

State-sponsored cyber-attacks

2010, Stuxnet

Developed by U.S. **National Security Agency's (NSA)** hacking group, **Tailored Access Operations** and Israel's **Unit 8200** cyber agency. Stuxnet sabotages Iran's uranium enrichment programme. Worm spreads through network, taking over Windows-based software which controls high-speed centrifuges



Centrifuges spin themselves to destruction

2014, Sony hack

Hack by North Korea's **Lazarus Squad** attempts to force **Sony Pictures** to abandon release of **"The Interview"** – comedy about **Kim Jong-un**



Hackers destroy company's internal network and leak studio data

2015, Ukraine power grid attack

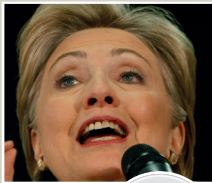
Unit of GRU – Russian military intelligence agency – known as **Sandworm Team** takes down Ukraine's electricity grid at height of winter



BlackEnergy malware attack is first successful assault on any power-grid control network

2016, U.S. DNC hacks

Russian cyber-espionage groups, **APT28** and **APT29** – collectively known as **Fancy Bear** – hack emails and documents from **Hillary Clinton's** presidential campaign and **Democratic National Committee**



GRU funnels more than 19,000 emails and documents to WikiLeaks to influence presidential election

2019, European Parliament elections

Russian APT28 and Sandworm try to influence vote in 27 member states for members of **European Parliament** by hacking into institutions and spreading fake news to damage candidates



Hackers target elections in Belgium, Denmark, Greece, Finland, Poland, Portugal and Spain

2010

2011

2012

2013

2014

2015

2016

2017

2018

2019

2020

2012, Flame

Toolkit created by **Equation Group** – part of NSA spy agency



Malware records screenshots, keyboard strokes, audio conversations and data from nearby Bluetooth devices

Flame relays what it learns back to controllers

Flame is deployed against Iran, Israel, and other Middle Eastern countries

2015, U.S. OPM hack

Chinese spear-phishing emails install backdoors onto servers of **Anthem Health Insurance** and **U.S. Office of Personnel Management**



Hackers steal 78.8 million medical records and 21.5 million records of government workers, including employees with top-secret security clearances

2016: Hong Kong hacks

Chinese government cyber-espionage group – known as **Buckeye** or **APT3 (Advanced Persistent Threat)** – uses U.S. weapons stolen from NSA's Equation Group. Buckeye uses NSA's **Bemstour** tool, which installs **DoublePulsar** backdoor, to exploit **Microsoft Windows** vulnerabilities



China attacks Hong Kong government agencies ahead of legislative elections

2017, NSA cyberweapon leaks

Suspected member of NSA's **Directorate of Operations** passes Equation Group's latest tools to **Shadow Brokers**. Shadow Brokers pass tools to North Korea and Russia



One tool, **EternalBlue**, which exploits flaw in Windows, is used for ransomware attacks. **WannaCry** is developed by North Korea to extort ransom payments in more than 150 countries, Sandworm uses **NotPetya** and **Bad Rabbit** to attack Ukrainian businesses

2020, Supply chain attack

Hackers inject malware into **SolarWinds Orion** network management platform. Between March and June, Orion software updates are infected with **Sunburst** malware



Victims include some 18,000 government and business organisations worldwide