

Cyber Events Since 2006

1. The Secretary of Defense's unclassified email was hacked by unknown foreign intruders.
2. 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.
3. The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.
4. The Department of Commerce had to take the Bureau of Industrial Security's networks off line for several months. This Commerce Bureau reviews high tech exports and its networks were hacked by unknown foreign intruders.
5. 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 spent the night carting off file cabinets it would be an act of war, but when it happens in cyberspace, we barely notice.
6. The databases of both the Republican and Democratic presidential campaigns were hacked in the summer of 2009 and downloaded by unknown foreign intruders.
7. Estonia and Georgia had their cyber networks attacked by unknown foreign intruders, most likely at the behest of the Russian government. These were more like cyber riots than crippling attacks, and the Estonians responded well, but they created a wave of fear in countries like the U.S. that depend heavily on cyberspace.
8. 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.
9. FAA computer systems were hacked and, as the FAA increases its dependence on modern IP-based networks, the risk of the intentional disruption of commercial air traffic has increased.
10. Contractors at DHS and DOD had their networks hacked, as a back door into agency systems.
11. The networks of several Congressional offices were hacked by unknown foreign intruders. Some incidents involved offices with an interest in human rights or Tibet.
12. 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.

13. Canadian researchers found a computer espionage system that they attributed to China implanted on the government networks of 103 countries.
14. Wall Street Journal articles have laid out the vulnerability of our power grid to cyber attack – a vulnerability we are busy increasing - and the intrusions into some F-35 databases by unknown foreign intruders.
15. 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.
16. 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.
17. American, European and Japanese companies are experiencing significant losses of intellectual property and business information to criminals and to industrial espionage in cyberspace, but details are not easily provided in an unclassified setting.
18. 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.
19. Cybercrime became the most profitable and least risky form of bank robbery and credit card fraud, costing our economy tens of millions of dollars. If a robber walked into a bank with a gun and stole a million dollars, it would be all over the front page, and there have been a few cybercrime incidents involving losses of a million dollars – a recent cyber robbery in Calgary netted \$1.8 million. A smart cybercriminal has zero chance of being caught and prosecuted.
20. 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.
21. 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, he added, and the organizations that owned the data and Congress were notified of the intrusion.
22. The German government warned that hackers were offering a freeware version of the new Microsoft operating system that installs Trojans
23. South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korean military networks.