The Sony Hack and the Use of Cyber Coercion

Tracing the Lazarus Group and North Korea's Rise as a Cyber Power

Santiago López de Toledo Soler

1. Executive summary

In November 2014, Sony Pictures Entertainment became the victim of one of the largest cyberattacks in history against a private entity. The attackers, identifying themselves as the *Guardians of Peace*, infiltrated Sony's network, exfiltrating massive volumes of confidential data before deploying a wiper malware that rendered thousands of workstations inoperable (Wakefield, 2014). The leaked information included personal data, executive emails, salary records of high-profile celebrities, and confidential film projects. The volume of exfiltrated data was estimated at approximately 100 terabytes (Zetter, 2014). Shortly after, the attackers wiped the affected systems, crippling large portions of Sony's global network. The attack caught the attention of the whole world, covered by every major international news channel even before authorities knew who the perpetrators were.

Later that year, the Federal Bureau of Investigation formally linked the attack and the *Guardians of Peace* (GOP) to a state-sponsored hacker group known as the Lazarus Group, operating under North Korea's Reconnaissance General Bureau (FBI, 2014). The operation was motivated by the upcoming release of *The Interview*, a comedy starring Seth Rogen and James Franco that depicted an assassination plot against DPRK leader Kim Jong-un. For the first time in history, the U.S. government condemned a state actor for a cyberattack on a private enterprise, breaking new ground and transforming the paradigm of cybercrime and cyber law, while exposing the intersection between espionage, terrorism, information warfare, and cyber sabotage (U.S. Department of Justice, 2018).

2. Consequences, impact and significance

Before explaining the consequences of the attack and its impact on both Sony and the U.S. government, and in order to contextualize the measures later taken by the company and regulators to prevent similar incidents, it is important to understand the chain of events that defined the attack.

According to Jeffrey Roman's *Sony Pictures Cyber-Attack Timeline* (2014), the North Korean Foreign Ministry had already described the upcoming release of *The Interview* as an act of

"undisguised terrorism" as early as June 24, 2014. Some Sony executives had also expressed concern regarding the potential risks to public safety if the film were to be released. GOP are believed to have infiltrated Sony's network months earlier, but on November 24, 2014, many of Sony's computers were compromised, and their Master Boot Records were erased using a wiper malware known as *Destover* (Roman, 2014). Beyond the enormous amount of data leaked and the destruction of a significant portion of the company's network, the most alarming phase of the attack came on December 16, when GOP released another data dump containing Michael Lynton's Outlook mailbox (Sony's CEO at the time) along with a terrorist message that warned: *"The world will be full of fear… remember the 11th of September of 2001. We recommend you to stay distant from the places at that time"* (Perlroth & Sanger, 2014). Worried they could be the target of a terrorist attack, many major theaters refused to show the movie, but over 300 independent cinemas started screening it December 25th, a day after it was released by Sony for digital download following a Department of Homeland Security report that declared that "there was not a credible terrorist active plot" (Roman, 2014).

In the midst of the chaos, Sony faced several class-action lawsuits from employees for failing to adequately protect private information, ultimately settling for up to $8 million (Canadian Underwriter, 2015) in addition to spending over $35 million in system restoration and remediation costs (Hornyak, 2015). One of the most significant post-attack actions was hiring external cybersecurity experts, including security firm Mandiant, to conduct a forensic investigation, identify vulnerabilities, and remove potential backdoors from the network. However, Mandiant later published an internal memo stating that Sony "could not have prepared for such an unprecedented attack" (Frizell, 2014).

In response, Sony implemented stronger internal cybersecurity policies, introducing company-wide awareness workshops and training on password hygiene and anti-phishing practices. The company redesigned its network architecture to include stricter segmentation, reducing the "blast radius" of potential future attacks. This restructuring limited the number of users with privileged access to sensitive data, mitigating the risk of horizontal escalation and credential theft (School of International and Public Affairs, Columbia University, 2022).

Private sector firms such as Trend Micro and Kaspersky lab linked the malware used, *Destover*, to previous attacks carried out in Saudi Arabia and South Korea, due to commonalities within its code that had been linked to the already notorious Lazarus Group. This hinted the FBI to thoroughly investigate North Korea as the prime suspect of the attack, followed by unsurprising furious statements from the DRPK's Foreign Ministry denying all involvement (Roman, 2014). The FBI asked several allies such as the United Kingdom and Japan to spearhead an international response against the North Korean government, while Pyongyang's sole major ally, China, only dared to say it saw "no clear evidence" tying North Korea to the attack, while condemning "all forms of cyberattacks and cyberterrorism".

This geopolitical finger-pointing concluded with the first ever public condemnation of a state-actor for a cyberattack on December 19th, 2014. The FBI published an *Update on Sony Investigation* (2014), claiming that the Bureau had "enough information" to conclude that the North Korean government was behind the attack (FBI, 2014). Years later, in 2018, the DOJ and the FBI would issue an arrest warrant for only one identified individual confirmed to be part of Lazarus Group (alleged matrix of GOP), a male North Korean national, also linked to 2017 WannaCry ransomware attack, believed to be born between 1981 and 1984, by the name of Park Jin Hyok (U.S. Department of Justice, 2018).

The public sector did not remain indifferent to the new cyber threats posed by foreign actors, even if they were targeted at private enterprises. The year following Lazarus Group's attack, cybersecurity concerns reached The White House. Some private sector firms' – like Sony – lobbied in order to get government funding to strengthen their network, pressure to which the Obama administration responded, holding several seminars on national cybersecurity, showing Sony's case as a living example of the catastrophic consequences of cyberattacks, especially to poorly protected networks (The White House, 2015).

Although the administration strongly advocated for new cybersecurity legislation, Congress, the Senate, and segments of the American public were not easily persuaded. Obama's proposal sought to give private companies a simplified and legally safe mechanism to share information

about cyber threats with the government, particularly with the Department of Homeland Security, which operates a 24/7 cyber monitoring center. Under the plan, firms would receive liability protection, meaning they could not be sued for sharing technical information (such as IP addresses, routing data, or timestamps) if it served to prevent or mitigate cyberattacks (Lyngaas, 2015). Unsurprisingly, privacy advocates raised concerns that granting the government expanded access to sensitive data could undermine citizens' privacy rights, reigniting the enduring debate between security and privacy. Nevertheless, the proposal – officially known as the Cybersecurity Information Sharing Act (CISA) – was approved and signed into law in late 2015 (Lyngaas, 2015).

3. Analysis and key points.

Even after enhancing cybersecurity measures and the enactment of CISA, the following years after the Sony attack would be prolific for criminal, and in some cases state-sponsored, hacker groups around the world. North Korean hacking campaigns quickly pivoted toward financially motivated cybercrime. The Lazarus Group was behind several major attacks, including the Bangladeshi Bank hack in 2016 and the WannaCry ransomware in 2017, both aimed at stealing money to fund their impoverished regime.

It is clear that both the private sector and the public sector have gotten better at following clues to attribute certain attacks to certain groups (even if it is after-the-fact) but after years of thorough investigation, authorities have only been able to pinpoint one individual, of which they do not even know his age or his whereabouts, *alleged* to be a part of Lazarus Group (FBI, 2014). This underlines a fundamental challenge in cyberspace: attribution. Getting a name and an address of a cybercriminal, especially a skilled one, has proven to be nearly impossible. Park is likely just one small piece inside Lazarus Group's broader infrastructure, and authorities still seem far from identifying other members (National Security Archive, 2017).

Back in 2010, *Stuxnet* was the first example of malware used as a weapon in a covert intelligence operation carried out by the United States and Israel against the Iranian nuclear development program (Greenberg, 2019). The Sony attack, however set a new precedent by revealing the geopolitical dimension in terms of cyberspace. For the first time, the world witnessed

how malware had been successfully used to send a political-ideological message from one state to another. This new use for cyber technical skills caught the attention of the most powerful governments in the world, who now see cyber operations as a cornerstone of geopolitical statecraft, a tool to undermine foreign regimes and gain leverage in the international stage, all done from the other side of a computer screen (Greenberg, 2019). This has changed the international power paradigm, where states with the most natural resources and strongest military forces had always held the upper hand in any type of conflict; economic, armed, or territorial. The rise of cyber operations as a strategic geopolitical asset now allows more resource-poor states, such as North Korea, to inflict millions of dollars in damage on their adversaries.

On a more domestic level, the attack on Sony should serve as a constant reminder to both private and public sector organizations that cybersecurity must be a top budgetary priority. Private giants such as Sony, Microsoft, or Meta should not have to rely on government funding to maintain robust, secure networks that protect both their clients' data and their own operations. Smaller tech startups, on the other hand, given their limited financial resources, should be the main focus of public-sector cybersecurity funding initiatives, as they represent highly attractive targets for cybercriminals seeking to exploit vulnerable, emerging systems (Todd & Rahman, 2013).

According to the Columbia University case study on the Sony hack (2022), a key factor to consider is the interdependence between technical infrastructure and corporate governance. The report emphasizes that Sony's vulnerabilities were not merely technical but also organizational – rooted in poor internal communication, fragmented IT management, and an overreliance on third-party contractors. Cybersecurity must be embedded as a core element of corporate governance rather than treated as a separate technical function. Even if the tools used, such as *Destover*, were state-of-the-art malware, as Frizell (2014) suggests, the organizational and corporate dimensions of cybersecurity cannot be underestimated by the private sector.

The Sony Pictures Entertainment attack establishes a pivotal moment in the evolution of cyber conflict. What began as an act of retaliation for ideological reasons against *The Interview* reshaped how states approach cyber in the modern age. It demonstrated that influence and sociopolitical disruption of a foreign state is no longer only achievable through traditional espionage, trade war

or military power, but it can also be achieved through code. More than a decade later, the consequences and impact of the attack keep defining the intersection between international law, power and cybersecurity.

4. References

BBC News. (2014). *What is FBI evidence against North Korea?* BBC. https://www.bbc.com/news/technology-30554444

Canadian Underwriter. (2015). *Sony settles employees' hacking lawsuit, to pay up to $8 million for loss, identity protection. Canadian Underwriter.* https://www.canadianunderwriter.ca/news/claims/sony-settles-employees-hacking-lawsuit-to-pay-up-to-8-million-for-loss-identity-protection/

Elkind, P. (2015). *Sony Pictures: Inside the hack of the century, part 2. Fortune.* https://fortune.com/longform/sony-hack-part-two/

Federal Bureau of Investigation. (2014). *Update on Sony investigation.* FBI. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Frizell, S. (2014). *Internal memo: Sony could not have prepared for 'unprecedented' hack. Time.* https://time.com/3623456/sony-hack-unprecedented/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.*

Hornyak, T. (2015). *2014 cyberattack to cost Sony $35M in IT repairs. Computerworld .* https://www.computerworld.com/article/1629515/2014-cyberattack-to-cost-sony-35m-in-it-repairs.html

Lyngaas, S. (2015). *The Obama administration is hoping enhanced privacy provisions can make a long-stalled proposal more palatable to the Senate. FCW.*

National Security Archive. (2017). *Lazarus under the hood.* National Security Archive & Kaspersky Lab. https://nsarchive.gwu.edu/sites/default/files/documents/3673007/Document-07-Kaspersky-Lab-Lazarus-Under-the-Hood.pdf

Roman, J. (2014). *Sony Pictures cyber-attack timeline: Infographic provides overview of events surrounding breach. BankInfoSecurity.* https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710

School of International and Public Affairs, Columbia University. (2022). *The hacking of Sony Pictures: A case study.* Columbia University. https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

The White House. (2015). *Remarks by the President at the National Cybersecurity Communications Integration Center.* Obama White House Archives.

Todd, M. S., & Rahman, S. M. (2013). Complete network security protection for SMEs within limited resources. *International Journal of Network Security & Its Applications (IJNSA).*

U.S. Department of Justice. (2018). *North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions.* U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Wakefield, J. (2014). *Whodunnit? The mystery of the Sony Pictures hack.* BBC.

Zetter, K. (2014). *Sony got hacked hard: What we know and don't know so far.* Wired.