Definition: **cyberterrorism** from *The Macquarie Dictionary*

1. a type of terrorism in which computer networks, data, etc., are damaged or altered to harm a targeted group or country.

cyberterrorist noun

Summary Article: **Cyberterrorism**
From *The SAGE Encyclopedia of Terrorism*

The term *cyberterrorism* refers to the convergence of terrorism and cyberspace, particularly the politically motivated sabotage of information systems. Since the 1990s, incidents of hacking, cybercrime, and highly destructive computer viruses have been widespread, and these tools have increasingly been used for specific political ends.

Barry Collin, of the Institute for Security and Intelligence in California, coined the term *cyberterrorism* in the 1980s. In a 1997 paper, Collin described possible cyberterror scenarios. In one, a cyberterrorist hacks into the computer system of a cereal manufacturer and raises the level of iron in each box, causing innumerable children to get sick and die. In another scenario, cyberterrorists destabilize an entire country by attacking financial institutions and stock exchanges en masse.

Collin's third scenario, in which a cyberterrorist hacks into an air traffic control system, came close to reality in 1997, when a teenager gained access to a phone switch at a small Massachusetts airport and accidentally cut off all communications for the control tower for several hours. Alarming as it was, the incident was seen more as hacking gone awry than cyberterror, as the teenager lacked any political motivation.

Still, many point to destructive viruses and worms, and to denial-of-service attacks, as the seedlings for larger events. In 1999 the Melissa virus, an e-mail virus named after a Florida stripper, affected more than a million computers and caused at least $80 million in damages. (Melissa's creator, David Smith, pled guilty and was sentenced to 20 months in prison in May 2002.) In May 2000, the Love Bug virus (also called the ILOVEYOU virus) affected even the CIA and British Parliament and caused more than $10 billion in damages worldwide. The Nimda virus, discovered in 2001, has caused damages estimated at $500 million and hobbled entire businesses for days at a time.

Though viruses still constitute a threat, a more recent form of cyber attack has been the denial-of-service attack. In February 2000, Yahoo, CNN, eBay, and other e-commerce sites were flooded by e-mail messages from attacking computers, which slowed service and blocked other users from the sites, causing an estimated $1 billion in losses.

Other incidents worldwide have combined these hacking techniques with political messages. In what is
believed to be the first cyber attack by terrorists against a country’s computer systems, in 1998, an offshoot of the Liberation Tigers of Tamil Eelam swamped the Sri Lankan embassies with thousands of e-mails that read, “We are the Internet Black Tigers and we’re doing this to disrupt your communications.” In India, a group of international hackers against nuclear proliferation, called Milw0rm, hacked into the Bhabha Atomic Research Centre and posted the message, “If a nuclear war does start, you will be the first to scream,” which was transposed over a photo of an atomic mushroom cloud. Similar attacks have been perpetrated against NATO sites during the conflict in Kosovo, to protest the World Trade Organization, and, particularly after the United States accidentally bombed the Chinese embassy in Belgrade, against U.S. government sites.

While denial-of-service attacks, e-mail bombs, website sit-ins, webpage takeovers, and viruses—sometimes referred to, collectively, as “hacktivism”—have not claimed lives or caused much more than nuisance and financial loss, many believe that these tactics could be used to complicate and magnify real-world attacks. Jeffrey A. Hunker, a former senior director for protection of critical infrastructure for the National Security Council, has stated that cyberattacks could act as a “force multiplier” for a bombing or attack by either by posting false information on the Internet to create panic, or by sabotaging financial, emergency, or communication networks. In 1997 the Clinton administration’s Commission on Critical Infrastructure Protection concluded that electronic money transfers, the power grid, 911 services, and military command sites were also vulnerable to cyber attack. The commission’s report stated, “Our dependence on the information and communications infrastructure has created new cyber-vulnerabilities, which we are only starting to understand.”

In response to the commission’s finding, President Clinton issued an order to create the National Infrastructure Protection Center, to protect vital national systems, such as telecommunications networks and the power grid, and to upgrade government computer security. One of Clinton’s officials, Richard Clarke, continued under the Bush administration to deal directly with the threat of cyberterror. He was named special advisor for cybersecurity to the president shortly after the September 11 terrorist attacks.

By the late 1990s, the U.S. government faced daily cyber assaults on its computers and websites. Attacks against Department of Defense computers rose from less than 1,000 in 1997 to nearly 23,000 in 1999. A series of cyber attacks on high-level businesses and the Pentagon, beginning in 1998, is believed to be linked to organized crime in Russia. American hackers engaged in a “cyberwar” with their Chinese counterparts, which consisted of little more than defacing the other country’s websites.

Of more concern were forays into large-scale sabotage, such as the 2000 hack into one of California’s electrical transmitting stations, believed to have been perpetrated by hackers in China, and espionage-like hacks into sensitive information systems, such as the 1998 hack into NASA’s Jet Propulsion Laboratory. Cyber espionage has become increasingly common as the decade has progressed.

State-Sponsored Cyberterror?

In 1996, CIA Director John Deutch warned of an upcoming “electronic Pearl Harbor.” Over the next decade, however, little happened to support that claim. Skeptics began to argue that cyberterror had little appeal to traditional terrorists, due to the lack of drama and small likelihood of significant injury or death, but also because traditional terrorist tools, such as suicide bombings, were still quite effective. It appeared that hackers with the tools to disable key governmental or corporate computer systems
lacked the political motivation to do so, while terrorists motivated to crumble information systems to
cause chaos lacked the requisite computer skills. While it might be true that an extremist terror group
like al Qaeda is not likely to pursue cyber attacks in the 2000s, another group of actors has found
cyberterrorism attractive, namely national governments. Cyberterror appeals to governments precisely
because it is a less dramatic form of attack. A cyber attack is unlikely to lead to mass casualties and the
retaliation such casualties would cause. In addition, attracting skilled hackers is easier for a government
than for a terrorist group, because the hackers are acting legally—at least by their own nation's laws.

The most enticing aspect of cyberterror for governments is its deniability. It is all but impossible to
prove that a government launched a cyber attack. Even if the attack can be traced back to a particular
country—and a skilled hacker can conceal an attack’s geographical origin—finding the individuals
responsible is very difficult, especially if the government involved is unwilling to conduct a serious
investigation. The government can always claim the attack was committed by independent hackers, and
since the target country cannot prove otherwise, retaliation is unlikely.

The first major incident of what is believed by most observers to have been state-sponsored
cyberterror occurred in 2007, when the country of Estonia came under a massive denial-of-service
attack that lasted for weeks. Estonia is very dependent on the Internet, and the attack not only shut
down government websites, it also targeted private-sector websites, such as stores and banks,
causing major inconveniences for Estonia's civilian population. Estonia's telephone system also proved
vulnerable, and for a period of several hours Estonians could not call emergency numbers. At the time
of the attack, Estonia was in the midst of a diplomatic confrontation with Russia, but the Russian
government denied involvement, and Estonia has never been able to prove that it was responsible.

In August 2008, Russia's military attacked the neighboring country of Georgia. At the same time,
Russian nationalists launched a website from which anyone could download a simple tool that would
allow their computer to participate in a denial-of-service attack against Georgian government
websites. Once again, the Russian government denied involvement, although many observers doubt
that such organized campaigns could have taken place without at least the tacit permission of the
Russian authorities.

Smaller attacks have been linked to North Korea and China, but in every case it has been impossible to
prove government responsibility. In addition, international law is unclear as to whether a country under
cyber attack can legally retaliate using other means, such as a military strike. There have been increasing
calls for the international community to address the issue, as well as a campaign to make the Internet
itself a less anonymous medium. At the moment, however, the penalties for cyberterrorism are
basically nonexistent, making it likely that nations will continue to sponsor and engage in surreptitious
cyberwarfare.

See Also:
Asymmetrical Warfare, Liberation Tigers of Tamil Eelam, State Terrorism, State-Sponsored Terrorism

Further Readings

- Alexander, Yonah, and Swetnam, Michael S., eds. Cyber Terrorism and Information Warfare. Dobbs

Laura Lambert

APA

Chicago

Harvard

MLA

APA

Chicago

Harvard

MLA