cyberattacks_comparison_fact_sheet

Incident	Targets	Description	Consequences
2007 - Estonia DDoS Attacks	Government, banks, media (Estonia)	Massive DDoS attacks disrupted Estonia's digital infrastructure amid political tensions with Russia.	Paralyzed online services; led to NATO establishing its Cyber Defence Centre.
2008 - Georgia Cyberattacks	Government websites, media (Georgia)	Cyberattacks coincided with Russia's military invasion, defacing websites and spreading propaganda.	Disrupted government communications; first case of cyberwarfare alongside conventional military action.
2016 - DNC Hack	Democratic National Committee (USA)	Russian hackers stole and leaked internal emails, influencing public opinion during the U.S. election.	Sparked political turmoil; led to U.S. sanctions and indictments against Russian intelligence officers.
2017 - NotPetya Malware	Multinational corporations, infrastructure (global)	Russian military hackers deployed destructive malware that spread worldwide, causing billions in damage.	Estimated $10 billion in losses; major corporations and governments forced to overhaul cybersecurity measures.
2020 - SolarWinds Attack	U.S. federal agencies, Fortune 500 companies	Russian SVR hackers inserted a backdoor into SolarWinds Orion software, compromising thousands of networks.	One of the largest cyber espionage operations; led to major cybersecurity reforms in the U.S. government.
2021 - Colonial Pipeline Ransomware	Critical U.S. energy infrastructure	Russian-linked cybercriminals shut down a major U.S. fuel pipeline with ransomware, demanding payment.	Led to fuel shortages across multiple states; spurred federal policies to combat ransomware threats.