CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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 cyber-attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

October 2018. The U.S. Department of Justice indicted Chinese intelligence officers and hackers working for them for engaging in a campaign to hack into U.S. aerospace companies and steal information

October 2018. Security researchers link the malware used to attack a petrochemical plant in Saudi Arabia to a research institute run by the Russian government.

October 2018. U.S. defense officials announced that Cyber Command had begun targeting individual Russian operatives to deter them from interfering in the 2018 midterm elections.

October 2018. Media reports state than U.S. agencies warned President Trump that that China and Russia eavesdropped on call made form an unsecured phone.

October 2018. News reports reveal that the Israel Defense Force requested that cybersecurity companies develop proposals for monitoring the personal correspondence of social media users.

October 2018. The U.S. Department of Homeland Security announces that it has detected a growing volume of cyber activity targeting election infrastructure in the U.S. ahead of the 2018 midterm elections.

October 2018. The Centers for Medicare and Medicaid Services announced that hackers had compromised a government computer system, gaining access to the personal data of 75,000 people ahead of the start of ACA sign-up season.

October 2018. The Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government groups

October 2018. The U.S. Justice Department announces criminal charges against seven GRU officers for multiple instances of hacking against organizations including FIFA, Westinghouse Electric Company, the Organisation for the Prohibition of Chemical Weapons, and the U.S. and World Anti-Doping Agencies.

September 2018. Security researchers found that a Russian hacking group had used malware to target the firmware of computers at government institutions in the Balkans and in Central and Eastern Europe.

September 2018. In a letter to Senate leaders, Sen. Ron Wyden revealed that a major technology company had alerted multiple Senate offices of attempts by foreign government hackers to gain access to the email accounts of Senators and their staff

September 2018. Researchers report that 36 different governments deployed Pegasus spyware against targets in at least 45 countries, including the U.S., France, Canada, and the UK.

September 2018. The U.S. State Department suffers a breach of one of its unclassified email systems, exposing the personal information of several hundred employees.

September 2018. Swiss officials reveal that two Russian spies caught in the Netherlands had been preparing to use cyber tools to sabotage the Swiss defense lab analyzing the nerve agent used to poison former Russian Agent Sergei Skripal.

September 2018. Security researchers find that Iranian hackers have been surveilling Iranian citizens since 2016 as part of a mobile spyware campaign directed at ISIS supporters and members of the Kurdish ethnic group.

September 2018. Russian hackers targeted the email inboxes of religious leaders connected to Ukraine amid efforts to disassociate Ukraine's Orthodox church from its association with Russia.

September 2018. The U.S. Department of Justice announces the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers.

September 2018. The U.S. Department of Justice announces the indictment of Park Jin Hyok, a North Korean Hacker allegedly involved in the 2014 Sony hack, the 2016 theft of $81 million from a Bangladeshi bank, and the WannaCry ransomware attacks.

September 2018. Researchers reveal a new cyber espionage campaign linked to attacks against Vietnamese defense, energy, and government organizations in 2013 and 2014.

August 2018. North Korean hackers stole $13.5 million from India's Cosmos Bank after breaking into the bank's system and authorizing thousands of unauthorized ATM withdrawals, as well as several illegal money transfers through the SWIFT financial network.

August 2018. Security researchers report that Iranian hackers had targeted the websites and login pages of 76 universities in 14 countries. The attackers stole the credentials of users who attempted to sign in, gaining access to library resources for the purposes of intellectual property theft.

August 2018. Facebook identified multiple new disinformation campaigns on its platform

sponsored by groups in Russia and Iran. The campaigns targeted users in the U.S., Latin America, Britain, and the Middle East, and involved 652 fake accounts, pages, and groups.

August 2018. Microsoft announces that Russian hackers had targeted U.S. Senators and conservative think tanks critical of Russia.

July 2018. Security researchers report that an Iranian hacking group had been targeting the industrial control systems of electric utility companies in the U.S., Europe, East Asia, and the Middle East.

July 2018. The Department of Homeland Security reveal that a campaign by Russian hackers in 2017 had compromised the networks of multiple U.S. electric utilities and put attackers in a position where they could have caused blackouts.

July 2018. Senator Claire McCaskill reveals that her 2018 re-election campaign was targeted by hackers affiliated with Russia's GRU intelligence agency. Attackers unsuccessfully targeted staffers in the Senator's office with phishing emails designed to harvest their passwords.

July 2018. Researchers report that a hacking group linked to Iran has been active since early 2017 targeting energy, government, finance, and telecommunications entities in the Middle East.

July 2018. Microsoft reveals that Russian hackers had targeted the campaigns of three Democratic candidates running for the 2018 midterm elections.

July 2018. Russian hackers were found to have targeted the Italian navy with malware designed to insert a backdoor into infected networks.

July 2018. Security researchers detect a spike in hacking attempts against IoT devices in Finland during the run-up President Trump's summit with Vladimir Putin in Helsinki. The majority of attacks originated in China.

July 2018. Singapore's largest healthcare institution was targeted by state-sponsored hackers, leading to the leakage of personal information for 1.5 million patients, along with prescription details for 160,000 others.

July 2018. Ukrainian intelligence officials claim to have thwarted a Russian attack on the network equipment of a chlorine plant in central Ukraine. The virus used in the attack is the same malware responsible for the infection of 500,000 routers worldwide in a campaign the FBI linked to state-sponsored Russian hackers.

July 2018. The U.S. Department of Justice announced the indictments of 12 Russian intelligence officers for carrying out large-scale cyber operations against the Democratic Party in advance of the 2016 Presidential election. The officers' alleged crimes included the theft and subsequent leakage of emails from the Democratic National Committee and Hillary Clinton campaign, and the targeting of election infrastructure and local election officials in an attempt to interfere with the election.

July 2018. Security researchers report that Chinese hackers had been actively spying on political actors on both sides of the upcoming Cambodian elections. Targets include the country's National Election Commission, several government ministries, the Cambodian Senate, at least one Member of Parliament, and multiple media outlets and human rights activists.

July 2018. Hackers targeted the campaigns of at least two local Democratic candidates during 2018's primary season, reportedly using DDoS attacks to disrupt campaign websites during periods of active fundraising and positive news publicity.

July 2018. Australian National University (ANU) was found to have been breached by Chinese hackers in an attack believed to be motivated by a desire to siphon intellectual property from the institution.

June 2018. Marketing data firm Exactis suffered a data breach exposing the information of 340 million people, including their political preferences, browsing habits, and purchase data.

June 2018. Ukraine police claim that Russian hackers have been systematically targeting Ukrainian banks, energy companies, and other organizations to establish backdoors in preparation for a wide-scale strike against the country.

June 2018. Chinese hackers were found to be engaged in a cyber espionage campaign to collect data from satellite, telecom, and defense organizations in the U.S. and Southeast Asia.

June 2018. A Russian hacking group linked to disrupting the Peyongchang Olympics targeted individuals in France, Germany, Switzerland, Russia, and Ukraine linked to a biochemical threat conference organized by a company involved in the investigation of the poisoning of Sergei Skripal in March 2018.

June 2018. A Chinese hacking group targeted a national data center in a Central Asian country, preparing a watering hole attack to inject malicious code onto other government websites connecting to the data center.

June 2018. Researchers reveal that North Korean hackers targeted a South Korean think tank focused on national security issues. The hackers used a zero-day exploit to compromise the organization's website and insert a backdoor for injecting code.

June 2018. The U.S. Treasury Department announced sanctions against five Russian companies and three individuals for enabling Russian intelligence and military units to conduct cyberattacks against the U.S.

June 2018. Chinese government hackers compromised the networks of a U.S. Navy contractor, stealing 614 GB of data related to weapons, sensor, and communication systems under development for U.S. submarines.

May 2018. Cyber security researchers reported that North Korean hackers had been targeting

defectors through compromised Android apps hosted through the Google Play market, stealing device information and allowing the insertion of executable code stealing photos, contact lists, and text messages.

May 2018. Security researchers reveal that the Pakistani military used Facebook Messenger to distribute spyware to targets in the Middle East, Afghanistan, and India in an attempt to compromise government officials, medical professionals, and others.

May 2018. Turkish government hackers were discovered to be using surveillance software FinFisher to infect Turkish dissidents and protesters.

May 2018. An unknown group of hackers stole between $18 and $20 million dollars from Mexican banks by exploiting the SWIFT transfer system, submitting a series of false transfer orders to phantom accounts in other banks and emptying the accounts in dozens of branch offices.

May 2018. Within 24 hours of President Trump's announcement that the US would withdraw from the Iran nuclear agreement, security firms reported increases in Iranian hacking activity, including the sending of emails containing malware to diplomats in the Foreign Affairs ministries of US allies, as well as global telecommunication companies.

May 2018. Researchers reveal that a hacking group connected to Russian intelligence services had been conducting reconnaissance on the business and ICS networks of electric utilities in the US and UK since May 2017.

April 2018. Security researchers report that an Indian hacking group had been targeting government agencies and research institutions in China and Pakistan since 2013.

April 2018. Cyber security researchers reveal that North Korean hackers targeted critical infrastructure, finance, healthcare, and other industries in 17 countries using malware resembling the code used in the 2014 Sony Pictures attack.

April 2018. Israeli cyber researchers revealed that Hamas had planted spyware in mobile phones owned by members of Fatah, a rival Palestinian faction

April 2018. Reports from cyber security researchers indicate that Chinese state-sponsored hacking groups have targeted Japanese defense companies in an attempt to gain information on Tokyo's policies towards North Korea

April 2018. US and UK officials issued a joint warning that Russia was deliberately targeting western critical infrastructure by compromising home and business routers

April 2018. The director of the UK's Government Communications Headquarters (GCHQ) announced that the organization had been conducting offensive cyber operations against ISIS to suppress their propaganda, disrupt their coordination, and protect deployed military personnel

April 2018. The chief of Germany's domestic intelligence services accused Russia of being

behind the December 2017 attack on the government's computer networks

April 2018. The UK's National Cyber Security Centre released an advisory note warning that Russian state actors were targeting UK critical infrastructure by infiltrating supply chains

April 2018. All government services of Sint. Maarten, a Caribbean island and constitute country of the Netherlands, were taken offline for a week after a cyber attack. According to local authorities, this is the third cyber attack the country has faced in just over a year.

April 2018. The North Korean hacking group responsible for the SWIFT attacks was found to have targeted a Central American online casino in an attempt to siphon funds

March 2018. Online services for the city of Atlanta were disrupted after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. The city would eventually spend approximately $2.6 million recovering from the attack.

March 2018. Baltimore's 911 dispatch system was taken down for 17 hours after a ransomware attack, forcing the city to revert to manual dispatching of emergency services

March 2018. The US Departments of Justice and Treasury accused Iran in an indictment of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.

March 2018. The FBI and Department of Homeland Security issued a joint technical alert to warn of Russian cyber attacks against US critical infrastructure. Targets included energy, nuclear, water, aviation, and manufacturing facilities.

March 2018. A data breach of the company Under Armor compromised the information of 150 million users of its fitness and nutrition tracking app MyFitnessPal

March 2018. Cybersecurity researchers reveal that a Chinese hacking group used malware to attack the service provider for the UK government in an attempt to gain access to contractors at various UK government departments and military organizations

March 2018. Cybersecurity researchers announce evidence that the same North Korean hacking group linked to the SWIFT financial network attacks has been targeting several major Turkish banks and government finance agencies.

March 2018. A UN report details attempts by North Korean hackers to compromise email accounts of the members of a UN panel enforcing trade sanctions against North Korea.

February 2018. German news reported that a Russian hacking group had breached the online networks of Germany's foreign and interior ministries, exfiltrating at least 17 gigabytes of data in an intrusion that went undetected for a year.

February 2018. The Justice Department indicted 13 Russians and three companies for their online

efforts to interfere in the 2016 US presidential elections.

February 2018. The US and UK formally blame Russia for the June 2017 NotPetya ransomware attack that caused billions of dollars in damages across the world.

February 2018. A cyberattack on the Pyeongchang Olympic Games attributed to Russia took the official Olympic website offline for 12 hours and disrupted wifi and televisions at the Pyeongchang Olympic stadium.

February 2018. Officials at the Department of Homeland Security confirmed that Russian hackers successfully penetrated the voter registration rolls of several US states prior to the 2016 election.

January 2018. China denied that the computer network it supplied to the African Union allowed it access the AU's confidential information and transfer it to China, or that it had bugged offices in the AU headquarters that it had built.

January 2018. A Japan-based cryptocurrency exchange reveals that it lost $530 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time.

January 2018. Norwegian officials discover a "very professional" attempt to steal patient data from a Norwegian hospital system, in an attack they speculate was connected to the upcoming NATO Trident Juncture 18 military exercise.

January 2018. A hacking group with ties to the Lebanese General Directorate of General Security was revealed to have been involved in a six-year campaign to steal text messages, call logs, and files from journalists, military officers, corporations, and other targets in 21 countries worldwide.

January 2018. The Unique Identification Authority of India and its Aadhaar system are hacked by unknown actors, resulting in the personal data of more than 1 billion people being available for purchase.

December 2017. French company Schneider Electric was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. Analysis by security researchers indicated that the attack was sponsored by a nation-state.

December 2017. The state-owned China Aerospace Science and Industry Corporation (CASIC) is alleged to have pre-installed backdoors in biometric equipment sold to Taiwan for its e-Gate border control system. The backdoors would have allowed CASIC to gather private data on both Taiwanese and foreign citizens traveling in and out of the country since the system's installation in 2012.

November 2017. Three Chinese nationals employed at a China-based Internet security firm are indicted by a US grand jury for computer hacking, theft of trade secrets, conspiracy, and identity

theft against employees of Siemens, Moody's Analytics, and Trimble.

November 2017. Uber discloses that it paid hackers $100,000 to delete the stolen data of 57 million of its customers and drivers, including names, phone numbers, email addresses, and license plate numbers.

November 2017. Cybersecurity researchers report a cyberespionage campaign targeting government organizations in South America and Southeast Asia. The group, deemed to have nation-state capabilities, aimed to acquire foreign policy information from diplomatic and government entities.

November 2017. Cybersecurity researchers report a sophisticated Vietnamese hacking group responsible for cyber espionage campaigns targeting the ASEAN organization, foreign corporations with an interest in Vietnamese industries, and media, human rights, and civil society organizations.

October 2017. A major wave of ransomware infections hits media organizations, train stations, airports, and government agencies in Russia and Eastern Europe. Security researchers found strong evidence linking the attack to the creators of NotPetya, and noted that the malware used leaked NSA-linked exploits to move through networks. Ukrainian police later reported that the ransomware was a cover for a quiet phishing campaign undertaken by the same actor to gain remote access to financial and other confidential data.

October 2017. Yahoo updates the previous projections of 1 billion account affected in its massive 2013 breach, acknowledging that all 3 billion accounts were compromised.

October 2017. Russian hackers reported to be targeting potential attendees of CyCon, a cybersecurity conference organized by the US Army and the NATO CCD COE

October 2017. DHS and FBI reports warn of Russia-linked hackers targeting industrial control systems at US energy companies and other critical infrastructure organizations

October 2017. Poland's Defense Minister reports that the country repelled a third Russian hacking attempt against companies in Poland, reportedly part of a larger campaign against Eastern European corporations.

October 2017. North Korean hackers were found to have targeted US electric companies in a spear-phishing campaign meant to probe utilities' defenses.

October 2017. North Korean hackers allegedly broke into South Korea's defense data center in 2016 and stole a large trove of sensitive documents over the course of a year, including joint U.S.-South Korean blueprints for war on the peninsula.

October 2017. China allegedly carried out a cyberattack against a U.S. think tank and law firm, both involved with fugitive Chinese tycoon Guo Wengui.

October 2017. The Australian Government revealed that hackers compromised an Australian national security contractor in 2016 and stole large amounts of data, including information related to the development of the F-35 Joint Strike Fighter.

October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer

September 2017. Russia compromised the personal smartphones of NATO soldiers deployed to Poland and the Baltic states.

September 2017. Press reports say that the US Cyber Command targeted North Korea's the Reconnaissance General Bureau for denial of service attacks.

September 2017. China allegedly inserted malware into widely used PC management tool. The malware targeted at least 20 major international technology firms.

September 2017. The SEC reported that cybercriminals accessed the agency's files in 2016 and used the information gathered for illicit trading

September 2017. Credit monitoring firm Equifax disclosed a July data breach that revealed 143 million people's full names, social security numbers, birth dates, home addresses and driver's license numbers, as well as 209,000 credit card numbers.

September 2017. Researchers report malware infections in Cambodia designed to surveil dissidents and disrupt domestic political activity.

August 2017. Researchers inform the Estonian Information System Authority of a vulnerability potentially affecting the use of 750,000 Estonian e-ID cards. The government replaced the compromised cards in late 2017, but claims that no cards were ever hacked.

August 2017. South Korea's Cyber Warfare Research Center reports that North Korea has been targeting South Korean Bitcoin exchanges.

August 2017. A state-sponsored spyware campaign targeted Indian and Pakistani government security and military organizations.

August 2017. The Scottish Parliament suffered from a brute force cyberattack similar to the one that compromised the British Parliament in June.

July 2017. The Swedish Transport Agency's outsourced data is hacked, potentially compromising confidential information and classified information on military plans.

July 2017. Security researchers revealed details of a wide-ranging malware campaign linked to China which used over 600 strains of malware to conduct espionage operations on Southeast Asian military and government organizations

July 2017. GCHQ issued a warning saying that state-sponsored hackers had likely broken into the Industrial Control Systems of UK energy companies

July 2017. Security researchers revealed an Iran-linked cyber espionage group active since 2013 that had used spear phishing and watering hole attacks to target government institutions, defense companies, IT firms and more in Israel, Saudi Arabia, the US, Germany, Jordan, and Turkey.

July 2017. The FBI and DHS announced that hackers had been targeting US energy facilities including the Wolf Creek Nuclear Operating Corporation in a campaign bearing resemblance to the operations of a known Russian hacking group

July 2017. Cyber research firms reported a new malware campaign launched the day after North Korea's July missile tests. The identified family of malware featured a command and control infrastructure with links to South Korea, and had previously been used in three other campaigns linked to North Korea.

July 2017. Hackers attacked a partner of UniCredit, Italy's largest bank, gaining access to loan and biographical data from 400,000 client accounts

July 2017. Russian hackers used leaked NSA tools to compromise Wi-Fi servers in European and Middle Eastern hotels in a campaign targeting top diplomats and industrial leaders.

July 2017. The Qatari government accused hackers in the United Arab Emirates of posting fake news and attacking Qatari state-run media websites in a campaign designed to widen a rift between Gulf states.

June 2017. The New York Times revealed that spyware sold to the Mexican government was being used to target human rights lawyers, journalists, and anti-corruption activists

June 2017. US-CERT identified the North Korean government as being behind a DDoS botnet infrastructure used to target media, financial, aerospace, and critical infrastructure organizations worldwide

June 2017. A Russia-linked hacking group was found to have launched a spear-phishing campaign against Montenegro after the country announced its decision to join NATO

June 2017. A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days, causing an estimated $300 million in associated costs

June 2017. Russian hackers used an updated ransomware program to target Ukrainian infrastructure, including power companies, airports, and public transit.

June 2017. A brute-force attack alleged to have been carried out by Iranian state actors compromised nearly 90 British members of parliament, whose email accounts were hacked.

May 2017. A ransomware campaign spread to 99 countries using a vulnerability revealed in the Shadow Brokers' April 2017 dump of NSA tools.

May 2017. Lebanon accused Israel of hacking the Lebanese telecoms network and sending audio and WhatsApp messages to 10,000 people claiming that Hezbollah's leader was behind the death of the group's top commander.

May 2017. Thousands of emails and other documents from the campaign of French president-elect Emmanuel Macron, totaling 9 gigabytes, were released shortly before the election, in an effort linked to Russia.

April 2017. Irish state-owned utility EirGrid suffered a security breach at the hands of state-sponsored hackers involving a virtual wiretap allowing access to the company's unencrypted communications.

April 2017. The Lazarus Group, thought to be associated with North Korea, was found to be involved in a spear phishing campaign against US defense contractors

April 2017. Cybersecurity researchers revealed a growing cyber-espionage campaign originating in China and targeting construction, engineering, aerospace and telecom companies, as well as government agencies, in the U.S., Europe, and Japan.

April 2017. The Danish Defense Intelligence Service reported that a "foreign player," alleged by the Danish press to be Russia espionage group, had accessed Defense Ministry email accounts in 2015 and in 2016, but was unable to retrieve classified information.

April 2017. The Shadow Brokers, the group that claimed to have hacked the NSA in August 2016, released yet another trove of purported NSA hacking tools, including one that suggests the NSA had gained access to SWIFT messages.

April 2017. Chinese attempts to penetrate South Korean military, government and defense industry networks continued at an increasing rate since a February announcement that the THAAD missile defense system would be deployed in South Korea.

March 2017. An intelligence report revealed a Russian operation to send malicious spear-phishing messages to more than 10,000 Twitter users in the Department of Defense. The malicious payloads delivered through these messages gave Russian hackers access to the victim's device and Twitter account.

March 2017. The U.S. Department of Justice indicted two Russian intelligence agents and two criminal hackers over the September 2014 Yahoo hack, which compromised 500 million user accounts.

March 2017. Chinese police arrested 96 suspects charged with hacking into the servers of social media, gaming and video streaming sites, stealing personal information, and posting the information for sale on online forums.

March 2017. Wikileaks released a trove of sophisticated CIA hacking tools dated from 2013 to 2016, claiming that the release reflected several hundred million lines of CIA-developed code.

February 2017. A suspected Russian hacker breaches at least 60 universities and US government organizations using SQL injections, including HUD, NOAA, Cornell University, and NYU, among many others. This follows up a hack by the same actor against the U.S. Electoral Assistance Commission in December 2016.

February 2017. Indian Central Bureau of Investigation and Army officers were targeted by a phishing campaign purportedly mounted by Pakistan.

February 2017. Hackers compromised the Singaporean military's web access system and stole the personal information of 850 people. The Ministry of Defense said it was likely the attack was state sponsored.

February 2017. A sophisticated malware operation extracted over 600 gigabytes of data from 70 mostly Ukrainian targets in the fields of critical infrastructure, news media, and scientific research.

January 2017. A Swedish foreign policy institute accused Russia of conducting an information warfare campaign, using fake news, false documents, and disinformation intended to weaken public support for Swedish policies.

December 2016. A cyber attack targeted Ukraine's national power company, Ukrenergo, and shut down power to northern Kiev for over an hour.

December 2016. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) warned its customers that they remain vulnerable to attacks by "sophisticated" threat actors, having witnessed "a meaningful number" of attacks on its customers since the Bangladesh heist in February 2016, a fifth of which had resulted in stolen funds.

December 2016. Yahoo revealed that its systems had been intruded into in August 2013, and that the breach compromised one billion user accounts. Compromised data included usernames, email addresses, phone numbers, dates of birth, passwords, and security questions and answers. The data was posted for sale for $200,000 or best offer on underground forums.

November 2016. An indiscriminate attack compromised systems at the San Francisco Municipal Transportation Agency (the Muni), locking operators out of computers and customers out of kiosks. As a result, the Muni offered customers free rides for two days, until administrators restored its systems without paying the demanded $73,000 ransom.

November 2016. Hackers targeted AdultFriendFinder, a dating website, compromising 412 million users and publishing their emails, passwords, member status and purchases on online criminal marketplaces.

November 2016. The hard-drive-wiping "Shamoon" virus used against Saudi Aramco in 2012

was deployed against four Saudi Arabian government agencies. The attack wiped data on thousands of computers at Saudi's General Authority of Civil Aviation and other agencies.

October 2016. Hackers grained control of a major Brazilian bank's Domain Name System addresses and seized the bank's entire online footprint for several hours.

October 2016. The U.S. Director of National Intelligence and Department of Homeland Security jointly identified Russia as responsible for hacking the Democratic National Committee and using WikiLeaks to dump emails obtained in the hack.

September 2016. Japanese Defense Ministry and Self-Defense Forces (SDF) communications networks linking SDF bases and camps were compromised.

September 2016. Yahoo revealed that it an intrusion into its network in late 2014 had given hackers access to 500 million users' usernames, email addresses, phone numbers, dates of birth, passwords, and a mix of encrypted and plaintext security questions and answers. The company's CIO claimed the attack was perpetrated by a state-sponsored actor.

August 2016. A group calling itself "Shadow Brokers" claimed to have penetrated NSA and published a collection of NSA tools on Pastebin.

August 2016. Brazilian hackers ramped up phishing attacks against tourists visiting Rio de Janeiro for the 2016 Olympics. Security researchers ranked Brazil second only to Russia in the sophistication of its financial fraud gangs.

August 2016. A cybercriminal gang purportedly from Russia breached enterprise software company Oracle's systems, possibly to install malware on point-of-sale (POS) systems. The POS malware would then allow hackers to gain access to financial information in data breaches at major retailers.

August 2016. Two Hong Kong government agencies were penetrated in an attack allegedly by China. The attack came weeks before legislative elections in Hong Kong.

August 2016. Designs and data regarding India's Scorpene submarines were leaked from the French shipbuilder DCNS. DCNS also builds submarines for Malaysia and Chile, and recently won contracts to build submarines for Brazil and Australia.

July 2016. Forensic evidence points to Russian intelligence agencies as responsible for the release of 20,000 emails from the Democratic National Committee.

July 2016. A series of DDOS attacks disrupted 68 Philippine government websites on July 12, the day the United Nations International Arbitration court released its decision ruling in favor of the Philippines on the West Philippine Sea territorial dispute.

July 2016: A new strain of cyberespionage malware with a dropper designed to target specific European energy companies has been discovered. Researchers say the malware appears to be the

work of a nation-state, may have originated in Eastern Europe, and its role seems to be battlespace preparation.

July 2016: A Chinese cyber espionage group targeted defense industries in Russia, Belarus, and Mongolia with APTs using phishing campaigns to exfiltrate data.

May 2016: Suspected Russian hackers attempted to penetrate the Turkish Prime Minister's office and the German Christian Democratic Union party. The attacks targeted personal email accounts and attempted to obtain login credentials.

May 2016. Germany's domestic intelligence agency accused Russia of perpetrating a series of cyber attacks on the German Bundestag in 2015. The attackers made off with an undisclosed amount of data.

May 2016: Saudi Arabian communications and defense organizations were hacked, possibly by Iran.

April 2016. The German Christian Democratic Union, the political party of Angela Merkel, was targeted in a credential phishing attack by a Russian cyber espionage group.

April 2016. The Phillipine Commission on Elections' (COMELEC) database was breached, exposing the personal information of all 55 million registered Filipino voters, including fingerprint data, passport numbers and expiry dates, and intentions to run for office.

April 2016. Microsoft researchers discover a highly skilled hack group that has targeted government agencies (including intelligence agencies), defense research centers and telecommunication service providers in South and Southeast Asia since 2009.

April 2016. North Korean hackers stole warship blueprints from the database of a South Korean shipbuilder.

Mach 2016. A suspected ransomware attack crippled MedStar Health-operated hospitals in Maryland and Washington.

March 2016. North Korean hackers broke into the smartphones of a dozen South Korean officials, accessing phone conversations, text messages, and other sensitive information.

March 2016. 21st Century Oncology, a cancer care company, revealed that 2.2 million patients' personal information may have been stolen in an October 2015 hack. Hackers had access to patient names, Social Security numbers, doctor names, diagnosis and treatment information, and insurance information.

March 2016. Finland's foreign ministry discovered it had been the victim of a four-year breach in their computer network.

February 2016. The Internal Revenue Service (IRS) announced that a breach of its systems in May 2015 had compromised over 700,000 American taxpayers. The IRS suspected that a Russian

tax fraud operation is responsible for the breach.

February 2016. Hackers breached the U.S. Department of Justice's database, stealing and releasing the names, phone numbers, and email addresses or 30,000 DHS and FBI employees.

February 2016. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) warned its customers that they remain vulnerable to attacks by "sophisticated" threat actors, having witnessed "a meaningful number" of attacks on its customers since the Bangladesh heist in February 2016, a fifth of which had resulted in stolen funds.

January 2016. Austrian-based aerospace parts manufacturer FACC had $54.5 million stolen in a cyber attack. The attackers ignored FACC's intellectual property or proprietary data, and business operations were not affected.

January 2016. Israel revealed an operation by the United States and Britain to hack into Israel's surveillance drones.

January 2016. The chief of Sri Lanka's Financial Crimes Investigation Division had his private email account hacked. It is believed the attack was an attempt at embarrassment motivated by an ongoing crackdown by the department.

January 2016. Armenian diplomatic missions in 40 countries had their websites defaced by Azerbaijani hackers.

January 2016. The Czech Republic's Prime Minister had his twitter and personal email account hacked by right-wing extremists.

December 2015. Security researchers say that power outages in Western Ukraine on December 23, 2015 were the result of a coordinated on several regional distribution power companies. SCADA systems and system host networks were targeted and damaged. Malware was used to probe for network vulnerabilities, establish command and control, and wipe SCADA servers to delay restoration. Attackers simultaneously launched a denial of service attack on system dispatchers to prevent customers from reporting disruptions. Approximately 225,000 Ukrainians were affected, but service was restored after 3-6 hours.

December 2015. The Australian Bureau of Meteorology was attacked by hackers the previous year, with unnamed sources attributing the incident to China.

October 2015. The ROK National Intelligence Service attributed hacks at the National Assembly, the Ministry of Unification, and the Blue House to North Korea's General Reconnaissance Bureau.

October 2015. A teenage hacker tricked Verizon and AOL customer service to gain access to the private email account of CIA Director John Brennan.

November 2015. Iran's Revolutionary Guard hacked the email and social media accounts of a number of Obama administration officials in attacked believed to be related to the arrest of an Iranian-American businessman in Tehran.

November 2015. Spies were found to have attempted to hack into the German, French, and Japanese submarine builders bidding for a contract to build Australia's new submarine fleet.

September 2015. Hackers sought access to the Dutch Safety Board and other parties involved in investigating the crash of flight MH17.

September 2015. Multiple Pakistani government websites were hacked by the 'Mallu Cyber Team.

September 2015. Cybersecurity researchers uncovered a Russian hacking group called "The Dukes" that is allegedly responsible for attacks against foreign governments and think tanks in Europe, Central Asia, and the United States over seven years.

July 2015. The website of the Permanent Court of Arbitration in The Hague went offline in an incident that sources are connecting to hearings regarding China's claims to territory in the South China Sea. The breach was traced back to an IP address in China. The vulnerability spread malware to the devices of website visitors.

July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator.

July 2015. United Airlines revealed that its computer systems were hacked in May or early June, compromising manifest data that detailed the movements of millions of Americans. The report, citing "several people familiar with the probe," stated that the group behind this attack is the same group suspected of the Office of Personnel Management hack discovered in June.

July 2015. Hacking Team, an Italy-based firm accused of the unethical sale of surveillance technology worldwide, was hacked and hundreds of gigabytes of sensitive data were stolen. Confidential documents leaked by the hackers appeared to show Hacking Team's material support for authoritarian governments such as those in Sudan, Ethiopia, Morocco, and the United Arab Emirates.

June 2015. Canada announced that it has experienced DDOS attacks against two government websites. The attacks, which took down the Canadian Security Intelligence Service (CSIS) and the general Canadian government website, Canada.ca also reportedly affected email, Internet access and IT services in the government. Anonymous has claimed responsibility, citing Canada's recently passed Anti-terrorism Act, 2015 as the reason behind the recent attack.

June 2015. Japan Pension Service (JPS) was hacked resulting in the exfiltration of personal data belonging to 1.25 million people.

June 2015. The Office of Personnel Management was hacked twice in the last year. The first resulted in the loss of 4.1 million records and the second resulted in the loss of 21.5 million records,

19.7 million of these involved background investigation records for cleared U.S. government employees.

June 2015. German media reports that hackers breached the lower house of parliament on the Bundestag network and exfiltrated data from over 20,000 accounts. German weekly *Der Spiegel* said that the Kremlin is the primary suspect behind the attack and that the malware involved closely resembles that used in a 2014 attack on a German data network.

June 2015. The Chinese company Qihoo360 reports discovering "OceanLotus," an espionage program operating since 2012 to target marine agencies, research institutions and shipping companies.

June 2015. Media reports say that Stuxnet-like attacks were attempted against North Korea by the US, without success.

May 2015. Hong Kong-based undersea cable company Pacnet's business management systems were breached by a malicious software that accessed sensitive data stored on a SQL server.

May 2015. A hack of an online IRS system results in a $50 million loss, which the IRS blames on Russian hackers.

May 2015. The Yemen Cyber Army claims it breached a server belonging to the Saudi Ministry of Foreign Affairs. The hackers leaded the alleged login credentials of Saudi Officials, as well as usernames, phone numbers, and email addresses.

April 2015. The Pentagon revealed that Russian hackers gained access to an unclassified network within the DOD, though Pentagon officials were able to block the hackers' access within 24 hours.

April 2015. Hackers claiming affiliation to ISIS hacked French public television network TV5 Monde. The hackers took off the air 11 of the networks' channels and defaced TV5 Monde's website and social media accounts with pro-ISIS imagery.

April 2015. U.S. officials report that hackers gained access to White House networks and sensitive information, such as "real-time non-public details of the president's schedule," through the State Department's network, which has had continued trouble in ousting attackers.

March 2015. Canadian researchers say Chinese hackers attacked U.S. hosting site GitHub. GitHub said the attack involved "a wide combination of attack vectors" and used new techniques to involve unsuspecting web users in the flood of traffic to the site. According to the researchers, the attack targeted pages for two GitHub users – GreatFire (https://en.greatfire.org/) and the New York Times' Chinese mirror site – both of which circumvent China's firewall.

February 2015. Anthem, a U.S. health insurance company, is hacked, resulting in the theft of 80 million customers' personally identifiable information. The information was taken from an unencrypted database. This may have been part of a larger campaign that included the OPM hack.

February 2015. Media reports say that Canada's Communication Security Establishment identified "Babar" and "EvilBunny" as malware developed for espionage purposes by the French government. Babar's primary function is to exfiltrate documents, but it can also log keystrokes, monitor a user's web history, intercept and record communications made via Skype and messenger programs.

January 2015. A report issued by Germany's Federal Office for Information Security reveals a German steel mill became the second recorded victim of a cyberattack causing physical destruction. The attack disrupted control systems so severely that a blast furnace could not be properly shut down. The report did not name the steel mill or detail the severity of the damage.

December 2014. Iranian hackers attacked a major Las Vegas casino in retaliation for its owner's support for Israel.

November 2014. Sony Pictures Entertainment is hacked with the malware deleting data and the hackers posting online employees' personal information and unreleased films. An FBI investigation revealed North Korea to be behind the attack.

November 2014. North Korean hackers attacked a British production company planning to release a television series revolving around the imprisonment of a British nuclear scientist in the DPRK. The attack caused the cancellation of the series.

November 2014. A report by the University of Toronto finds that human rights organizations are routinely hacked by foreign intelligence services, using readily available crime ware as well as specially designed programs, with intrusion lasting for years.

October 2014. U.S. Postal Service servers are hacked, exposing employees' names, addresses, and Social Security numbers.

October 2014. The National Oceanic and Atmospheric Administration (NOAA) at the U.S. Department of Commerce is hacked, skewing the accuracy of some National Weather Service forecasts, according to NOAA.

October 2014. The Department of State reports breaches of its unclassified networks, and shut down its entire unclassified email system to repair possible damage. A month later, "suspicious cyber activity" was noticed on a White House computer network, but the White House said that no classified networks had been breached.

October 2014. Chinese users are redirected to a false iCloud login page that monitors their activities, putting their iCloud usernames, passwords, files, and contacts at risk.

October 2014. Ten percent of Dairy Queen outlets are hacked and customer credit card data compromised. Like the Target hack, hackers reportedly exploited a third party system to obtain access.

October 2014. A five-year cyber espionage campaign attributed to Russia exploits a zero-day

vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian government.

October 2014. Australian mining and natural resources companies and their associated legal and financial advisors attacked during sensitive business negotiations.

September 2014. A false Occupy Central smartphone app with audio recording capabilities, likely of Chinese origin, targets Hong Kong protestors and accesses users' locations, call and message logs, and browser histories.

September 2014. Using fraudulently obtained certificate, cyber criminals obtain access to 300 government and company websites in Germany, Austria and Switzerland in a multiyear operation.

September 2014. Home Depot reports a server breach affecting 56 million debits cards in the U.S. and Canada.

August 2014. The contractor responsible for security clearances at DHS has their networks hacked and employee personal information is compromised.

July 2014. Hackers in Eastern Europe breached energy sectors in the U.S., Spain, France, Italy, Germany, Turkey, and Poland in a major cyberespionage campaign.

July 2014. U.S. Office of Personnel Management networks that contain information on thousands of applicants for top secret clearances are breached.

July 2014. Canada's Foreign Minister asks his Chinese counterpart about PLA cyber espionage against the National Research Council, Canada' leading technology research agency.

May 2014. Alleged Chinese hackers posed as C-Suite executives in a spear phishing campaign to access the network of Alcoa. The hackers stole 2,907 emails and 863 attachments.
March 2014. Indian Army and DRDO computers (Defense Research and Development Organization) were hacked, and the Indian government warned that the spyware could read the files of computers not even connected to internet.

March 2014. The OPM contractor responsible for U.S. security clearance background investigations is breached, allegedly by Chinese hackers.

March 2014. Cybercriminals steal 40 million credit card numbers from Target, with an additional 70 million accounts compromised.

January 2014. Hackers targeted 28 embassies in Tehran using emails about the Syrian conflict that contained a new data-mining malware.

November 2013. Finland's Foreign Minister reports that hackers breached Finland's diplomatic communications for several.

October 2013. Federal prosecutors announce Vietnamese cyber criminals obtained as many as 200 million personal records, including Social Security numbers, credit card data, and bank account information.

October 2013. Press reports based on Snowden leaks reveal NSA hacked into German Chancellor Merkel's mobile phone, one of a larger series of leaks on NSA activities.

September 2013. The U.S. Navy says that Iran hacked into unclassified networks.

September 2013. North Korea again hacks South Korean targets, including think tanks, the South Korean Ministry of Defense, and Koreans defense industry firms.

August 2013. The Syrian Electronic Army hijacks and reroutes major Western social media and media sites to a malicious hosting site in Russia.

August 2013. A massive DDOS takes down China's .cn country code top level domain for several hours.

June 2013. The FBI charged five Ukrainian and Russian hackers with stealing over 160 million credit card numbers and causing hundreds of millions in losses.

June 2013. The U.S. and Russia sign a bilateral agreement that establishes a hotline and other confidence building measures.

June 2013. Edward Snowden, a former systems administrator at the NSA, reveals documents showing among other things that the US conducted cyber espionage against Chinese targets.

May 2013. An alleged Chinese hacker steals the blueprints for the Australian Security Intelligence Organization's new $631 million building.

May 2013. Israeli officials report a failed attempt by the Syrian Electronic Army to compromise water supply to the city of Haifa.

May 2013. DHS reports that the U.S. electrical grid is constantly being probed by multiple actors, including Iran.

May 2013. India is believed to have used a zero-day exploit to penetrate Pakistani mining, automotive, legal, engineering, food service, military, and banks.

May 2013. The Syrian Electronic Army claims to have breached the Saudi Arabian Ministry of Defense email system, and leaked several confidential emails.

May 2013. Over the course of the month, unknown hackers breached major automotive parts suppliers in North American and Europe.

May 2013. Anonymous' Saudi branch launches OpSaudi and takes down government web sites,

including the Ministry of Foreign Affairs, Ministry of Finance, and the General Intelligence Presidency via DDos attack.

May 2013. The U.S. identified a gang of eight hackers who extracted $45 million from banks in the UAE and Oman. The attacks eliminated the withdrawal limits on prepaid debit cards, permitting the hackers to withdraw massive amounts.

May 2013. An unknown attacker utilized a DDoS attack to bring down the website of the Iranian Basij military branch (basij.ir).

May 2013. Chinese hackers compromise the U.S. Department of Labor and at least nine other agencies, including the Agency for International Development and the Army Corps of Engineers' National Inventory of Dams.

April 2013. A Russian internet security firm announced that they discovered malware on millions of android mobile devices, primarily in Russia and Russian speaking countries.

March-June 2013. The Syrian Electronic Army, a pro-Assad hacktivist group, hacked into major Western media organizations as part of a propaganda campaign.

March 2013. The Indian Defence Research Organization was hacked, with thousands of documents uploaded to a server with an IP address in Guangdong, China.

March 2013. North Korea blames the United States and South Korea for a series of attacks that severely restricted Internet access in the country.

March 2013. South Korean television networks and banks were attacked with malware (designed to evade popular South Korean anti-virus software) thought to have originated in North Korea.

February 2013. DHS says that between December 2011 and June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. Forensic data suggests the probes originated in China.

February 2013. Der Spiegel reveals that EADS and German steelmaker ThyssenKrupp recorded major attacks by Chinese hackers in 2012.
January 2013. The New York Times, Wall Street Journal, Washington Post, and Bloomberg News experience persistent cyberattacks, presumed to originate in China.

January 2013. The Japanese Ministry of Foreign Affairs (MOFA discovers it has been hacked and has lost "at least" twenty documents, including highly classified documents.

January 2013. Iran's Izz ad-Din al-Qassam claims responsibility for another series of distributed denial-of-service attacks against US Bank websites, as part of Operation Ababil phase two.

December 2012. Al-Qaida websites are taken offline for two weeks.

December 2012. Two power plants in the U.S. were infected through unprotected USB drives.

October 2012. A Russian cybersecurity firm found a virus used against embassies, research firms, military installations, energy providers, and critical infrastructure in Eastern Europe, Russia, and Central Asia.

September 2012. Izz ad-Din al-Qassam, a hacker group linked to Iran, launched "Operation Ababil" targeting bank websites for sustained denial-of-service attacks. Targets include Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, and Regions Bank.

August 2012. A group called "Cutting Sword of Justice" linked to Iran claimed it has used the "Shamoon" virus to attack Aramco, a major Saudi oil supplier, deleting data on 30,000 computers and infecting (without causing damage) control systems. The attack also affected the Qatari company RasGas, a major LNG supplier.

August 2012. Malware nicknamed "Gauss," infected 2,500 systems worldwide. Gauss appears to have been aimed at Lebanese banks, and contains code whose encryption has not yet been broken.

July 2012. Regarded as the largest attack on Indian government networks, over 10,000 email addresses of top Indian government officials were hacked, including officials in the Prime Minister's Office, Defense, External Affairs, Home, and Finance ministries, as well as intelligence agencies. India blames the attack on state actors.

July 2012. NSA Director General Keith Alexander said that there had been a 17-fold increase in cyber incident at American infrastructure companies between 2009 and 2011.

July 2012. Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems.

July 2012. A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings.

June 2012. The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of state cyberattacks.

June 2012. A global fraud campaign using automated versions of SpyEye and Zeus Trojans targeted high-value personal and corporate accounts and bypassed two-factor authentication.

June 2012. A phishing campaign targets the U.S. aerospace industry experts attending the 2013 IEEE Aerospace Conference.

May 2012. Researchers at the University of Toronto report that versions of the installer for the

proxy tool Simurgh, which anonymizes net use and is popular in countries such as Iran and Syria to circumvent government internet controls, also installs a keylogger Trojan which sends the user name, keystrokes, and program use to another site.

May 2012. An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world.

May 2012. UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks.

April 2012. A hack of Japan's Ministry of Agriculture, Forestry, and Fisheries resulted in more than 3,000 documents exfiltrated to a foreign destination, including 20 classified documents on negotiations on the Trans-Pacific Partnership (a broad free-trade agreement). According to press reports, the hackers searched Ministry computers for TPP documents, transferred all that were found to a single computer, and then compressed them to make them easier to send.

April 2012. Iran was forced to disconnect key oil facilities after a cyberattack against internal computer systems. The malware was found inside the control systems of Kharg Island – Iran's main oil exporting terminal. Equipment at Kharg Island and at other Iranian oil plants was disconnected from the internet as a precaution. Iran reported that oil production was not affected, but the websites of the Iranian oil ministry and national oil company were forced offline and data about users of the sites was taken as a result of the attack.

March 2012. The U.S. Department of Homeland Security issued amber alerts warning of a cyber-intrusion campaign on U.S. gas pipelines, dating back to December 2011. Press reports indicated that Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) described the attack as a sophisticated spear phishing campaign emanating from a single source.

March 2012. India's Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government websites had been compromised from December 2011 to February 2012. Most of the incidents involved website defacement and many of the hacks appeared to originate in Pakistan.

March 2012. The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC's Director General blamed Iran for the incident.

March 2012. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

February 2012. Media reports say that Chinese hackers stole classified information about the technologies onboard F-35 Joint Strike Fighters.

December 2011. U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the People's Liberation Army. The Hackers had access to everything in Commerce's computers, including member company communications and industry positions on U.S. trade policy.

November 2011. Norway's National Security Agency (NSM) reports that at least 10 major Norwegian defense and energy companies were hacked. The attacks were specifically "tailored" for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords.

November 2011. According to a major U.S. news source, Chinese hackers interfered with two satellites belonging to NASA and USGS.

November 2011. Apple computers belonging to European Commission officials, including EC Vice President for the "Digital Agenda," were hacked at an Internet Governance Forum (IGF) meeting in Azerbaijan.

October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China.

September 2011. A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove.

September 2011. Australia's Defense Signals Directorate says that defense networks are attacked more than 30 times a day, with the number of attacks increasing by more than 350 percent by 2009.

September 2011. Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates are used to verify that a website is genuine. By issuing a false certificate, an attacker can pretend to be a secure website, intercept e-mail, or install malicious software. This was the second hack of a certificate authority in 2011.

August 2011. Email and documents from 480 members of the Japanese Diet and lawmakers and their staff were compromised for a month after a phishing attack implanted a Trojan on members' computers and Diet servers. The hijacked machines communicated with a server in China and the attackers included Chinese characters in their code.

August 2011. According to sources in the Japanese government, Mitsubishi Heavy Industries and twenty other Japanese defense and high tech firms were the target of an effort to extract classified defense information. Japanese officials believed the exploits all originated from the same source.

The intruder used email with a malicious attachment whose contents were the same as a legitimate message sent 10 hours earlier.

July 2011. South Korea said hackers from China had penetrated an internet portal and accessed phone numbers, e-mail addresses, names and other data for 35 million Koreans.

July 2011. The German Bundespolizei (Federal Police) and the Bundeszollverwaltung (Federal Customs Service) discovered that servers used to locate serious criminals and terrorism suspects by gathering information from GPS systems in cars and mobile phones were penetrated (using a phishing attack)as early as 2010. Following the cyberattack, the relevant servers had to be temporarily shut down to prevent further data losses.

July 2011. In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen.

June 2011. Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

June 2011. The IMF's networks were reportedly compromised by a foreign government using fraudulent emails with malware attachments, and a "large quantity of data, including documents and e-mails," are exfiltrated.

May 2011. Cybercriminals masquerading as members of the hacktivist group "Anonymous" penetrated the PlayStation network. Sony estimated that personal information for more than 80 million users was compromised and that the cost of the breach was over $170 million.

April 2011. Employees at Oak Ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the Lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007.

April 2011. Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

March-April 2011. Hackers used phishing techniques in attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

March-April 2011. Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

March 2011. Hackers penetrated French government computer networks in search of sensitive information on upcoming G-20 meetings.

March 2011. The European Commission and EU's External Action Service are both targeted in a widespread espionage effort just before a major EU summit. Hackers were apparently very interested in documents related to the G20 summit being held in Paris that year.

January 2011. The Canadian government reported a major cyberattack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.

January 2011. Hackers extracted $6.7 million from South Africa's Postbank over the New Year's Holiday.

January 2011. Hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and steal more than $7 million in credits, forcing the market to shut down temporarily.

December 2010. India's Central Bureau of Investigation (CBI) website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected.

December 2010. British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defense contractor and other "British interests" that evaded defenses by pretending to come from the White House.

October 2010. Australia's Defence Signals Directorate reported a huge increase in cyberattacks on the military. Australia's Defence Minister, john Faulkner, revealed there had been 2400 "electronic security incidents" on Defence networks in 2009 and 5551 incidents between January and August 2010.

October 2010. The Wall Street Journal reported that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over $12 million from five banks in the US and UK. Zeus uses links in emails to steal account information, which the hackers then use to transfer money into bank accounts they control. 100 "mules", or low end criminals, were arrested for opening bank accounts under false names into which the hackers transferred stolen money.

October 2010. Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

October 2010. Public facing networks run by NASDAQ, as well as an information sharing application called Directors Desk, are compromised by an unknown external group. NASDAQ says it is unsure how far hackers might have penetrated into their network.

July 2010. A Russian intelligence agent (allegedly named Alexey Karetnikov), was arrested and

deported after working for nine months as a software tester at Microsoft.

May 2010. A leaked memo form the Canadian Security and Intelligence Service (CSIS) says that "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually un-attributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

April 2010. A Chinese telecommunications firm accidently transmitted erroneous routing information for roughly 37,000 networks, causing internet traffic to be misrouted through China. The incident lasted 20 minutes and exposed traffic from more than 8,000 U.S. networks, 8,500 Chinese networks, 1,100 Australian networks and 230 French networks.

April 2010. Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems.

March 2010. Unknown hackers post the real incomes of Latvian government officials after accessing their tax records, creating political turmoil.

March 2010. Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China to gain inside information on the trial defense strategy.

March 2010. Google announced that it had found malware targeting Vietnamese computer users. Google said that the malware was not especially sophisticated and was used to spy on "potentially tens of thousands of users who downloaded Vietnamese keyboard language software" the malware also launched distributed denial of service attacks against blogs containing political dissent, specifically, opposition to bauxite mining efforts in Vietnam.

March 2010. NATO and the EU warned that the number of cyberattacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

January 2010. Intel disclosed that it experienced a cyberattack at about the same time that Google, Adobe, and others were attacked. The hackers exploited the vulnerabilities in Internet Explorer software that had been used in the other attacks as well. Intel said that there was no intellectual property or financial loss.

January 2010. A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December with a similar message.

January 2010. M. K. Narayanan, India's National Security Adviser, said his office and other government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to

penetrate Indian government computers.

January 2010. Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers in December 2009, according to leaked e-mails from a cyber-security company working for the bank.

January 2010. Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

January 2010. The UK's MI5 Security Service warned that undercover intelligence officers from the People's Liberation Army and the Ministry of Public Security have approached UK businessmen at trade fairs and exhibitions with the offer of "gifts" - cameras and memory sticks - which contain malware that provides the Chinese with remote access to users' computers.

December 2009. Downlinks from U.S military UAVs were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV had viewed.

December 2009. The Wall Street Journal reported that a major U.S. bank had been is hacked, losing tens of millions of dollars.

November 2009. Jean-Pascal van Ypersele, the vice-chairman of the United Nations' Intergovernmental Panel on Climate Change, ascribed the hacking and release of thousands of emails, from the University of East Anglia's Climatic Research Unit to Russia as part of a plot to undermine the Copenhagen climate talks.

August 2009. Ehud Tenenbaum was convicted of stealing $10 million from U.S. banks. Tenenbaum was known for hacking into DOD computers in 1998, which resulted in a sentence of six months of community service from an Israeli court.

August 2009. Albert Gonzalez was indicted on charges that between 2006 and 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. This was the largest hacking and identity theft crime in U.S. history.

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.

June 2009. German Interior Minister Wolfgang Schaeuble noted, when presenting the Interior Ministry's 2008 security report, that China and Russia were increasing espionage efforts and Internet attacks on German companies.

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.

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.

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.

April 2009. Chinese hackers reportedly infiltrated South Korea's Finance Ministry via a virus attached to e-mails claiming to be from trusted individuals.

April 2009. Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National Peoples Congress.

April 2009. Wall Street Journal articles laid out the increasing vulnerability of the U.S. power grid to cyberattack also highlighted was the intrusions into F-35 databases by unknown foreign intruders.

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.
March 2009. Canadian researchers found a computer espionage system that they believe China implanted on the government networks of 103 countries.

March 2009. The German government warned that hackers were offering a free version of the new Microsoft operating system that installs Trojans.

February 2009. French naval aircraft planes were grounded after military databases were infected with the "confickr" virus. Naval officials suspected someone in the Navy had used an infected USB key.

February 2009. 600 computers at India's Ministry of External Affairs were hacked.

February 2009. FAA computer systems were hacked. Increased use by FAA of IP-bases' networks also increases the risk of the intentional disruption of commercial air traffic.

January 2009. Indian Home Ministry officials warned that Pakistani hackers had placed malware on popular music download sites used by Indians in preparation for cyberattacks.

January 2009. Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.

2008. Britain's MPs were warned about e-mails apparently sent bythe European Parliament amid fears that they could be used by Chinese hackers to implant viruses.

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.

December 2008. Retail giant TJX was hacked. The one hacker captured and convicted (Maksym Yastremskiy) is said to have made $11 million from the hack.

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 re-secure the networks.

November 2008. Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million dollars from machines in 49 cities.

October 2008. Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

August 2008. Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions.

Summer 2008. Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data detailing the quantity, value, and location of oil discoveries around the world. One company put the losses in the millions.

Summer 2008. The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

June 2008. The networks of several Congressional offices were hacked by unknown foreign intruders. Some infiltrations involved offices with an interest in human rights in Tibet.

May 2008. The Times of India reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict.

May 2008. Belgium's Justice Minister China of hacking Belgian governmental computer networks.

April 2008. Germany's BND is accused of hacking Afghanistan's Commerce Minister and Ministry of Commerce and Industry networks, gaining access to internal email accounts and exfiltrating documents.

April – October 2008. A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department.

March 2008. U.S. officials reported that American, European, and Japanese companies were experiencing significant losses of intellectual property and business information to criminal and industrial espionage in cyberspace. However, details cannot be provided in an unclassified setting.

March 2008. South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.

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.

November 2007. Jonathan Evans, the head of Britain's Security Service (MI5), warned 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."

October 2007. More than a thousand staffers at Oak Ridge National Labs received an email with an attachment that, when opened, provides unknown outsiders with access to the Lab's databases.

October 2007. China's Ministry of State Security said that foreign hackers, 42% from Taiwan and 25% from United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

September 2007. British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments.

September 2007. Contractors employed by DHS and DOD had their networks hacked as backdoors into agency systems.

September 2007. Francis Delon, Secretary-General of National Defence in France, stated that information systems in France had been infiltrated by groups from China.

September 2007. Israel disrupted Syrian air defense networks (with some collateral damage to its

own domestic networks) during the bombing of an alleged Syrian nuclear facility.

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.

June 2007. The Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit DOD networks.

May 2007. Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well; however, they created a wave of fear in cyber dependent countries like the U.S.

May 2007. The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.
April 2007. The Department of Commerce had to take the Bureau of Industrial Security's networks offline for several months because its networks were hacked by unknown foreign intruders. This Commerce Bureau reviews confidential information on high tech exports.

2006. Chinese hackers were thought to be responsible for shutting down the House of Commons computer system.

December 2006. NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.

November 2006. Hackers attempted to penetrate U.S. Naval War College networks, resulting in a two week shutdown at one institution while infected machines are restored.

August 2006. A senior Air Force Officer stated publicly that, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (the unclassified military network)."

May 2006. The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies had 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 constitute an act of war. But when it happens in cyberspace, we barely notice.