Order Code RL31534

CRS Report for Congress
Received through the CRS Web

Critical Infrastructure: Control Systems and the Terrorist Threat

Updated January 20, 2004

Dana A. Shea
Analyst in Science and Technology Policy
Resources, Science, and Industry Division

Critical Infrastructure: Control Systems and the Terrorist Threat

Summary

Much of the U.S. critical infrastructure is potentially vulnerable to cyber-attack. Industrial control computer systems involved in this infrastructure are specific points of vulnerability, as cyber-security for these systems has not been previously perceived as a high priority. Industry sectors potentially affected by a cyber-attack on process control systems include the electrical, telephone, water, chemical, and energy sectors.

The federal government has issued warnings regarding increases in terrorist interest in the cyber-security of industrial control systems, citing international terrorist organization interest in critical infrastructure and increases in cyber-attacks on critical infrastructure computer systems. The potential consequences of a successful cyber-attack on critical infrastructure industrial control systems range from a temporary loss of service to catastrophic infrastructure failure affecting multiple states for an extended duration.

The National Strategy for Securing Cyberspace, released in February 2003, contains a number of suggestions regarding security measures for control systems. A focus on the further integration of public/private partnerships and information sharing is described, along with suggestions that standards for securing control systems be developed and implemented.

The Homeland Security Act of 2002 (P.L. 107-296) transferred and integrated several federal entities that play a role in cyber-security of control systems into the Department of Homeland Security. These entities include the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the National Infrastructure Simulation and Analysis Center, and parts of the Department of Energy's Office of Energy Assurance. Additionally, the Homeland Security Act of 2002 created a new class of information, critical infrastructure information, which can be withheld from the public by the federal government.

Efforts in increasing the cyber-security of control systems occur both at federal government facilities and, in critical infrastructure sectors, through industry groups. The Department of Energy National Laboratories, the Department of Defense, and the National Institute of Standards and Technology all have programs to assess and ameliorate the cyber-vulnerabilities of control systems. Industry-based research into standards, best practices, and control system encryption is ongoing in the natural gas and electricity sector.

Possible policy options for congressional consideration include further development of uniform standards for infrastructure cyber-protection; growth in research into security methods for industrial control systems; assessing the effectiveness of the new exemptions to the Freedom of Information Act; and the integration of previous offices in the new Department of Homeland Security.

This report will be updated as events warrant.

Contents

Critical Infrastructure: Control Systems and the Terrorist Threat

Introduction

This report addresses the cyber-vulnerability of critical infrastructure industries which regularly use industrial control systems. Industrial control systems may be vulnerable to infiltration by different routes, including wireless transmission, direct access to control system computers, exploitation of dial-up modems used for maintenance, or through the Internet. This report will specifically discuss the potential for access to industrial control systems through the Internet.

The vulnerability of U.S. critical infrastructure to cyber-attack and catastrophic failure was brought to light in 1997 in the report of the President's Commission on Critical Infrastructure Protection.[1] Among other concerns, the computer systems used to remotely control process equipment were highlighted as specific points of vulnerability. These systems were updated during the Y2K crisis, but their cyber-security generally has not been a high priority. The events of September 11, 2001 have heightened the public awareness of the nation's vulnerability to terrorist attack, and a National Research Council report has identified "the potential for attack on control systems" as requiring "urgent attention."[2]

Critical infrastructure is defined in the USA PATRIOT Act as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3] Several industry sectors considered to be critical infrastructures use industrial control systems in their daily activities. These industries could be significantly affected by a cyber-attack targeting industrial control systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems, and others. The President's Commission on Critical Infrastructure Protection report stated,

> From the cyber perspective, SCADA systems offer some of the most attractive targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. With the exponential growth of information system networks that interconnect the business, administrative, and operational systems, significant

---

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

[2] National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, June, 2002.

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, Title X, Section 1016.

disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers.[4]

Current Industrial Control System Vulnerability

The most commonly discussed industrial control systems include supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS).[5] SCADA systems are often used for remote monitoring over a large geographic area and to transmit commands to remote assets, such as valves and switches. For example, they can be found in water utilities and oil pipelines, where they monitor flow rates and pressures. Based on the data that these systems provide, computer programs or operators at a central control center balance the flow of material. Generally, SCADA systems process little data internally, instead performing analysis in a more central location, but are the primary conduits for raw data to and commands from a control center. They may be vulnerable to implantation of faulty data and to remote access through dial-up modems used for maintenance.

Distributed control systems are process control systems, commonly deployed in a single manufacturing or production complex, characterized by a network of computers. DCS generally provide processed information to, or a series of commands from, a central location. For example, at a chemical plant, a DCS might simultaneously monitor the temperature of a series of reactors and control the rate at which reactants are mixed together, while performing real time process optimization and reporting the progress of the reaction. An attack targeting a DCS might cause extensive damage at a single facility, but might not affect more than the single site.

These process control systems can be interconnected within a single industry as well. This might be the case in an infrastructure which both transports and processes material. As an example, the oil and gas infrastructures contain both processing and refining sites, as well as holding facilities and distribution systems. Refining and processing sites may utilize DCS in discrete locations. The distribution and holding facilities might be managed by a SCADA system which collected data from and issued commands to different geographic sites from a single location.[6]

---

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

[5] For a simple overview of control system types, see Micrologic Systems, "SCADA Primer," found online at [http://www.micrologic-systems.com/primers/scada.htm], or Dan Capano, "Distributed Control Systems Primer," *Waterandwastewater.com*, (2002), found online at [http://www.waterandwastewater.com/www_services/ask_dan_archive/toc.htm]. Other types of control systems, such as programmable logic controllers, exist, but are not explicitly discussed here.

[6] This example was taken from "IT Security for Industrial Control Systems" by Joe Falco, Keith Stouffer, Albert Wavering, and Frederick Proctor, Intelligent Systems Division, National Institute of Standards and Technology, available online at [http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf].

Industrial control system technologies are often employed in critical infrastructure industries to allow a single control center to manage multiple sites. Industrial control systems were originally implemented as isolated, separate networks.[7] They were viewed as secure systems which protected remote locations from being physically broken into and mistreated. For example, the establishment of remote control systems in dams reportedly protected against unlawful release of the dammed water, as no hand-operable valves and switches were accessible.[8]

The networking of industrial control systems on a greater scale has led to increased synergy and efficiency, and, due to market needs (e.g. deregulated markets), real time information from these systems is increasingly important for commercial purposes. Consequently, industrial control systems are becoming linked to corporate computer systems, potentially making them vulnerable to cyber-attack through the Internet. Original control systems were designed to be free standing networks without Internet access. Therefore, it has been necessary to add network access capabilities to these legacy systems to integrate them into the corporate structure. This has created, in the worst cases, a labyrinth of connections which is perhaps not rigorously constructed for cyber-security or well documented.

Many organizations, including the General Accounting Office, researchers at several Department of Energy National Laboratories, and private security and consulting companies, have identified systemic and specific security vulnerabilities in select process control systems.[9] Among these vulnerabilities are poor cyber-security practices, such as weak passwords, a lack of robust protocols, and communication in clear text. While some vulnerabilities arise from the manner by which the process control system is operated, others are believed to be integral to the control system configuration itself.

Some industrial control systems, including legacy systems, are proprietary, and contain non-standard architectures and command syntax. This can be considered both an advantage and a disadvantage. Proprietary systems with esoteric command structures are often non-intuitive, and could be difficult to operate by an untrained individual. Incorrect commands could cause no results, and may increase the probability that the intruder would be noticed and removed from the system. Additionally, different companies may have different command sets, even if they are both members of the same industry, as their proprietary systems may have significantly different structures. Thus, if a hacker or terrorist successfully attacks one company, that experience may not be valuable for use at the next company.

---

[7] Separation of control system networks from other computer networks still occurs in some businesses. For an example, see Alex Salkever, "If These Networks Get Hacked, Beware," *Business Week Online*, September 17, 2003.

[8] Scott Berinato, "The Truth about Cyberterrorism,"*CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

[9] See Statement of Robert F. Dacey, Director, Information Security Issues Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, "Critical Infrastructure Protection: Challenges in Securing Control Systems," GAO-04-140T; and Alan S. Brown, "SCADA vs. the Hackers," *Mechanical Engineering*, December, 2002.

Others assert that many new control systems, as well as upgrades to legacy systems, are being assembled from commercial, off-the-shelf equipment and software, providing commonalities across different industry sectors. They point to the needs of system maintenance and new component integration as leading to similar control system architectures both within and between critical infrastructure sectors. By adopting such equipment and software, vulnerabilities that are identified impact all sectors.

The degree of integration between control system networks and publicly accessible networks is difficult to judge from the open literature. This makes assessment of the vulnerability of critical infrastructure industries from Internet based attack difficult to know with certainty.[10] Faced with an unclear risk, it may be difficult, from an industry perspective, to justify the additional costs of upgrading privately-held industrial control systems to higher security standards.[11] Current off-the-shelf industrial control systems have been designed for operational speed and functionality, rather than for secure operation, and therefore may not have a high degree of operational security.[12] Addition of security requirements may degrade the performance of these components below operating standards.

Events have shown that utility control system networks may be vulnerable to cyber-based incidents. Computers at an inactive nuclear power plant in Ohio were infected by the Slammer worm in January 2003. The infection disabled some computer functionality, including monitoring systems for portions of the power plant.[13] Also, it has been reported that other control system computers have been compromised by other viruses.[14]

Given the uncertain vulnerability level and the potential systemic weaknesses involved in current off-the-shelf technology, there appears to be little market incentive to directly increase industrial control systems security. Therefore the security systems for the corporate network, which block initial intrusion through the Internet, may be the sole planned protection for the industrial control systems. Such

---

[10] The Department of Energy and the Department of Defense have performed vulnerability assessments, through "red team" exercises, of some individual stakeholders in critical infrastructure industries. (Barton Gellman, "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post*, June 27, 2002) These detailed results, while provided to the individual stakeholders, are not widely available. (Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002)

[11] Eric Pianin and Bill Miller, "Businesses Draw Line On Security, Firms Resist New Rules For Warding Off Terror," *Washington Post*, September 5, 2002.

[12] Jennifer Alvey, "Digital Terrorism: Holes in the Firewall? Plugging Cyber Security Holes Isn't as Easy as Everyone Wants to Think," *Public Utilities Fortnightly*, March 15, 2002.

[13] It should be noted that the systems infected were monitoring systems, not computers which control plant operations. Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Net," *The Register*, August 20, 2003.

[14] Dan Verton, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, September 1, 2003.

an approach has been criticized, as while it may provide initial barriers to intrusion, it would not reduce any inherent vulnerabilities in the control system network.[15]

Security analysts also contend that industrial control systems are less obscure now than when they were initially developed. Foreign utility companies increasingly use current commercial off-the-shelf industrial control systems, increasing the international availability of systems and their documentation. Due to the similarity between these systems and systems installed domestically, potential terrorists need not break into an American utility to test their plans.[16] Instead, preliminary testing might be performed outside of the United States on equipment held in other countries.

Some security analysts believe that the industrial control system vulnerability should be addressed before potentially catastrophic events occur, and that techniques for reducing the vulnerability are already known. They contend that the majority of attacks on industrial control systems will come through corporate networks, via the Internet. While standardized information technology protection methods have not yet been developed specifically for industrial control systems, these analysts contend that if general network benchmark standards were uniformly applied across corporate networks, corporate networks vulnerability to intrusion could be reduced by 80-88%.[17] This would indirectly reduce the industrial control systems vulnerability to intrusion, as routes through the corporate network would no longer be available. These benchmark standards include disabling unneeded server functionality, patching known security flaws, and updating programs to the most recent version.

Other security analysts claim that in addition to general network security, specific protection for industrial control systems must also be established. Such protection might be addressed by successfully isolating the control system network from the corporate computer network or by implementing stronger security measures at known junctions of the two networks. Such an effort might significantly increase the difficulty of infiltrating the control system network from the Internet.[18]

In contrast, control systems may have vulnerabilities unrelated to those associated with corporate networks, and may require more specific protection,

---

[15] British Columbia Institute of Technology, "BCIT Cyber Security Expert Warns U.s. Congressional Subcommittee of Critical Infrastructure Vulnerabilities," News Release, October 10, 2003.

[16] Testimony by Timothy G. Belcher, Chief Technology Officer, Riptech, Inc., before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[17] Testimony by Alan Paller, Director of Research, The SANS Institute, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[18] Such methods have been reportedly employed by DuPont Chemical Company. Mathew Schwartz, "Wanted: Security Tag Team," *Computerworld*, June 30, 2003.

including against attacks not transiting the corporate network.[19] Protecting corporate networks from intrusion may not address enough of the vulnerable access routes into industrial control systems. Joe Weiss, Executive Consultant with KEMA Consulting, asserts that firewalls, intrusion detection, encryption, and other technology need to be developed specifically for control systems.[20]

Some companies have taken aggressive steps to protect their industrial control systems, and are possible examples for how secure industrial control systems can be established.[21] While most security experts agree that critical infrastructure industries which view secure industrial control systems as a priority can reduce vulnerabilities, some assert that most critical infrastructure industries are not willing to voluntarily commit resources, time and effort into reducing these vulnerabilities. Stuart McClure, President and Chief Technical Officer of the security company Foundstone, claims, "[Industries] have fallen into the regulation trap. Unless the government regulates it, they're not yet taking [security] seriously."[22]

The Magnitude of the Terrorist Threat

Some critical infrastructure industry representatives are skeptical that a cyber-terror attack would target industrial control systems.[23] Since there are no reported terrorist cyber-attacks on domestic critical infrastructure industrial control systems which have caused significant, publicly reported damage, even in cases where hackers have successfully broken into these systems, industry representatives believe the cyber-threat to be low. Diane Van de Hei, executive director of the Association of Metropolitan Water Agencies and contact person for the water utility Information Sharing and Analysis Center (ISAC), was quoted as saying, "If we had so many dollars to spend on a water system, most of it would go to physical security."[24]

Analysts have also doubted that terrorist groups will use cyber-attacks to affect critical infrastructure. They point to the lack of documented terrorism-related cyber-attacks on critical infrastructure as indicative of low threat probability. "It suggests

---

[19] Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002.

[20] Testimony by Joe Weiss, Consultant, KEMA Consulting, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, July 24, 2002.

[21] For example, see Alex Salkever, "If These Networks Get Hacked, Beware," *Business Week Online*, September 17, 2003 and Scott Berinato, "The Truth about Cyberterrorism,"*CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

[22] Robert Vamosi, "Cyberterrorists Don't Care About Your PC," *ZDNet Reviews*, July 10, 2002.

[23] Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers," *San Francisco Chronicle*, June 30, 2002.

[24] Robert Lemos, "What Are the Real Risks of Cyberterrorism?" *ZDNet*, August 26, 2002.

that, as so many commentators have noted, that cyberterror or cyberattacks on infrastructure are an unlikely threat to the security of the United States."[25]

Some critical infrastructure companies believe that the potential damage likely to be caused by a cyber-attack on control systems would be small and manageable through already existing procedures. Since fluctuations and equipment failure are part of expected, normal business, plans and procedures for these naturally occurring events are in place. They assert that the damage caused by cyber-attack would be similar to that already routinely seen.[26]

Some industry representatives emphasize that the unfamiliar and uncommon commands used in legacy industrial control systems will continue to provide as high a barrier to future destructive attempts as it has in the past.[27] While utility industry leaders agree that they have been the target of millions of cyber-security incidents, some do not analyze the origin or method of attack. Will Evans, vice president of IT services at People's Energy Corp., reportedly claimed, "[A large utility] could have a million [intrusion] events that need to be analyzed. I don't think anybody has the capability to do that in-house."

Utility industry representatives contend that the vast majority of computer intrusion events are searches for vulnerable computers in the corporate network by inexperienced hackers, and, of the dangerous minority actually performed by experienced crackers, many are focused on economic aspects of the corporate network rather than the industrial control systems network.[28] From the perspective of critical infrastructure industries, discontented employees who possess inside information about industrial control systems are a greater security risk than external attempts to breach security.

There is evidence that al Qaeda is interested in the vulnerabilities of the U.S. public and private utilities. The discovery in Afghanistan of a computer containing structural analysis programs for dams, combined with an increase in Web traffic relating to SCADA systems,[29] prompted the National Infrastructure Protection Center (NIPC) to issue a warning information bulletin.[30] An analysis of cyber-attack data collected during the second half of 2001 showed that the corporate systems of energy industry companies are attacked twice as often as other industries, and that a large

---

[25] Jim Lewis, *CyberAttacks: Missing in Action*, Center for Strategic and International Studies, April 2003.

[26] Kevin Poulsen, "Sparks Over Power Grid Cybersecurity," *Business Week Online*, April 16, 2003.

[27] Scott Berinato, "Debunking the Threat to Water Utilities," *CIO Magazine*, Vol. 15, No. 11, March 15, 2002.

[28] Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers," *San Francisco Chronicle*, June 30, 2002.

[29] Sean Webby, "4 Cities Take Data Off Web; Authorities Remove Info After Hits From Mideast," *San Jose Mercury News*, June 28, 2002.

[30] "Terrorist Interest in Water Supply and SCADA Systems," National Infrastructure Protection Center, Information Bulletin 02-001, January 30, 2002.

number of these attacks originate from the Middle East.[31] Additionally, according to one expert, these statistics do not reflect intrusions directed at control systems which lack firewalls or intrusion detection systems, resulting in an under-reporting of the actual number of attacks.[32]

There have been examples of individuals specifically breaking into utility companies' control systems. The most notable event occurred in Maroochy Shire, Australia, where, in Spring, 2000, a discontented former employee was able to remotely access the controls of a sewage plant and discharge approximately 264,000 gallons of untreated sewage into the local environment.[33] In 1994, a hacker successfully broke into the computer system of the Salt River Project in Arizona and was able to gain access to computers monitoring canals.[34] Another example, from March, 1997, occurred when a teenager in Worcester, MA was able to remotely disable part of the public telephone switching network, disrupting telephone service for 600 residents, including the fire department, and causing a malfunction at the local regional airport.[35] Reportedly, an intrusion into the SCADA systems of a global chemical company occurred where a former employee attempted to disable chemical operating systems at a production plant.[36]

Often, it is difficult to assess from public reports to what degree a critical infrastructure industry has been breached.[37] For example, a cyber-break-in at the California Independent System Operator (Cal-ISO), California's primary electric power grid operator, went undetected for 17 days in April, 2001. Greg Fishman, a representative of Cal-ISO, reported the intruders "never really got close at all to our operational systems that run the grid."[38] It is not clear what information was compromised during the intrusion, who the perpetrators were, or what their goal in gaining access was. To date, there has been no indication that the perpetrators of this attack were able to access any sensitive information or systems.

---

[31] Dan Verton, "Vulnerability Assessment Triggers Alarms," *Computerworld*, January 21, 2002.

[32] Joe Weiss, KEMA Consulting, private e-mail communication, September 8, 2002.

[33] A summary of this event can be found in National Infrastructure Protection Center, *Highlights*, 2-03, June 15, 2002.

[34] Robert Lemos, "What are the Real Risks of Cyberterrorism?" *ZDNet*, August 26, 2002.

[35] "Juvenile Hacker Charged with Disabling Airport Control Tower Telephones," *Agence France Press*, March 18, 1998.

[36] Esther D'Amico, "Cybersecurity Gains Momentum," *Chemical Week*, August 21, 2002.

[37] *Ibid.*

[38] Dan Verton, "California Hack Points to Possible Surveillance Threat; Power Grid Unaffected; Perps Unidentified," *Computerworld*, June 18, 2001.

Potential Consequences of a Terrorist Attack

The consequences of an attack on the industrial control systems of critical infrastructure could vary widely. It is commonly assumed that a successful cyber-attack would cause few, if any, casualties, but might result in loss of infrastructure service while control was wrested from the attacker and damage repaired. For example, a successful cyber-attack on the public telephone switching network might deprive customers of telephone service while technicians reset and repaired the switching network. An attack on a chemical or liquid natural gas facility's control systems might lead to more widespread physical damage.

Lower probability events include catastrophic infrastructure failure, where the failure of one part of the infrastructure leads to the failure of other parts, causing widespread effect. Such failure might occur due to the synergistic effect of infrastructure industries on each other. A simple example might be an attack on electrical utilities where electricity distribution was disrupted; sewage treatment plants and waterworks could also fail, as perhaps the turbines and other electrical apparatuses in these facilities shut down. On August 5, 2002, the faulty closure of an emergency valve at one of Singapore's two natural gas suppliers blocked the flow of natural gas to seven electrical power plants. As an immediate result, power levels dropped 30%, and even after reserve power was employed, there was still a 8% shortfall. The power outage lasted up to 90 minutes.[39] Several chemical production plants were forced to shutdown their facilities during the power outage, and required several days to restore full production.[40]

Some experts warn of a cascade event, where a terrorist is able to manipulate control systems and cause catastrophic failure within an infrastructure. Cascade events can be very damaging, causing widespread utility outages. Twice in 1996, arcing between high voltage transmission lines and trees resulted in widespread power outages. On July 2, 1996, a cascade event left 2 million customers in 11 states and 2 Canadian provinces without power.[41] Most service was restored within 30 minutes.[42] On August 10, 1996, a similar event caused 7.5 million customers in seven western states and part of Canada to be without power for up to nine hours.[43]

---

[39] Krist Boo and Tan May Ping, "90-Minute Blackout in Several Areas," *The Straits Times (Singapore)*, August 6, 2002, and Krist Boo, "Computer Glitch Behind Worst Blackout in Decade," *The Straits Times (Singapore)*, August 15, 2002.

[40] Sam Cage, "Power Failure Downs Three Singapore Crackers," *Chemical Week*, August 14, 2002.

[41] Susan Reed, "Massive Power Outage in West Still Unexplained," *CNN*, July 3, 1996 and Bonneville Power Administration, "Tree Triggers Power Outage," *Journal*, August, 1996, found online at [http://www.bpa.gov/corporate/kc/home/journal/96jl/jl0896x.shtml].

[42] "Parts of Idaho Darkened by Power Outage, Earlier Western Blackout Traced to Short Circuit," *CNN*, July 3, 1996.

[43] John F. Hauer and Jeff E. Dagle, "Consortium for Electric Reliability Technology Solutions Grid of the Future, White Paper on Review of Recent Reliability Issues and System Events," prepared for Transmission Reliability Program, Office of Power

(continued...)

The August 2003 blackout of the northeastern United States and parts of Canada, also a cascade event, has been invoked as indicative of the potential effects a successful terrorist cyber-attack on electrical utility control systems.[44] While it was quickly determined that the power outage was not caused by terrorism,[45] there were questions whether control system failure, computer viruses or worms, or operator-error played roles in the outage.[46] It has been suggested by some that the Blaster worm, which had been contributing to congestion of the Internet, might have exacerbated the problems faced by utilities leading up to the blackout event.[47]

The scenario which causes the highest degree of concern among experts is the combined use of a cyber-attack on critical infrastructure in conjunction with a physical attack.[48] This use of cyber-terrorism could result in an amplification of the physical attack's effects. An example of this might be a conventional bombing attack on a building combined with a temporary denial of electrical or telephone service. The resulting degradation of emergency response, until back-up electrical or communication systems can be brought into place and used, could increase the number of casualties and public panic.

Others believe that the consequences of a cyber-attack on critical infrastructure would be very limited, and that excessive focus has been given to an unsubstantiated terrorist threat.[49] Cyber-security experts who doubt the effectiveness of such an attack range in opinion regarding an attack's impact. Some believe that a cyber-attack on critical infrastructure control systems, while having some effect, would not

---

[43] (...continued)
Technologies, Assistant Secretary for Energy Efficiency and Renewable Energy, U.S. Department of Energy, August 30, 1999.

[44] Kevin Maney and Michelle Kessler, "Blackout Prompts Worries About Security of Power Grid," *USA Today*, August 18, 2003; Johanna McGeary, "An Invitation to Terrorists?" *Time*, August 16, 2003; Knut Royce, "Tempting Targets for Terrorists," *Newsday*, August 17, 2003; and Rick White and Stratton Sclavos, "Targeting Our Computers," *Washington Post*, August 15, 2003, p. A27.

[45] Philip Shenon, "Agency Quickly Concludes No Terrorist Were Involved," *New York Times*, August 15, 2003.

[46] "Power Outage Not Internet Worm-Related," *Reuters*, August 14, 2003; Dan Verton, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, September 1, 2003; Dan Verton, "IT Security in Energy Sector Under Scrutiny," *Computerworld*, August 21, 2003; and Dan Verton, "IT Links to Blackout Under Scrutiny", *Computerworld*, September 5, 2003; and

[47] Jim Krane, "Computer-heavy Electrical Grid Vulnerable to Hackers, Viruses," *Associated Press*, September 12, 2003.

[48] For an overview of this type of scenario, see National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, Washington, DC, 2002.

[49] See, for example, Joshua Green, "The Myth of Cyberterrorism," *The Washington Monthly*, November, 2002; and Joris Evers, "CeBIT: Terrorists Won't Hit the Internet, Panelists Agree," *Computerworld*, March 14, 2003.

be devastating, but rather only have minor impact.[50] For example, security managers in some electric utilities reportedly believe that experience in dealing with natural disasters and power outages may translate well to recovering quickly from a cyber-attack.[51] Other believe that there could be significant impacts from a successful attack on control systems, but that such success would be very unlikely.[52] Finally, some believe that while it is possible to use computers to generate high consequence attacks, it would be much more likely that a terrorist group would resort to a simpler conventional attack which would yield results of a similar magnitude.[53]

Current Initiatives

Department of Homeland Security

The creation of the Department of Homeland Security has centralized within the Directorate of Information Analysis and Infrastructure Protection a number of offices related to critical infrastructure control system security: the Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Protection Center, the National Infrastructure Simulation and Analysis Center (NISAC), and part of the Department of Energy's Office of Energy Assurance.[54]

CIAO and NIPC were created in response to Presidential Decision Directive No. 63, issued in 1998.[55] CIAO coordinated the federal government's initiatives on critical infrastructure assurance and promotes national outreach and awareness campaigns about critical infrastructure protection. NIPC was a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response agency. Among other programs, NIPC developed the InfraGard program, which serves as a clearinghouse for information sharing and analysis for members of critical infrastructure industries.

NISAC was created in 2001 through the passage of the USA PATRIOT Act. It is charged to "serve as a source of national competence to address critical

---

[50] Steve Alexander, "Some Experts Say Cyberterrorism Is Very Unlikely," *Star Tribune*, February 13, 2003.

[51] Michael A. Gips, "They Secure the Body Electric," *Security Management*, November 1, 2002.

[52] Mark Harrington, "In Cyber-Attack, The System Bends, Doesn't Break," *Newsday*, February 11, 2003

[53] Bill Wallace, "Security Analysts Dismiss Fears of Terrorist Hackers," *San Francisco Chronicle*, June 30, 2002; Jennifer Alvey, "Cyber Security: A 'Virtual' Reality," *Public Utilities Fortnightly*, September 15, 2003; and Bruce Schneier, "Embedded Control Systems and Security," *Crypto-Gram Newsletter*, July 15, 2002.

[54] Homeland Security Act of 2002, P.L. 107-296.

[55] Presidential Decision Directive No. 63 set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks. For more information regarding this directive and other critical infrastructure policy, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation* by John D. Moteff.

infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation."[56] This center is to provide modeling and simulation capabilities for the analysis of critical infrastructures, including electricity, oil, and gas sectors.[57] It is located at Sandia National Laboratories and Los Alamos National Laboratory.[58]

The Department of Homeland Security created a National Cyber Security Division, located in the Information Analysis and Infrastructure Protection Directorate, to identify, analyze, and reduce cyber-threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning.[59] This division has the responsibility for implementing programs for research and development in cyber-security, using expertise from the Science and Technology Directorate to provide research and development functions and execution.

The President's Critical Infrastructure Protection Board has released *The National Strategy to Secure Cyberspace*, in which a general strategic overview, specific recommendations and policies, and the rationale for these actions are presented.[60] This document addresses concerns regarding digital control systems and SCADA networks, rates SCADA network security as a national priority, and recommends joint public/private efforts in discovering solutions to potential vulnerabilities. This strategy identifies the Department of Homeland Security, in coordination with other federal agencies, as the department responsible for developing best practices and new technologies to increase SCADA security. Some cyber-security experts have criticized this plan, claiming that vulnerabilities will remain because of its lack of enforcement regulations.[61]

Department of Energy

The Department of Energy's Office of Energy Assurance has also been involved in developing techniques to secure energy production and availability.[62] Part of this effort has been the development of "simple, common-sense approaches to improve

---

[56] USA PATRIOT Act, P.L. 107-56, Section 1016.

[57] Jennifer Jones, "Models of Mayhem," *Federal Computer Week*, September 30, 2002.

[58] For more information on NISAC, see [http://www.sandia.gov/CIS/NISAC.htm].

[59] Office of the Press Secretary, Department of Homeland Security, "Ridge Creates New Division to Combat Cyber Threats," June 6, 2003.

[60] *The National Strategy to Secure Cyberspace* is available for download at the President's Critical Infrastructure Protection Board website, found online at [http://www.whitehouse.gov/pcipb/].

[61] Robert Lemos, "Bush Unveils Final Cybersecurity Plan," *CNET News*, February 14, 2003.

[62] The Department of Energy's Office of Energy Assurance can be found online at [http://www.ea.doe.gov/].

the overall level of protection in SCADA and digital control networks."[63] A document describing a general approach to improving cyber-security in SCADA systems has been released.[64]

Department of Energy National Laboratories. The Department of Energy National Laboratories have developed a series of test bed facilities to test security measures developed for critical infrastructure. The Idaho National Engineering and Environmental Laboratory, in conjunction with Sandia National Laboratory, are developing a SCADA test bed to help identify vulnerabilities and improve the security and stability of SCADA systems.[65] This test bed is part of an integrated Critical Infrastructure Test Range, which includes cyber security, wireless communications, power transmission, and physical security testbeds.[66] The Pacific Northwest National Laboratory has developed a Critical Infrastructure Protection Analysis Laboratory where, among other things, the vulnerability of SCADA systems can be determined.[67]

Research into advanced technologies is currently underway at Department of Energy laboratories to address process control system security. For example, Sandia National Laboratory under the Laboratory Directed Research and Development program has been developing secure control systems for the energy industry.[68] Research includes new information architectures, cryptographic methods, and information system security assessments. Much of this work arises from needs discovered through partnerships with systems manufacturers. While a prototype system to demonstrate proof of principle has been implemented at the Sandia National Solar Thermal Test Facility, this system has not been widely implemented in the field.[69] Similar security efforts, though less directly focused on industrial control systems, are being developed at both Lawrence Livermore National Laboratory and Los Alamos National Laboratory.

---

[63] Remarks of James F. McDonnell, Director of the Office of Energy Assurance, at a press conference in Palo Alto, CA, on September 19, 2002.

[64] "21 Steps to Improve Cyber Security of SCADA Networks," Department of Energy, 2002.

[65] For more information about the Idaho National Engineering and Environmental Laboratory's Critical Infrastructure Protection Program, see online at [http://www.inel.gov/nationalsecurity/critical_infrastructure_protection_program/].

[66] Personal Communication from Robert Tuttle, Office of Congressional and Intergovernmental Affairs, U.S. Department of Energy, August 27, 2003.

[67] *Securing Our Homeland*, Pacific Northwest National Laboratory, available online at [http://www.pnl.gov/main/sectors/homeland.html].

[68] Rolf Carlson, "Sandia SCADA Program High-Security SCADA LDRD Final Report," Sandia Report SAND2002-0729, Sandia National Laboratories, April, 2002.

[69] Sandia National Laboratories, "Dish/Sterling Provides Test for Secure Control System," *Sandia Technology*, Vol. 3, No. 1, Spring, 2001.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has initiatives in industrial control system security. NIST, in conjunction with a number of industry groups, federal government agencies, and professional societies, have created the Process Control Security Requirements Forum to develop process control information security requirements. Through their Critical Infrastructure Protection program, the National Institute of Standards and Technology is developing information security requirements, best-practice guidelines, and test methods for the process control sector.[70] Scientists at NIST are also actively involved in many industry-standards forums.

Department of Defense

The Department of Defense, through the Combating Terrorism Technology Support program, provides support for the protection of infrastructure elements. As part of this program, encryption algorithms for SCADA systems are being developed and tested with the end goal of providing recommendations to industry regarding their use.[71]

Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) is an independent regulatory agency within the Department of Energy that, among other duties, regulates interstate commerce in oil, natural gas, and electricity. FERC has published a final rule related to critical energy infrastructure information. In this rule, critical energy infrastructure information (CEII) is defined as:

> ... information about proposed or existing critical infrastructure that: (i) Relates to the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and (iv) Does not simply give the location of the critical infrastructure.[72]

Whether or not information falls under the CEII categorization is initially determined by the companies submitting the information to FERC. Categorization of select information as CEII may lead to greater information sharing between industry and the federal government.

---

[70] For more information on the Critical Infrastructure Protection program and the Process Control Security Requirements Forum, see [http://www.mel.nist.gov/proj/cip.htm].

[71] Office of the Secretary of Defense, Department of Defense, *OUSDC Budget Justification Materials, FY 2004 Budget*, PE 0603122D8Z, February 2003.

[72] *Federal Register*, Volume 68, Number 41, March 3, 2003, pp. 9857-9873, at p. 9857.

The FERC has also published a notice of public rulemaking which includes cyber-security standards for the electric industry.[73] This proposed regulation would require the electric industry to self-certify that they are meeting minimum cyber-security standards. It has been reported that FERC will likely adopt standards developed by the North American Electric Reliability Council in the final version of this regulation.[74] The final version of this regulation has not been issued.[75]

Industry Initiatives

Some industry groups have taken steps towards addressing control system security, generally as part of an overall cyber-security initiative.[76] Some groups have launched initiatives in developing infrastructure security programs.[77] The North American Electric Reliability Council has developed a set of minimum cyber-security standards for the electricity industry, as well as guidelines for securing remote access to critical electric infrastructure.[78]

Another approach is to develop voluntary best-practices for process control system security. Several organizations are taking part in such initiatives. For example, the Instrument Society of America has formed a committee, ISA-SP99, to develop a series of reports on best-practices and procedural improvements which would enhance control system security.[79] Similar efforts are underway in other technical societies, including the Institute of Electrical and Electronics Engineers and the International Electrotechnical Commission, where working groups on process control systems and their security are established.

Some industry groups have focused on developing near-term solutions to the legacy equipment security vulnerabilities. For example, the Gas Technology Institute

---

[73] *Federal Register*, Volume 67, Number 168, August 29, 2002, pp. 55451-55550.

[74] "FERC Likely to Adopt Electric Industry's Cyber Security Standards," *Electric Power Alert*, Vol. 13, No. 14, July 9, 2003, and Rick Nicholson and Terry Ray, "How Tight Is Your Padlock?" *Platts Energy Business & Technology*, May 2003.

[75] Due to controversies surrounding other provisions of this proposed regulation, questions have arisen regarding when, or if, this proposed regulation will be promulgated. For more general information on this proposed regulation, see CRS Report RS21407, *Federal Energy Regulatory Commission's Standard Market Design Activities* by Amy Abel.

[76] For example, the chemical sector has begun a Cybersecurity Practices, Standards and Technology Initiative, which will develop practices and standards and encourage development of improved security technology. For more information, see online at [http://www.cidx.org/default_CyberSec.asp?Level=2&SecondLevelURL1=/Security/Security.asp].

[77] The Electric Power Research Institute, for example, has developed a series of primers addressing information security within the energy and power industry. For more information about the Electric Power Research Institute, see [http://www.epri.com].

[78] Information on the North American Electric Reliability Council's efforts in critical infrastructure protection can be found online at [http://www.nerc.com/cip.html].

[79] For more information on ISA-SP99, see online at [http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821].

has focused on developing cryptographic protection of SCADA communications and developing a mechanism for retrofitting legacy equipment to handle these encrypted signals.[80] Other groups have increased outreach efforts to improve understanding of security issues relating to cybersecurity and process control systems.[81]

Policy Options

The vulnerability of industrial control systems may be reduced through a range of federal actions. These include the development of standards, either voluntary or mandatory, for cybersecurity of control systems; identifying and addressing critical infrastructure interdependencies; developing encryption methods for control systems; identifying and establishing technologies to address existing vulnerabilities; funding long-term research into secure SCADA systems; providing for free exchange of risk information between the federal government, private industry, and other critical infrastructure sectors; and assessing federal activities in this area.

Developing Standards

The federal government could mandate and enforce a uniform security standard for cybersecurity of industrial control systems, or support the development of industry developed and based standards. Because of the national importance of critical infrastructure systems, a uniform standard might be developed, with the input of advocates, industries and the federal government, which would include the functionality necessary to protect industrial control systems, while providing for more secure operation. A voluntary, standards-based approach has been developed for server operating systems with some success, and a similar mechanism might be used to develop standards for commercial off-the-shelf control systems.[82] Alternately, processes and specifications currently being developed through industry-led programs might be generalized across critical infrastructure industries and established as a voluntary standard. Critics of this approach cite the many different uses of industrial control systems in different industry sectors as making such a standard unwieldy. Some experts have expressed concerns that a mandated standard would be less effective than a voluntary standard, as solutions to new problems could not be implemented immediately, but would wait for changes to the standard, and that such a standard may not be uniformly applicable across industry sectors. Others have stated that there is a need for federal requirements to assure that appropriate attention is focused on process control system security.

---

[80] See, for example, American Gas Association, "Cryptographic Protection of SCADA Communications," AGA Report 12-1, April 2003.

[81] For more information about the Partnership for Critical Infrastructure Security working groups, see online at [http://www.pcis.org/library.cfm?urlSection=WG].

[82] The Center for Internet Security, a not-for-profit organization, develops consensus security standards for computer systems. They can be found online at [http://www.cisecurity.org/].

Identifying Sectoral Interdependencies

Identifying the dependencies between critical infrastructure sectors, the vulnerabilities that are present in information technologies in these sectors, and the possible cross-sectoral impacts of a control system attack may lead to a greater understanding of the scale of the control system threat. As shown by the August 2003 blackout, the loss of a single infrastructure sector, here the energy sector, may have serious effects in other critical infrastructures, such as public health and transportation. Both the Department of Homeland Security, in its role of protecting infrastructure, and the Department of Energy, in its role of ensuring a robust and reliable energy infrastructure, perform activities in determining sectoral dependencies and commonalities. Policymakers may wish to enhance current funding into SCADA security research, test bed modeling, or critical infrastructure vulnerability assessment to further clarify the current vulnerability.

Securing Control System Communications

Another option would involve supporting encryption research to protect industrial control system data transfer. Encrypting the information transmitted between remote units and their controllers would inhibit inclusion of false information to and from industrial control systems. Current encryption technology may not be compatible due to the time required to process the encrypted data and the level of technology built into control system components. Industrial control systems have stringent timing requirements and tend to be built out of less computationally robust components, which complicate the use of current encryption technologies.[83] While a prototype encryption method for industrial control systems has been developed, it is still in the validation process[84] and is only recently being evaluated for implementation in industry.[85] Further research into encryption techniques for these processes could provide efficient, market-driven technology for securing industrial control systems information. Some experts highlight that securing data transfer does not assure the security of the control system itself. They assert that other routes of attack exist that do not rely on the security of the control system communications. Thus, securing those communications, while lowering system vulnerability, may not be addressing the most likely threat.

---

[83] See, for example, Alan S. Brown, "SCADA vs. the Hackers," *Mechanical Engineering*, December, 2002.

[84] William F. Rush and John A. Kinast, "Here's What You Need To Know To Protect SCADA Systems From Cyber-Attack," *Pipeline & Gas Journal*, February 2003.

[85] Jennifer Alvey, "Digital Terrorism: Holes in the Firewall? Plugging Cyber Security Holes Isn't as Easy as Everyone Wants to Think," *Public Utilities Fortnightly*, March 15, 2002; and American Gas Association, *Cryptographic Protection of SCADA Communications – Draft 2*, AGA Report No. 12, January 2, 2004, found online at [http://www.gtiservices.org/security/AGA12Draft2r20.pdf].

Securing Legacy Equipment

Further research and development into methods for retrofitting existing SCADA systems with more secure components or communications may be another method to reduce system vulnerability. This approach has been taken by researchers in both industry and federal government laboratories. While potentially addressing short term needs to reduce vulnerability, retrofit solutions are not likely to solve inherent shortfalls in SCADA security especially with respect to the inclusion of COTS equipment potentially vulnerable to cyber attack. Critics of retrofit solutions cite high costs and potential compatibility concerns as barriers to easy implementation of such solutions.

Increasing Research and Development Funding

A long term approach to limiting the vulnerability of SCADA systems is to provide further targeted investment into developing "next-generation" secure control systems. Development of a secure SCADA architecture may provide incentives to replace components in a secure manner during the normal replacement cycle, incrementally reducing the present vulnerability. While some argue such product research and development is a responsibility of private industry, others may assert that control system security is of national import, requiring enhanced federal investment.

Several National Laboratories have developed complementary testbed facilities to investigate potential vulnerabilities and solutions to SCADA systems. Such testbed facilities could be used to evaluate and validate the security of commercial SCADA systems, act as a proving ground for new technologies, or be dedicated to the development of federal efforts in secure process control systems.

Increasing Information Sharing

The new FOIA exemptions created in the Homeland Security Act of 2002 (P.L. 107-296) may provide a higher volume, freer exchange of information between the federal government and industry, as industry may become more forthcoming about potential vulnerabilities. The Critical Energy Infrastructure Information category for electrical infrastructure information may provide a model for how regulatory agencies might craft regulations protecting critical infrastructure information within a sector. Comments from various groups on the proposed implementation of the Homeland Security FOIA exemption have indicated that industry concern still remains over the potential release of information given to the federal government by private industry.[86] Policymakers may wish to inquire into whether vulnerabilities transmitted to the federal government are eventually reduced, and how the information being provided to the federal government is used.

---

[86] *Federal Register*, Volume 68, Number 72, April 15, 2003, pp. 18524; and "Businesses Support Sharing Information on Infrastructure with Federal Agencies," *BNA Daily Environment Reporter*, September 4, 2003, p. A-7.

Oversight of Department of Homeland Security Coordination

Policymakers may also wish to assess the effectiveness of the Department of Homeland Security in coordinating security enhancements to control systems, promoting government/industry partnerships, and performing risk and vulnerability assessments. With the concentration of previously existing agencies into the Directorate of Information Analysis and Infrastructure Protection, previous duplication of effort may be removed, but critics have suggested that difficulties in integrating these agencies may lead to a reduction in effectiveness. Some policymakers have expressed concern that the priorities DHS have placed on physical and cyber-security are not appropriate for the risks involved.[87] Oversight of DHS's efforts to rectify this potential homeland security vulnerability may provide insight into successful models used within critical infrastructure sectors which might be used across multiple sectors.

---

[87] "Blackout, Computer Viruses Have Congress Worried," *Gainesville Sun*, September 7, 2003.