electric power distribution systems. They could also include cyber warfare in their anti-US warfighting strategies. For example, CIA Director George Tenet recently testified before the Senate Governmental Affairs Committee that China and others have begun to focus on U.S. computer networks as a target for possible hi-tech cyber attacks that could cripple anything from telephones to electricity.

China allegedly has the world's largest cyber warfare program, and Tenet felt that the scope of the overall threat was serious. He told the Senators, "We know with specificity of several nations that are working on developing an information warfare capability. It is clear that nations developing these programs recognize the value of attacking a country's computer systems both on the battlefield and in the civilian arena." Tenet went on to quote comments in an article in China's official newspaper, the *People's Liberation Daily*, "An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. economy."

The Economic Threat

In addition to the foreign national security threat from cyber attacks, there is the economic threat. Industry has been experiencing an increasing number of cyber-related incidents:

- Industry security directors find that "insiders" cause an estimated 80 percent of overall security-related incidents. The number of "insider" cyber security problems will probably increase in the future because more hacker tools and techniques are becoming available to anyone with the ability to point, click, and download from the Internet.

- Hackers abused credit cards, telephone switches, and billing systems. For example, the “Five Hacker Group” broke into computers at the Bank of America, ITT and Martin Marietta.

- The FBI reported in 1997 that 23 nation states engage in economic espionage. They range from foreign government-controlled corporations targeting information from its American telecommunications competitors to foreign firms that steal micro-processing manufacturing technology.

These are not isolated cases. They are examples of thousands of cyber-related incidents that occur everyday against our government and the private sector, and they foreshadow potential threats to our critical infrastructure that need to be attended to now. Knowledgeable officials are concerned that these cases are part of a growing trend that consists of mostly hackers and criminals today, but possibly terrorists and foreign agents tomorrow. Thousands of other computer penetrations take place without the knowledge of system administrators in government, law enforcement, or industry. Joint government-industry solutions are required today to prepare for the level of cyber threats we will experience in five to ten years when computer literacy, the Internet, and electronic capability to intrude into various process control and information systems will be global. Between now and then US government and industry need to install defenses to prevent an electronic Pearl Harbor from occurring in the U.S.

When companies have cyber experts, their focus is on business continuity for their data processing contingencies, such as virus contamination problems. Many companies network their business, administrative and process operations systems, both internally and externally. Although many industry officials understand that connecting to the Internet can increase vulnerabilities, most companies still lack appropriate Internet controls.

The Range of Technical Risks Facing US Industry

Vulnerabilities and risks facing the energy industries include those resulting from:

- Rapid proliferation of industry-wide information systems based on open system architectures, centralized operations, increased communications over public telecommunications networks, and remote maintenance.

- Supervisory control and data acquisition systems that use commercial off-the-shelf hardware and software, connect to other company networks, and rely on dial-back modems that wrong doers can by-pass.

- Increased availability of vulnerability information, mandated often by regulators, to facilitate competition, and the tools to exploit those particular vulnerabilities.

- Rapid assimilation of advanced technologies with their inherent complexities.

- Consolidation of infrastructure corridors (e.g., communications, electric transmission lines, pipelines, etc.) leading to easier targeting.

- Previously identified physical vulnerabilities of critical assets that have not been adequately addressed throughout the industry.

Government Response to the Problem

To meet these challenges, on May 22, 1998 President Clinton signed two important new Decision Directives. The first, Presidential Decision Directive 62 creates a new and more systematic approach to fighting the unconventional threats of the next century and brings a program management perspective to U.S. counter-terrorism efforts. PDD 62 reinforces the mission of the many U.S. agencies charged with roles in defeating terrorism. It also codifies and clarifies government agency activities in the wide range of U.S. counter-terrorism programs, including protecting the computer-based systems that lie at the heart of America's economy. PDD 62 will help achieve the goal of ensuring that America can meet the threat of terrorism in the 21st century with the same vigilance that we have met past military threats in 20th century.

To achieve this new level of agency integration in the fight against terror, PDD-62 established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, and named Richard Clark, an experienced national security official, to take that post. Mr. Clark will oversee the broad variety of relevant polices and programs including such areas as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction. He will work within the National Security Council, report to the President through the Assistant to the President for National Security Affairs and produce an annual Security Preparedness Report for the President.

The second directive that President Clinton signed, the Critical Infrastructure Protection (PDD-63) calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. This directive requires immediate federal government action including risk assessment and planning to reduce exposure to cyber attack. It stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives.

Within the framework of these new PDDs, government and industry can work together to adopt uniform physical and cyber security guidelines, standards and industry best practices to enhance cyber protection. Hopefully, industry will be provided with the information that it needs to make informed risk management decisions and leverage their research and development activities by understanding the Government's cyber intrusion and energy reliability research and development (R&D) projects.

Summary

Our best hope for maintaining a strong and secure future for our nation against the threats to our vital systems is to achieve a national consensus to manage risks and protect critical national infrastructures. Such consensus can support a new relationship for how government and industry should work together to meet the challenges of the new Information Age. It appears that the White House now has a framework and the management team to begin addressing the problems identified by the Presidential Commission on Critical Infrastructure Protection.

***Edward V. Badolato**, is the Executive Director of the International Association of Counterterrorism and Security Professionals. He currently serves as the Chairman of the National Cargo Security Council, and as Chairman of the FAA's Air Cargo Security Working Group. He is a retired US Marine Colonel, and was a Deputy Assistant Secretary of Energy during the Reagan. and Bush Administrations.*