How Do We Protect the Civilian Infrastructure?

By Stewart A. Baker and Paul R. Hurst
URL: www.steptoe.com Email: sbaker@steptoe.com
Steptoe & Johnson LLP

Threats to the national critical infrastructure are much in the news. Is there a cyber-terrorist currently plotting a strike on America's power companies? Many argue that right now there is no active information warfare threat. But others, including many close to the Clinton Administration's thinking, argue that the absence of a threat is a temporary thing, that the nation's enemies will sooner or later be tempted by the "naked vulnerabilities" of our increasingly networked infrastructure.

The Commission on Critical Infrastructure Protection

To remedy these vulnerabilities, President Clinton created the Commission on Critical Infrastructure Protection (CCIP) by Executive Order Number 13010 in July 1996. This Commission's task is to evaluate the current physical and cyber threats to the civilian infrastructure (e.g., power companies, banking, telecommunications) and to develop a national security strategy for this infrastructure by July 1997. Although the President has yet to officially appoint the Chairman of the Commission, Robert Thomas Marsh is the expected nominee; he and most of the Commissioners have already begun working towards meeting the Commission's tight deadline.

One of the most difficult challenges CCIP faces is developing the trust required to adequately evaluate and address the vulnerabilities of the infrastructure. Many companies are reluctant to report computer intrusions or other vulnerabilities due to possible negative ramifications and the proprietary nature of this information. One way to ease this concern is to protect such information from Freedom of Information Act requests, leaks, and similar risks. The CCIP is already seeking ways to achieve this goal.

Government v. private security standards

The Commission also faces other challenges. First, should the federal government mandate a certain level of computer security? Large parts of the civilian infrastructure are subject to existing regulatory regimes that the government could use to mandate security standards. For instance, federal regulators already review the computer security practice of banks. But the computer security standards imposed on banks have been criticized as lagging rather than leading technical change. And private industry would resist mightily any federal government mandates that set wide-reaching security standards.

Complete reliance on market forces to dictate the level of security, however, may leave the infrastructure vulnerable in many ways. If some businesses choose to forgo high security standards, breaches of their systems may provide a gateway into the systems of their business partners. Other industries simply may not have financial incentives to establish the most secure standards to protect their systems. This is particularly true for industries -- like the energy sector -- where theft of service has not made security the sort of bottom-line issue it is in, say, banking or cellular telephones.

Other roles for government?

Even if government does not regulate private-sector computer security standards, it may play a role in protecting

against information warfare attacks. Instead of issuing mandates, for example, it could use reduced liability as an incentive to follow good security practices.

Second, the government -- perhaps even the Defense Department -- may have a proper role in helping the civilian system recover after an attack. Some minimum recovery mechanism is desperately needed, but it is not clear who will pay for it or how it would work.

The Role of NSA

All of these proposals create legal issues. In addition, restrictions on the National Security Agency (NSA) pose special problems for the Commission. For example, should NSA divulge advanced defensive measures for information systems to private industry? Even though this may bolster the security of the private sector's systems, what will be the effect on the security of our government systems or our intelligence efforts? Also, giving NSA a large role in dealing with the private sector on these issues raises concerns under the Computer Security Act, which restricts direct consultation between NSA and the private sector.

Similarly, who should have jurisdiction over computer attacks? Computer attacks clearly invoke the jurisdiction of law enforcement authorities, but the intelligence community (e.g., NSA) has the greater expertise and is better suited to responding to organized attacks. The intelligence community, however, has jurisdiction principally in foreign and national security matters and is highly restricted in domestic affairs. Since authorities rarely know who a computer attacker is or from where an attack originated, how can the government decide which intrusions are serious enough to allow the defense intelligence communities to respond?

Conclusion

CCIP is an important step in recognizing the need to address the vulnerabilities of the civilian infrastructure. Importantly, CCIP is both a public and private commission consisting of Commissioners from the government and industry. To address these issues (and others), there must be a consensus between government and industry whereby both the civilian infrastructure and American businesses are adequately protected.