CYBER WAR AND ESPIONAGE

"**Sony has agreed to pay up to $8m over employees' personal data lost in the 2014 hacking scandal surrounding the release of The Interview.**" BBC, 21 October 2015.

Hackers associated with the government of North Korea were found responsible for a cyber-attack on Sony Pictures after Sony released the film The Interview, which portrayed the North Korean leader Kim Jong Un in a negative light. This hack was conducted using malware and a Server Message Block worm tool. U.S. investigators believe the perpetrators of this economic espionage took two months to copy critical files and targeted Sony as a trial-run for future political cyber espionage.

Hackers broke into the company's computers and released thousands of items of personal information. The cyber-attack wiped out massive amounts of data and led to the online distribution of emails, personal and sensitive employee data as well as pirated copies of new movies. The lawsuit against Sony was filed by former employees claiming the company's negligence caused them economic harm by forcing them to step up credit monitoring to address their increased risk of identity theft. They described the data breach as an "epic nightmare."

Same Team was found Responsible for Global WannaCry 2.0 Ransomware, Central Bank Cybertheft in Bangladesh, and Other Malicious Activities.

"**Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks**" by Donghui Park, Michael Walstrom, The Henry M. Jackson School of International Studies, University of Washington, October 11, 2017.

The Ukrainian electricity grid was hacked in December 2015 and December 2016. The attacks were attributed to Russian hackers believed to have had links to the Russian government. While military action is visible and open to scrutiny from the international community, cyber-activity is considerably harder to track and attribute to a source.

These attacks were aimed at destabilizing Ukraine as it leaned towards NATO and the EU and proving the capabilities of Russian hackers. The group behind the attacks is known as the Sandworm Team, and they used malware, including the BlackEnergy3 Trojan, to gain access to the Ukrainian grid's SCADA system.

Sandworm Team's first hacking campaign began as early as May 2014 with phishing. In this case, BlackEnergy3 was likely installed on utility company systems six months before hackers caused the blackouts on December 23, 2015. Phishing emails with infected attachments were sent to the companies' offices. When the attachments were opened, macros enabled hackers to gain remote access. After they gained access, they began harvesting credentials for the virtual private networks (VPN) used by grid operators to access the control centers remotely. Using the VPNs, they explored control center networks and connected devices. Staying inside the system for 6 months, they learned about all the internal operations before finally carrying out the attack.

“**Russia and Ukraine in cyber 'stand-off'**” BBC, 5 March 2014.

The conflict between Ukraine and Russia in 2014 spilled over into cyberspace, with Ukrainian authorities accusing the Russian army of disrupting mobile communications. Security forces in Ukraine accused the Russian army of disrupting mobile communications. Cyber-attacks were utilised heavily before as well during Russia's 2008 conflict with Georgia. In that case, distributed denial of service attacks - known as DDoS - were used to overwhelm websites and servers in Georgia in the weeks leading up to the military action. In 2014, Ukrainian authorities confirmed that communication networks had been targeted, the first significant disruption of technology. The attacks coincided with a disagreement between Estonia and Russia over the relocation of a Soviet war memorial. While military action is visible and open to scrutiny from the international community, cyber-activity is considerably harder to track and attribute to a source.

“**What we know – and still don’t – about the worst-ever US government cyber-attack**” by Kari Paul and Lois Beckett in The Guardian, 19 Dec 2020.

In 2020, U.S. organizations and government agencies were the targets of a nation-state attack. Key federal agencies, from the Department of Homeland Security to the agency that oversees America’s nuclear weapons arsenal, were targeted, as well as powerful tech and security companies including Microsoft. At least six US government departments, including energy, commerce, treasury and state, were breached. The National Nuclear Security Administration’s networks were also breached.

Security researchers discovered a backdoor in a popular IT management product from SolarWinds. FireEye, one of SolarWinds' 300,000 customers, disclosed that the nation-state attack it suffered was the result of a massive supply chain attack on SolarWinds. Attackers gained access to victims through infected updates to SolarWind's Orion IT monitoring and management software. Up to 18,000 SolarWinds customers were vulnerable, including various U.S. government agencies. Multiple media outlets reported APT29, a Russian state-sponsored hacking group also known as Cozy Bear, was behind the SolarWinds attack.

“**We are not ready’: a cyber expert on US vulnerability to a Russian attack**” by Kari Paul in The Guardian, Mar 2022.

Cyber warfare between Russia and Ukraine is feared by the US, which is not well prepared for a significant cyber-attack, according to Glenn S Gerstell, a senior adviser at the Center for Strategic and International Studies and the former general counsel of the National Security Agency. He said the US has an extraordinary offensive capability, but the private sector is not prepared for attacks. Gerstell called for a mandatory solution as cyber threats grow faster than the ability to adapt to them. He added that if Russia attacks the US, the latter may respond with a stealth or open cyber-attack or military action.

“**Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack**” The Guardian May 2021.

Colonial Pipeline, operator of the largest fuel pipeline in the US, has confirmed that it paid a ransom of $4.4m to hackers who breached its computer systems in a ransomware attack on 7 May. The company’s CEO, Joseph Blount, told the Wall Street Journal that the decision to pay was taken in order to restart the pipeline quickly and safely, with the attack having taken the system offline. Colonial Pipeline restarted its pipeline a week ago, but shortages have persisted in some areas.

The cyberattack on the Colonial Pipeline, which is a major fuel pipeline in the United States, was not a traditional cyber war, but it did have significant consequences on the energy sector and the economy. In May 2021, a ransomware attack was launched against Colonial Pipeline by a cybercriminal group called DarkSide. The attack disrupted the pipeline's operations for several days, leading to a fuel shortage across the Eastern United States. The attack was not an act of war, but rather a criminal act aimed at extorting money from the pipeline operator. However, the consequences of the attack were significant and showed the vulnerability of critical infrastructure to cyber threats. The attack led to fuel shortages across 13 states, panic-buying and lengthy queues at gas stations. The attack also highlighted the need for increased cybersecurity measures to protect critical infrastructure from similar attacks in the future.

AFP. (2022, October 10). “**US Airport Websites Hit by Suspected Pro-Russian Cyberattacks**.” Retrieved October 11, 2022, from securityweek.com: https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks

Several major US airports, including those in Atlanta, Chicago, Los Angeles, New York, Phoenix, and St Louis, were hit by distributed denial of service (DDoS) attacks after a pro-Russian hacking group called KillNet published a list of sites and encouraged its followers to attack them. However, the DDoS attacks only affected the public-facing websites of the airports and did not impact operations. KillNet made public declaration of war against enemies of Russia and Ukrainian supporters alike, targeted the US airports as a retaliation for US involvement in the Russian invasion of Ukraine. The group is responsible for attacks against other government and financial institutions in recent weeks as well, such as JP Morgan-Chase, and dozens of US Department of Defense websites such as TRICARE, army.mil, DS Logon, and several state government websites as well. Damages caused have been minimal, but the takeaway from these attacks is that both Russian and Ukraine have non-sanctioned cyber-war combatants that are willing and able to act on behalf of their loyalties and increasing the size of the battlegrounds to a world-wide network.

“**Russian-speaking hackers knock US state government websites offline**” By Sean Lyngaas, CNN, October 5, 2022.

Russian-speaking hackers known as Killnet have claimed responsibility for knocking offline state government websites in Colorado, Kentucky and Mississippi, among other states. The websites affected were those of government agencies and the Kentucky Board of Elections, which provides information on voter registration. Although the campaign does not appear to specifically target US elections infrastructure, it represents a type of digital disruption that US officials and election officials were preparing for ahead of the November 2022 midterm elections. In February, Killnet stepped up their activity after Russia’s invasion of Ukraine to target organizations in NATO countries. They are a loose band of politically motivated hackers who support the Kremlin, although their ties to that government are unknown. Multiple states have confirmed intermittent connection issues to their websites following suspected cyberattacks, according to the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), a non-profit-backed threat-sharing center.

While none of the Killnet attacks have long lasting effects, it does show a trend that, in addition to state-sponsored threat actors such as Fancy Bear and Sandworm, Russia has a vast following of unsanctioned hackers that are growing increasingly more organized, and which continue to carry out attacks against any targets that these fringe groups perceive to be enemies. This trend—which manifest on both sides of the Russia-Ukraine conflict and includes groups that act in favor of Ukraine or Russia like KillNet shows that cyberwarfare is escalating to a world-wide stage and involves any volunteers that have access to the internet.