98-675 STM
August 13, 1998

Critical Infrastructures: A Primer

John Moteff
Specialist in Science and Technology
Science, Technology, and Medicine Division

Summary

The nation's health, wealth, and security rely on the supply and distribution of certain goods and services. The array of physical assets, processes and organizations across which these goods and services move are called critical infrastructures. Computers and communications, themselves critical infrastructures, are increasingly tying these infrastructures together. There is concern that this reliance on computers and computer networks makes the nation's critical infrastructures vulnerable to "cyber" attacks, be they from mischievous teenage hackers or information warriors from foreign countries. In May 1998, the President released Presidential Decision Directive No. 63. The Directive organizes the federal government to develop and implement plans that would protect government-operated infrastructures and calls for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect the nation's critical infrastructures by the year 2003.

Introduction

Certain socio-economic activities are vital to the day-to-day functioning and security of the country; for example, transportation of goods and people, communications, banking and finance, and the supply and distribution of electricity and water. Domestic security and our ability to monitor, deter, and respond to outside hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering and command and control of police and military forces. A serious disruption in these activities and capabilities could have a major impact on the country's well-being.[1]

[1] As a reminder of how dependent society is on its infrastructure, in May 1998, PanAmSat's Galaxy IV satellite's on-board controller malfunctioned, disrupting service to an estimated 80-90% of the nation's pagers, causing problems for hospitals trying to reach doctors on call, emergency workers, and people trying to use their credit cards at gas pumps, to name but a few.

These activities and capabilities are supported by an array of physical assets, processes, information, and organizations forming what is being called the nation's critical infrastructures. The country's critical infrastructures are growing increasingly complex, relying on computers and, now, computer networks to operate efficiently and reliably. The growing complexity and the interconnectedness resulting from networking means that a disruption in one may lead to disruptions in others.

Disruptions can be caused by any number of factors: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightening strikes, etc.) or physical destruction due to intentional human actions (theft, arson, sabotage, etc.). Over the years, operators of these infrastructures have taken measures to guard against and to quickly respond to many of these risks. However, the growing dependency of these systems on information technologies and computer networks introduces a new vector by which these problems can be introduced.

Of particular concern is the threat posed by "hackers" who can gain unauthorized access to a system and who could destroy, corrupt, steal, or monitor information vital to the operation of the system. Unlike arsonists or saboteurs, hackers can gain access from remote locations. The ability to detect and track their actions is still being developed. While infrastructure operators are also taking measures to guard against and respond to cyber attacks, there is concern that the number of "on-line" operations is growing faster than security awareness and sound security measures.

Hackers range from mischievous teenagers, to criminals, to spies, to military units. As the number of organizations and people that go "online" increases, the number of reported intrusions has also increased.[2] Whether this is the result of an increasing number of hackers is unknown, but there is concern that criminals, spies, and military personnel from around the world are perfecting their skills and pose a potential threat to the reliable operations of our critical infrastructures.[3]

The President's Commission on Critical Infrastructure Protection

The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996. Its tasks were to: report to the President the scope and nature of the vulnerabilities and threats to the nation's critical infrastructures (focusing primarily on cyber threats); recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations.

---

[2] It is unknown how many hackers are operating or how many intrusions occur. In its third annual survey, the Computer Security Institute (CSI) reported that an increasing percentage (64%) of the firms that responded reported that their systems have been hacked into. See Computer Security Institute, *Computer Security Issues and Trends*, Vol. IV. No. 1, Winter 1998.

[3] The Director of the Central Intelligence Agency testified before the Senate Committee on Governmental Affairs (June 24, 1998) that a number of countries are incorporating information warfare into their military doctrine and training and developing operational capability.

The PCCIP released its report to the President in October 1997.[4] While the Commission found no immediate crisis threatening the nation's infrastructures, it did find reason to take action. The rapid growth of a computer-literate population (implying a greater pool of potential hackers), the inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker "tools" (available on many websites), and the fact that the basic tools of the hacker (computer, modem, telephone line) are the same essential technologies used by the general population indicated to the Commission that the threat and vulnerability exist.

The Commission's general recommendation was that greater cooperation and communication between the private sector and government was needed. Much of the nation's critical infrastructure lies in private hands. As seen by the Commission, the government's primary role (aside from protecting its own infrastructures) is to collect and disseminate the latest information on intrusion techniques, threat analysis, and ways to defend against hackers.

The Commission also proposed a strategy for action:

- facilitate greater cooperation and communication between the private sector and appropriate government agencies by: setting a top level policy-making office in the White House; establishing a council that includes corporate executives, state and local government officials, and cabinet secretaries; and setting up information clearinghouses.
- develop a real-time capability of attack warning.
- establish and promote a comprehensive awareness and education program.
- streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers in pursuing hackers electronically).
- expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.

The Commission's report underwent interagency review to determine how to respond. That review led to a Presidential Decision Directive released in May 1998.

Presidential Decision Directive No. 63

Presidential Decision Directive No. 63 (PDD-63)[5] sets as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

PDD-63 identified the following activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation,

---

[4] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

[5] See, *The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998, which can be found on [http://www.ciao.gov/resources.html].

highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production, and storage. In addition, the PDD identified four activities where the federal government controls the critical infrastructure: internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense.

A lead agency was assigned to each of these "sectors" (e.g. the Environmental Protection Agency was assigned the water supply). Each lead agency is to appoint a **Sector Liaison Official** to interact with appropriate private sector organizations. The private sector is encouraged to select a **Sector Coordinator** to work with the agency's sector liaison official. Together, the liaison official, sector coordinator, and all affected parties will contribute to a sectoral security plan which will be integrated into a **National Infrastructure Assurance Plan** (see below). Each of the activities performed primarily by the federal government also are assigned a lead agency who will appoint a **Functional Coordinator** who will coordinate efforts similar to those made by the Sector Liaisons.

The PDD creates the position of **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism, who reports to the President through the Assistant to the President for National Security Affairs.[6] Among his many duties the National Coordinator will chair the **Critical Infrastructure Coordination Group**. This Group will be the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group includes high level representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

Each federal agency is responsible for securing its own critical infrastructure and shall designate a Critical Infrastructure Assurance Officer (CIAO) to assume that responsibility. The agency's current Chief Information Officer (CIO) may double in that capacity. In those cases where the CIO and the CIAO are different, the CIO is responsible for assuring the agency's information assets (databases, software, computers), the CIAO is responsible for any other assets that make up agency's critical infrastructure. The agencies were given 180 days from the signing of the Directive to develop their plans. Those plans are to be fully implemented within 2 years and updated every 2 years.

The PDD sets up a **National Infrastructure Assurance Council**. The Council will be a panel that includes private operators of infrastructure assets, representatives of state and local governments, and relevant federal agency representatives. The Council will meet periodically and provide reports to the President as appropriate. The National Coordinator will act as the Executive Director of the Council.

The PDD also calls for a **National Infrastructure Assurance Plan**. The Plan is to integrate the plans from each of the sectors mentioned above and should consider the following: vulnerability assessment, including the minimum essential capability required to meet its purpose; remedial plans to reduce its vulnerability; warning requirements and procedures; response strategies; reconstitution of services; education and awareness

---

[6] The President designated Richard Clarke, Special Assistant to the President for Global Affairs, National Security Council, as National Coordinator.

programs; research and development needs; intelligence strategies; needs and opportunities for international cooperation; and legislative and budgetary requirements.

The PDD also sets up a National Plan Coordination Staff to support the plan's development. This function will be performed by the **Critical Infrastructure Assurance Office** (CIAO, not to be confused with the agencies' Critical Infrastructure Assurance Officers) and has been placed in the Department of Commerce. CIAO will support the National Coordinator's efforts to integrate the sectoral plans into a National Plan, will support individual agencies in developing their internal plans, and will provide legislative and public affairs support.

Most of the Directive establishes policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addresses operational concerns. The Federal Bureau of Investigation was given the authority to expand its existing computer crime capabilities into a **National Infrastructure Protection Center (NIPC)**. The NIPC is to be the focal point for federal threat assessment, vulnerability analysis and expertise, warning capability, law enforcement investigations, and response coordination. While the FBI is given the lead, the NIPC will also include the Department of Defense, the Intelligence Community, and a representative from all lead agencies. Depending on the level of threat or the character of the intrusion, the NIPC may be placed in direct support of either the Department of Defense or the Intelligence Community. The NIPC will utilize warning and response expertise located throughout the federal government. The private sector is encouraged to establish its own Information Sharing and Analysis Center to interact directly with the NIPC.

Issues

Bureaucratic. The PDD sought to use existing authorities and expertise as much as possible in assigning responsibilities. However, the structuring does raise some bureaucratic questions. To the extent that the major concern here is the impact cyber attacks may have on the nation's critical infrastructure, this effort in many respects expands the government's current efforts in computer security. One question is to what extent does it duplicate, supersede, or incorporate on-going computer security efforts. For example, the Office of Management and Budget has had the primary responsibility of coordinating and reviewing all federal agencies' computer security plans generated by each agency's CIO. Does the NICG supersede OMB and its CIO Coordinating Committee? The National Institute of Standards and Technology has the responsibility for setting computer security technology standards for all federal unclassified computer systems and for operating a clearinghouse for information on computer security threats, procedures, responses, etc. The National Security Agency (NSA) does the same for the government's classified systems. The NSA also performs security assessments on government systems. These functions will presumably feed into the NIPC, directed by the FBI. What authority or influence will the FBI have over these activities? The FBI will now lead the organization that is responsible for warning, responding to, and investigating intrusions. Are these functions compatible?

Another bureaucratic issue has been raised by some Members who have questioned the decision to place CIAO within the Department of Commerce. To them, a threat to the nation's critical infrastructures is a national security risk and should be the responsibility of the Department of Defense. The Department of Defense did serve as the

executive agent for the PCCIP's Transition Office which is to be the model for National Plan Coordinating Staff function. On the other hand, the Department of Commerce has on-going relationships with many of the private infrastructure operators.

Public - Private Partnerships. How successful will this effort be in generating the communication and cooperation needed between the government and the private sector? The PDD offers guidance that any recommended action should result in little or no new regulations or oversight bodies. All parties are expected to be involved in the planning process. The PDD also states that individual liberties and rights to privacy are to be preserved. Still, the nature of cyber threats (e.g. hundreds of intrusions a year) has the potential to make the federal government involved in monitoring the day-to-day operations of private infrastructures. And, if an "attack" should disrupt operations, what authority will the federal government try to exercise over the response? Another question is how open the private sector and the government will be in sharing information? The private sector primarily wants from the government information on potential threats which the government may want to protect in order not to compromise sources or investigations. The government wants information on intrusions which companies may want to protect to prevent adverse publicity.

Costs. Many of the actions called for in the PDD will be part of on-going administrative duties. However, there is a call for developing and implementing education and awareness programs. There is also a call for developing research and development requirements (the PCCIP called for increasing R&D from an estimated $250 million to $1 billion over the next 5 years). As plans are developed costs may increase. In testimony before the Senate Judiciary's Subcommittee on Technology, Terrorism, and Government Information (June 10, 1998), the National Coordinator said that requests should begin to appear in the President's FY2000 Budget. Can and will these budgets be broken out to allow for easy oversight of the effort being made?

Other Possible Congressional Action. Aside from oversight and appropriating funds, Congress may need to consider legislation. The Administration is still reviewing what legislation requirements may be needed. The PCCIP report, however, gives a glimpse of the types of legislative actions that might be requested to support infrastructure protection plans. For example, possible modification of the Defense Production Act to provide the federal government with the authority to direct private resources to help reconstitute critical infrastructures suffering from a cyber attack such as exists now with the supply and distribution of energy and critical materials in an emergency. Other potential areas include: the ability to issue a single warrant that would allow investigators to track and identify intruders across numerous jurisdictions; federal licensing of private computer investigators to require them to report to the federal government information on intruders; waivers to Employee Polygraph Protection Act to allow firms to investigate and monitor information security personnel, similar to waivers granted now to certain security personnel; and clarifying the potential liabilities of contractors hired to hack into a client's computer system to test its security.