

Significant Cyber Incidents Since 2006

This list is a work in progress that we update as new incidents come to light. If you have suggestions for additions, send them to techpolicy@csis.org. Significance is in the eye of the beholder, but we focus on successful attacks on government agencies, defense and high tech programs, or economic crimes with losses of more than a million dollars.

1. **May 2006:** The Department of State's networks were hacked and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spend the night carting off file cabinets it would be an act of war, but when it happens in cyberspace, we barely notice.
2. **August 2006** A senior Air Force Officer states publicly that "China has downloaded 10 to 20 terabytes of data from the NIPRNet [the unclassified military network]."
3. **September 2006:** Israel disrupts Syrian Air defense networks (with some collateral damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility
4. **December 2006:** NASA was forced to block email with attachments before shuttle launches out of fear they would be hacked, and Business Week Reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.
5. **2006** Chinese hackers are thought to be responsible for shutting down the House of Commons computer system.
6. **April 2007:** The Department of Commerce had to take the Bureau of Industrial Security 's networks offline for several months. This Commerce Bureau reviews high tech exports and its networks were hacked by unknown foreign intruders.
7. **May 2007:** "The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that let spyware on the system."
8. **May 2007:** Estonian government networks are harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services are temporarily disrupted and online banking is halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well, but they created a wave of fear in countries like the U.S. that depend heavily on cyberspace.
9. **June 2007:** The Secretary of Defense's unclassified email was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit on DOD networks.
10. **August 2007:** The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.
11. **September 2007:** Contractors at DHS and DOD had their networks hacked, as backdoors into agency systems.

12. **September 2007:** British authorities report that hackers, believed to have come from China's People's Liberation Army, penetrate the network of the Foreign Office and other key departments.
13. **October 2007:** China's Ministry of State Security says foreign hackers steal Chinese key areas' information. 42% from Taiwan and 25% from United States. In 2006, when China's CASIC (China Aerospace Science & Industry Corporation) Intranet Network was surveyed, spywares are all found in computers in classified departments and corporate leaders.
14. **November 2007:** Jonathan Evans, the head of Britain's Security Service (MI5), warns 300 business firms of the increased online threat from Russian and Chinese state organizations, saying "a number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They. ...increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks."
15. **January 2008:** A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.
16. **March 2008:** South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.
17. **March 2008:** US officials report that American, European and Japanese companies are experiencing significant losses of intellectual property and business information to criminal and to industrial espionage in cyberspace, but details cannot be provided in an unclassified setting.
18. **May 2008:** the Times of India reports that Indian official accuse China of hacking into government computers, and say that the core of the assault is the Chinese scanning and mapping India's official networks, to gain access to content and to plan how to disable or disrupt networks during a conflict..
19. **June 2008:** The networks of several Congressional offices were hacked by unknown foreign intruders. Some incident involved offices with an interest in human rights in Tibet.
20. **Summer 2008:** The databases of both Republican and Democratic presidential campaigns were hacked in the summer of 2008 and downloaded by unknown foreign intruders.
21. **August 2008:** Computer networks in Georgia are hacked by unknown foreign intruders, most likely at the behest of the Russian government. There is little or no disruption of service but much press attention is given to annoying graffiti on Georgian government websites.
22. **November 2008:** Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and resecure the networks.

23. **December 2008:** Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some CSIS staff would go into the new administration and may have thought it might be interesting to read their emails beforehand.
24. **2008:** Britain's MPs are warned about e-mails apparently sent by the European Parliament, amid fears that they could be used by Chinese hackers to implant viruses. Chinese hackers were also thought to be responsible for shutting down the House of Commons computer system in 2006.
25. **January 2009:** Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip that briefly paralyzed government sites. The attack, which focused on government Websites, was executed by at least 5000,000 computers. Israeli officials believe carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.
26. **January 2009:** Indian Home Ministry officials warn that Pakistani hackers have placed malware on popular music download sites used by Indians in preparation for cyber attacks.
27. **February 2009:** FAA computer systems were hacked. As the FAA's increasing use of modern IP-bases' networks increase, so does the risk of the intentional disruption of commercial air traffic.
28. **February 2009:** 600 computers at India's Ministry of External Affairs are hacked.
29. **February 2009:** French naval aircraft planes were grounded after military databases were infected with the Microsoft "conficker" virus. Naval officials suspect someone at the navy had used an infected USB key.
30. **March 2009:** The German government warned that hackers were offering a freeware version of the new Microsoft operating system that installs Trojans."
31. **March 2009:** Canadian researchers find a computer espionage system that they attributed to China implanted on the government networks of 103 countries.
32. **March 2009:** Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.
33. **April 2009:** Wall Street Journal articles have laid out the vulnerability of the U.S. power grid to cyber attack – a vulnerability the U.S. is busily increasing – and the intrusions into F-35 databases by unknown foreign intruders.
34. **May 2009:** In May 2009, Merrick Bank, a leading issuer of credit cards, claimed it lost \$16 million after hackers compromised as many as 40 million credit card accounts.

35. **May 2009:** The Homeland Security Information Network (HSIN) was hacked by unknown intruders. The hackers gained access to the data by getting into the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed.
36. **June 2009:** The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated.
37. **June 2009:** German Interior Minister Wolfgang Schaeuble noted (when presenting the Interior Ministry's 2008 security report), that China and Russia are increasing espionage efforts and Internet attacks on German companies.
38. **July 2009:** Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks. The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention.
39. **August 2009:** Albert Gonzalez was indicted on charges that between 2006-2008, he and unidentified Russian or Ukrainian colleagues allegedly stole more than 130 million credit and debit cards by hacking into the computer systems of five major companies, the largest hacking and identity theft crime in U.S. history.