Distributed by Penny Hill Press

BT-1028
Updated Sept. 10, 2002

Congressional Research Service
CRS

http://pennyhill.com

Cyberterrorism

Steven A. Hildreth

Issue Definition

In the wake of the terrorist attack on September 11, 2001, some observers renewed their warnings of possible terrorist attacks on U.S. critical infrastructures using easily accessible computer networks. For instance, Marv Langston, former Department of Defense official, warned that the United States needs to prepare for an "electronic Pearl Harbor." Concerns were registered previously by White House officials, Members of Congress, and the private sector about how best to live with inherent vulnerabilities of the information age and dependencies upon critical systems that control key government and industry networks.

After the U.S. air strikes began against the Taliban and bin-Laden in Afghanistan, the FBI issued a nationwide alert to law enforcement agencies and the private sector to prepare for the possibility of attacks against critical infrastructure facilities. Some of these attacks might come electronically, they warned. To date, however, no evidence has surfaced that terrorists have mounted such attacks.

A key issue is how best to balance reaction to the likelihood of cyberterrorist threats compared to other terrorist threats, and their potential consequences for American and democratic values. The challenge of dealing with cyberterrorism is compounded by concerns over privacy and national security.

Current Situation

Cyber threats or cyber intrusions are unauthorized attempts to penetrate computers, computer controlled systems, or networks. Such unauthorized activities can range from simply penetrating a system and examining it for the challenge, thrill, or interest, to entering a system for revenge, to steal information, to cause embarrassment, to extort or steal money, or to cause deliberate localized harm to computers or damage to a much larger infrastructure, such as a water supply or energy system.

Cyberterrorism is one of many types of cyber threats generating concern. These other threats include computer hacking, cyber warfare, and cyber crime. Cyberterrorism is different, however, in that its goals might include political or economic destabilization, or sabotage or theft of military or civilian assets and capabilities for political purposes or tactical advantage.

Cyberterrorists might work on behalf of nations hostile to U.S. interests, or they might operate outside the control or influence of other nations. In general, however, it would be difficult to discern cyberterrorist attacks from any other cyber attack in a timely manner.

Terrorists reportedly use computers and the Internet to conduct the business of terrorism. This includes communicating and planning with one another, raising money, gathering intelligence, recruiting, and spreading their message and propaganda.

But terrorists apparently have not used or planned to use computers or the Internet to try and disrupt critical infrastructures. This is a point Richard Clarke, currently Special Adviser to the President on

Cyberspace Security and former NSC Coordinator for Security and Infrastructure Protection, has made several times.

Even so, government officials at various agencies have focused on the possibility of cyberterrorism since the September 11th terrorist attack. For instance, The FBI's National Infrastructure Protection Center held an emergency meeting on September 12 to assess possible cyber threats. But there was not much of a change at the Defense Department where the Joint Task Force for Computer Network Operations was already on continuing alert for unauthorized cyber attacks. Richard A. Clarke, appointed October 9, 2001, by President Bush as Special Adviser to the President for Cyberspace Security, said his mandate is to secure U.S. cyberspace from a range of possible threats, "from hackers to criminals to terrorist groups, to foreign nations."

The private sector also has taken steps to protect its own networks. One organization called Riptech, which oversees computer security for hundreds of companies, reportedly went on heightened alert after the September 11th attack.

Policy Analysis

The concern over possible cyber threats to U.S. critical networks from terrorists focuses primarily on potential rather than known capabilities possessed by terrorists. Some computer experts assert that computer and software tools can be exploited to penetrate and disrupt important networks, power plants, commercial centers, and water systems, for instance. Others would take issue with how easily this might be accomplished, noting the complexity and redundancy that exists with many systems, as well as the defensive mechanisms already in place to thwart or mitigate such attacks. These observers would also cite the paucity of evidence that terrorists have considered this form of attack.

Another issue that is debatable is the degree to which such an attack might be disruptive. Those who believe such attacks are possible or inevitable generally predict relatively catastrophic results. Others would suggest such attacks may be far more localized, perhaps similar in disruptive effect to large storms and power outages in a metropolitan area.

Options and Implications for U.S. Policy

The possibility of cyberterrorism presents several key challenges. First, due to their inherent nature, computer attacks are virtually impossible to predict or trace in real time. Hence, an attack might originate at any time, here or abroad, by thrill-seeking teenagers, hostile nations, criminals, spies, or terrorists; it would take considerable resources to determine with high confidence who was responsible. Technology in the near-term does not appear to be able to resolve this problem. Second, due to the complexity of disparate laws around the world governing the collection of evidence in such events that might use the Internet or other electronic means, as well as their prosecution, the pursuit, capture, and extradition of individuals responsible is problematic. Changing conflicting laws currently in place in numerous countries would be a challenging long-term endeavor. Third, in the wake of the September 11th attack, there may be an unprecedented opportunity for the United States to deal with some of the previously intractable issues associated with cyberterrorism. With proper allocation of resources, government, industry, and others in the private sector might find solutions to potentially dangerous and worrisome scenarios.

Role of Congress/Legislation

In a general sense, Congress can play a vital role in providing funding and exercising oversight of programs for 1) intelligence gathering on potential cyberterrorist threats and capabilities (e.g., through the intelligence community and FBI budgets); 2) protection and possible recovery of critical U.S. infrastructure against cyberterrorist attacks (e.g., through the various and numerous executive branch agency appropriations); and 3) developing technologies and capabilities to detect and thwart cyber attacks from terrorists and others (e.g., through the research and development efforts of numerous agencies and labs).

A bill that touched on some of these points and others was H.Con.Res. 22, introduced by Rep. Jim Saxton in February 2001. This bill would designate cyberterrorism as an emerging national security threat. It also calls for federal and private sector partnership, a revised legal framework for dealing with the problem, and a new federal study to assess the threat posed by cyberterrorists. The bill remains under consideration by the Committee on the Judiciary and the Committee on Education and the Workforce.

Several bills were introduced in October 2001 related in whole or part to cyberterrorism, including S. 1568 (the Cyberterrorism Prevention Act of 2001; introduced by Sen. Hatch), H.R. 3108 (the USA Act of 2001; introduced by Rep. Sensenbrenner), and H.R. 3162 (the USA Patriot Act; introduced by Rep. Sensenbrenner).

Section 814 of the USA PATRIOT ACT (P.L. 107-56) is entitled Deterrence and Prevention of Cyberterrorism. This section drew heavily on elements of the three bills mentioned above. In general, the new law clarifies what are protected computers and systems and increases fines and prison terms for damages to computer systems and networks.

More recently, legislation to create a new Homeland Security agency would centralize responsibilities for cyber protection, which would include cyberthreats from terrorists. S. 2452 (the National Homeland Security and Combating Terrorism Act of 2002) would create a Directorate of Critical Infrastructure Protection; H.R. 5005 (the Homeland Security Act of 2002) would create the position of Under Secretary for Information Analysis and Infrastructure Protection.

CRS Products

CRS Report RL30735, *Cyberwarfare*.