Timeline: Key events in cyber history

Explore some of the technological advances that led to cyberspace and examples of notable hacks.

1943-1944	**History** The digital era jumped ahead with the creation of Colossus, the first programmable digital machine. Though limited compared to later computers, Colossus played a pivotal role in code breaking during World War II. In effect, the British developed the first digital machine to hack German codes. • The National Museum of Computer: Colossus • Colossus: The first large-scale electronic computer
1961-1962	**History** Key steps in the history of global computer networks came when Leonard Kleinrock at MIT published the first paper on packet switching theory in July 1961, and the next year when J.C.R. Licklider, also at MIT, wrote a series of memos spelling out his ideas for a "Galactic Network" in which people could access data from anywhere. • Internet Society: Origins of the Internet
1967-1969	**History** The Advanced Research Projects Agency, later known as DARPA, accelerated work on what was initially dubbed ARPANET and eventually came to be known as the Internet. The first ARPANET message was sent at 10:30 p.m. on Oct. 29, 1969. • Internet Society: Oirginal Internet concepts • Stanford Research Institute: Celebrating the first ARPANET transmission
1971	**History** Intel released the first integrated microprocessor, a major leap forward in the history of the computer. It had 2,300 transistors and processed 60,000 instructions per second.

1982	**Hack** National security officials in the United States launched one of the world's first cyberattacks on another country: the Soviet Union. U.S. officials heard, through a KGB source named Farewell, that the Soviets intended to buy computer equipment through a front company to operate a gas pipeline. U.S. agents altered the software, which later caused the pipeline to explode. • CIA: The Farewell Dossier • At the Abyss: An Insider's History of the Cold War (book)
1986-1987	**Hack** In 1986 and 1987, a physics researcher at the University of California at Berkeley uncovered a global hack of academic, military and government computers in the United States. Chronicled later in the book “The Cuckoo's Egg,” it was the first investigation of its kind, and it revealed online hacker threats spread around the globe. • Wikipedia: The Cuckoo's Egg
1988	**Hack** The first "worm" attack occurred on the Internet. A Cornell University student named Robert Tappan Morris released several dozen lines of code, which replicated wildly and hit thousands of computers hard. It stopped about 10 percent of the 88,000 computers linked to the Internet at the time. • The What, Why, and How of the 1988 Internet Worm • CERT: Security of the Internet
1990	**History** ARPANET became an operation network known as the Internet. About 2.6 million people around the globe had access.
1994	**Hack** Anonymous hackers repeatedly attacked the Air Force's Rome Laboratory in New York, underscoring the threat to military systems. Investigators discovered that a British teenager and an Israeli technician had used phone systems and networks in eight countries to cloak their attacks on numerous military and government computer systems. • GAO (PDF): Computer attacks at the Department of Defense pose

	increasing risks
1997	**Hack** The Pentagon's first "information warfare" exercise, known as Eligible Receiver, found that industrial and information systems throughout the United States are vulnerable to cyberattacks from hackers using readily available technology and software. Specialists said it appeared as though simulated attacks on power and communications networks in Oahu, Hawaii; Los Angeles; Colorado Springs, Colo.; Washington, D.C.; and elsewhere succeeded with ease. • Congressional Research Service report (PDF): Cyberwarfare
2003	**History** The amount of digital information created by computers, cameras and other data systems this year surpassed the amount of all information created in human history, according to studies by International Data Corp. and EMC.
November 2003	**Hack** Hackers apparently supported by China attacked military and government systems in the United States with impunity, making off with terabytes of data. The attacks were dubbed Titan Rain by officials in the United States. • Washington Post: Hackers attack via Chinese Web sites
May 2007	**Hack** During a dispute between Estonia and Russia, hackers launched massive attacks on Estonian government agencies, banks, newspapers and other organization, using networks of computers to shut down Estonian systems online. Some analysts, blaming Russia, asserted the attacks represent one of the first instances of cyberwar. • Wired: Kremlin Kids: We launched the Estonian cyber war
2008	**History** Cyberspace accelerated its expansion, with the number of devices connected to the Internet exceeding the number of people on Earth for the first time. That number hit an estimated 12.5 billion in 2010, according to a researcher at Cisco who predicted it will rise to 50 billion in 2020. Hundreds of millions of new Internet users also sign on, many millions of them via mobile phones and other portable devices.

November 2008	**Hack** The most significant breach of U.S. computer security occurred, apparently when someone working with the Pentagon's Central Command inserted an infected flash drive into a military laptop computer at a base in the Middle East. The case was code named Buckshot Yankee. "The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control," a senior U.S. official later wrote in Foreign Affairs magazine. • Washington Post: Cyber-intruder sparks massive federal response
March 2009	**Hack** Canadian researchers identified a Chinese espionage network operating on government computer systems in 103 countries, making it the largest operation of its kind ever publicly identified. The researchers dubbed the system GhostNet. • New York Times: Vast spy system loots computers in 103 countries
December 2009	**Hack** Communications links with U.S. drones were hacked by Iraqi insurgents, who used laptop computers and inexpensive software. The hack apparently enabled the insurgents to see video images the drone was recording.
January 2010	**Hack** Google announced that it and dozens of other companies were the focus of a "highly sophisticated and targeted attack" originating from China. The attack resulted in a huge amount of data being stolen. It was later dubbed Operation Aurora.
February 2010	**History** The number of Internet users topped 2 billion. The Defense Department said that although "it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air and space."
July 2010	**Hack** Researchers discovered the most sophisticated cyberweapon ever to be made public. A "worm" known as Stuxnet, it was designed to seek out certain

	industrial control systems made by Siemens. Stuxnet took advantage of four zero-day vulnerabilities and appeared to be targeted at a uranium enrichment program in Iran. Specialists said it appeared to have a devastating effect, destroying or damaging hundreds of centrifuges. The New York Times reported that President Obama approved the operation as part of a secret U.S.-Israeli cyberwar campaign against Iran begun under the Bush administration.
November 2010	**History** A group of the nation's top scientists concluded in a report to the Pentagon that "the cyber-universe is complex well beyond anyone's understanding and exhibits behavior that no one predicted, and sometimes can't even be explained well." The scientists, part of a Pentagon advisory group called JASON, said, "Our current security approaches have had limited success and have become an arms race with our adversaries. In order to achieve security breakthroughs we need a more fundamental understanding of the science of cyber-security."
May 2011	**Hack** Sony told Congress that hackers had penetrated the PlayStation network, stealing or misusing the personal information of at least 77 million users. Sony estimated that fallout from the hack cost at least $170 million. It appeared as though criminals masqueraded as members of the anarchist-activist group known as Anonymous.
March 2012	**Hack** Gen. Keith Alexander, commander of U.S. Cyber Command, blamed China for taking "astounding" amounts of intellectual propery and for the hack last year of security giant RSA. In testimony before a congressional panel, Alexander hinted at military reprisals. "We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law," Alexander testified.