Cyber Law

MSGSCC, Fall 2025

Santiago López de Toledo Soler

The 2014 Sony Pictures Entertainment breach

A legal analysis of the Lazarus Group cyber operation

1. Background and context of the attack

In November 2014, Sony Pictures Entertainment was hit by one of the most significant cyberattacks ever carried out against a private company. The group calling itself the Guardians of Peace (GOP) breached Sony's network, exfiltrating enormous amounts of confidential data before deploying wiper malware that disabled thousands of workstations (Wakefield, 2014). The leaked materials included personal information, executive email correspondence, salary details of major celebrities, and sensitive film content. Estimates put the volume of stolen data at around 100 terabytes (Zetter, 2014). Soon after the exfiltration, the attackers wiped Sony's systems, effectively shutting down large parts of the company's global operations. The incident drew immediate worldwide attention, dominating major news outlets even before investigators had identified who was responsible.

Later that year, the Federal Bureau of Investigation (FBI) formally attributed the attack, and the Guardians of Peace, to the Lazarus Group, a state-sponsored hacking unit operating under North Korea's Reconnaissance General Bureau (FBI, 2014). According to U.S. authorities, the operation was driven by the planned release of *The Interview*, a comedy starring Seth Rogen and James Franco that portrays an assassination attempt on DPRK leader Kim Jong-un. It marked the first time the U.S. government publicly condemned a foreign state for conducting a cyberattack against a private corporation, setting a major precedent and reshaping discussions around cybercrime and cyber law. The case exposed how espionage, coercion, information warfare, and destructive cyber operations can converge in a single incident (U.S. Department of Justice, 2018).

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 "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 25, 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).

Private sector firms such as Trend Micro and Kaspersky 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 DPRK'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".

The investigation ended with the public condemnation of a state actor for a cyberattack on December 19, 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 (and 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).

This essay analyzes the Sony Pictures cyberattack within the peacetime framework of international law, examining attribution to the DPRK, the operation's status under the prohibitions on intervention and sovereignty, and its relationship to the use-of-force thresholds. It also evaluates the United States' available legal responses and the jurisdictional issues raised by prosecuting individuals involved in the operation.

2. Legal issues involving the attack

North Korea was not engaged in an armed conflict with the United States at the time of the Sony attack. Despite the hostile diplomatic relationship between the two states, their tensions had not escalated to an armed conflict. As a result, the appropriate legal framework for assessing this operation is the peacetime framework, which provides a distinct set of rules and principles governing state conduct in cyberspace. Had the two states been in an armed conflict, the analysis would fall under the Law of Armed Conflict (LOAC) and international humanitarian law (IHL), which establish a different set of obligations for cyber operations (Fleming, 2025).

In order to analyze any cyber operation under international law, the first step is establishing attribution. In this case, GOP was tied to the Lazarus Group, which in turn reports to the RGB, the intelligence branch of the North Korean government. It is crucial to note that intelligence agencies are organs of the state. The same way the Central Intelligence Agency (CIA) is an organ of the United States' Government, the RGB is one of the DPRK. Any operations carried out by the RGB, including cyber operations executed by Lazarus Group, are therefore attributable to North Korea.

Moreover, given the political nature of the DPRK's authoritarian regime, it is highly implausible that an operation of the scale and sophistication of the Sony attack could have been carried out by an independent or rogue group without state involvement. North Korea's long history of state-sponsored cyber operations, together with the FBI's findings, makes attribution to the DPRK the only reasonable conclusion. Furthermore, according to the Tallinn Manual, even if an operation is not executed by a formal organ of the state, it is still attributable when the group acts under the state's effective control – that is, when the state provides instructions, direction, resources, or has the ability to stop the operation if it chooses to. Under this standard, the Sony attack would remain attributable to the DPRK (Rule 15 of the Tallinn Manual 2.0) (Schmitt, 2017).

In the following sections, the different legal issues spotted in the analysis of the Sony attack are explained.

1) *Prohibited Intervention:* A central legal issue raised by the Sony attack is whether the attack amounted to what is known as a "prohibited intervention" under international law. International law prohibits states from coercively interfering with other states matters,

especially those that fall under a state's *domain réservé;* political, cultural or social decision making, and other areas of exclusive sovereign authority. Applying this standard requires careful framing. The attack did not merely target Sony as a private corporation; the associated threats of violence against movie theaters were intended to influence whether the United States would allow the release of *The Interview*, arguably raising the seriousness of the situation to a matter of national security, even if shortly after the Department of Homeland Security deemed the terrorist threat not credible (Perlroth & Sanger, 2014). By attempting to induce U.S. authorities to intervene in the distribution of a film – a cultural and political decision falling within the sovereign discretion of the U.S. Government – the operation arguably satisfies the coercion requirement, and added to the 9/11-style threats, demonstrates a deliberate attempt to pressure U.S. decision-making, giving the incident the characteristics necessary to constitute a prohibited intervention under international law. Since the operation has already been shown to be attributable to the DPRK and to constitute a prohibited intervention under international law, it satisfies both elements of Rule 14 of the Tallinn Manual 2.0. Accordingly, the Sony attack qualifies as an internationally wrongful act (IWA) (Schmitt, 2017).

2) *Sovereignty:* Another legal issue to address is whether the United States' sovereignty was violated. States exercise sovereignty over all of its territory, including all cyber infrastructure located within it, including privately owned systems[1]. Under the peacetime framework and the Tallinn Manual 2.0, a cyber operation breaches the sovereignty of a foreign state if it causes physical damage, significant functional loss to systems on state territory or interferes with inherently governmental functions. If we only take into account the functional loss of Sony's systems, caused by the destruction of data through the *Destover* malware, the disruption of operations, and the disabling of thousands of devices, these effects may very well qualify as a violation of sovereignty under the view that significant loss of functionality can infringe a state's territorial sovereignty (Tallinn

[1] The definition of sovereignty under international law includes several components (such as maritime sovereignty or sovereignty over foreign missions). This analysis focuses solely on territorial cyber-sovereignty, as it is the element directly relevant to the Sony case.

Manual 2.0, Rule 4). However, the operation did not directly affect any inherently governmental functions such as elections, diplomacy or national defense. The sovereignty assessment in this case therefore falls within a contested area of international law: the functional loss was significant and clearly satisfies one of the recognized requirements for a sovereignty violation, but the absence of interference with any kind of inherently governmental functions makes the argument less definitive. As a result, whether sovereignty was violated ultimately depends on where one draws the threshold for infringement in the context of cyber operations.

3) *The threat of use of force:* One of the most important elements of the incident was the threat of terrorist attacks if *The Interview* was finally released in theaters. The GOP threatened Sony and the United States Government by invoking the 9/11 attacks, raising serious concern in Washington. Nevertheless, although alarming, these statements do not meet the threshold for a prohibited "threat of force". Under peacetime framework, a threat is unlawful when the action threatened also constitutes an unlawful use of force under Article 2(4) of the United Nations Charter. The Tallinn Manual also reinforces this standard noting that a cyber threat must be (1) attributable to a state and (2) conduct that, if executed, amounts to a use of force (Schmitt, 2017). This terrorist threat fails to satisfy both criteria. Even if Lazarus Group is an organ of the state or under its effective control, the threat did not come *directly* from the DPRK's government, nor was public state policy. In addition, there was no indication of any active terrorist plot within U.S. territory, and no credible capability of executing such threat (Roman, 2014). As for the second criterion, the threat was not a clear promise of direct kinetic military action against the U.S. It is safe to conclude that this specific threat does not constitute a threat of use of force and therefore does not legally allow the United States to engage in self-defense kinetic countermeasures such as a military response (raising the issue to an armed conflict). Nevertheless, this analysis does not make the threats inherently irrelevant. By attempting to intimidate Sony Pictures, theaters and pressure U.S. authorities into banning the film's release, the threats reinforce the previous argument that the operation was coercive in nature, consistent with the elements of a prohibited intervention (Fleming, 2025).

3. Jurisdiction and individual responsibility

Under international law, and applied to cyberspace, there are several types of jurisdictions a state may claim. In this case, the United States had *prescriptive jurisdiction*: the legal authority to make and apply its criminal laws to certain conduct, persons, or situations. In the cyber context, a state may exercise prescriptive jurisdiction even when the perpetrator or the infrastructure used are located abroad, as long as there is a valid jurisdictional basis (Fleming, 2025). The attack was directed at an American firm located in U.S. territory, which gives the United States objective territorial jurisdiction, a basis that applies when a cyber operation is initiated outside the state, but its harmful effects occur within it (Sullivan, 2015). Additionally, under the effects doctrine, a state may assert jurisdiction over foreign cyber operations that produce substantial effects on its economy, security, or legal order (Fleming, 2025).

Nevertheless, there is one action the United States cannot exercise: enforcement jurisdiction inside North Korea, as doing so would violate the DPRK's territorial sovereignty (Sullivan, 2015). In some cases, States can cooperate during criminal investigations through instruments such as Mutual Legal Assistance Treaties (MLATs), which allow one State to request investigative assistance from another. If the United States and North Korea had a cooperative diplomatic relationship, an MLAT could facilitate joint investigative measures across both territories, but that is not the case here. As a result, the United States would require explicit authorization from the DPRK before conducting any investigative or arrest operations within North Korean territory, a highly unlikely scenario. It is important to also note that a state cannot claim a right to exercise enforcement jurisdiction inside another sovereign territory simply because its own sovereignty was violated first. The victim State may resort to countermeasures, which permit certain otherwise unlawful acts aimed at inducing compliance, but even countermeasures cannot breach fundamental rules, including the prohibition on exercising enforcement powers within another State's territory (Fleming, 2025).

Regarding the enforcement and liability, there is still one more issue to discuss. As mentioned earlier, the investigation concluded with the indictment of Park Jin Hyok, a North Korean national believed to be central to the operations of the Lazarus Group, including the Sony breach in 2014.

Authorities do not have specific information about his whereabouts (he is believed to reside either in China or North Korea) or even his age (FBI, 2014). Under legal analysis, Park Jin Hyok does not hold any kind of immunity for his actions as part of the Lazarus Group.

It is important to understand that state responsibility and individual responsibility operate at a parallel level; one does not exclude the other, and domestic criminal law still applies to people who directly participate in cyber-criminal offenses (Schmitt, 2017). In addition, the U.S. can legally indict a foreign national even if he is not physically in the United States, since Park broke U.S. laws. This means that if Park Jin Hyok sets foot in U.S. territory (or in any allied State under an MLAT), and authorities identify him, they are legally allowed to apprehend him and take him into custody for later judicial prosecution. The only other possible alternative that the U.S. has to bring Park Jin Hyok into their judicial system is *extradition*. Extradition is a formal legal process through which one state surrenders an individual to another state for the purposes of criminal prosecution. It is not an automatic obligation under international law and exists only when states have consented to it through extradition treaties or similar agreements. In the Sony case, no extradition treaty exists between the United States and the DPRK, meaning North Korea has no legal obligation to surrender Park Jin Hyok (Fleming, 2025). However, in some cases, MLATs facilitate extradition of individuals. That means that if Park Jin Hyok (or any other foreign indicted individuals) travel to a country that is under an MLAT and/or extradition treaty with the United States, and recognizes the same crimes, the American authorities can request legal and enforcement collaboration, potentially leading to detention and extradition (Sullivan, 2015).

This is where the immunity question comes into play. There are two main types of immunity under international law: *ratione personae* (personal immunity) and *ratione materiae* (functional immunity). Personal immunity applies only to individuals who are heads of state, heads of government, foreign ministers, or diplomats. Park is none of those. Functional immunity applies to "official acts" of the State but does not cover criminal acts under domestic law, such as fraud, persistent penetration of networks/hacking, or terrorist threats[2]. For this reason, the United States

[2] Park Jin Hyok and the Lazarus Group are also behind several ransomware attacks that have had effects in the United States. The U.S. Department of Justice attributed the WannaCry ransomware attack to the Lazarus Group and specifically linked Park Jin Hyok to its development and deployment, noting that the operation caused widespread

has indicted other Advanced Persistent Threat actors (APTs) from various States, including Chinese PLA hackers, Russian GRU individuals believed to be part of the "Sandworm" group, and Iranian IRGC hackers. Nevertheless, even though the U.S. can indict Park and he has no immunity, the U.S. cannot enforce jurisdiction inside DPRK territory for the reasons mentioned earlier. Doing so would violate North Korea's sovereignty (Fleming, 2025).

4. Lawful retaliation available to the United States

Since it has already been established that the IWA is attributable to the state of North Korea, the United States had several lawful options available to retaliate. All of these responses remain within the peacetime framework and do not elevate the situation into an international armed conflict. The first category of lawful responses is *retorsions*, which do not require a prior IWA. Retorsions are unfriendly but always lawful acts. In this case, the United States publicly attributed the attack to North Korea (for which the evidentiary threshold is low) and adopted additional economic sanctions against the regime through Executive Order 13466, issued by President Barack Obama (The White House, 2015).

Another option available to the United States, and one that *does* require a prior IWA, is the use of countermeasures, which are otherwise unlawful acts rendered lawful due to the other state's breach of international law. Countermeasures vary widely, but they must comply with strict requirements reflected in the peacetime legal framework. They must be proportionate to the cyber operation they respond to; for example, the United States could not lawfully disable the North Korean power grid for several days, as that would be grossly disproportionate to the Sony attack and would risk human life (Fleming, 2025). Countermeasures must also remain non-forceful, must be directed at the responsible State rather than private actors (the U.S. could not target a private North Korean firm if those existed), and cannot violate fundamental rules such as the prohibition on the use of force or human rights obligations even though they may otherwise breach an international obligation, as mentioned above (Schmitt, 2017). Despite having the option to employ countermeasures, the United States chose not to engage, at least publicly, in any form of non-

---

disruptions across sectors, including healthcare, logistics, and finance. WannaCry and other operations attributed to Lazarus would also fall under U.S. criminal jurisdiction (U.S. Department of Justice, 2018).

forceful cyber countermeasure against North Korea. Everything the U.S. disclosed fell within the realm of lawful retorsions such as public attribution and economic sanctions. There is no official record or acknowledgment of a U.S. cyber operation carried out as a countermeasure in response to the Sony attack, which indicates that Washington deliberately kept its response within the lowest rung of lawful peacetime measures (FBI, 2014).

5. Conclusion and main findings

The Sony breach of November 2014 became one of the most notorious cyber intrusions against a private firm's network. Much of the public attention focused on the sensational aspects of the leak: celebrity salaries, confidential emails, and unreleased film projects, but the real consequences of the attack were largely overlooked by the general public. The Sony breach is one example within a broader and growing trend of malicious actors targeting specific companies and institutions inside a state. Operations like these have contributed to the rapid expansion of the cybersecurity industry over the past decade, as both private firms and governments attempt to keep pace with the evolving threat landscape created by state-sponsored and non-state actors (Sullivan, 2015).

On the legal front, the attitude remains the same. Every time a new cyber operation takes place, questions come up about attribution, scale, jurisdiction, retaliation, and possible sovereignty violations, and the law keeps shifting as it tries to adapt to an ever-changing cyber environment. In this case, the legal analysis is relatively straightforward. Attribution is clear because of the way Lazarus Group operates and because nothing of this scale happens without the involvement of North Korea's autocratic regime. That makes the DPRK the perpetrator and turns what could have been treated as a criminal matter into an internationally wrongful act. The jurisdiction aspect of the breach is also clear, especially with the absence of an MLAT that could support cooperative enforcement against the individuals involved in Lazarus Group (Fleming, 2025). Park Jin Hyok does not hold any type of immunity in U.S. territory and could be apprehended in any state that maintains an MLAT with the United States.

The retorsion-focused response of the United States is consistent with how most states behave in cyberspace during peacetime. Operations like Aurora, Stuxnet, Cloud Hopper and many others

never triggered forceful retaliation and stayed well below that threshold. States seem to have accepted cyberspace as a kind of "new battlefield" where activity can remain non-violent, with a few exceptions, and where geopolitical goals can be pursued without the costs of traditional conflict.

Cyber espionage, cyber intelligence and cyber military operations have become especially useful for states with fewer resources, like North Korea, to compete with global powers. The DPRK likely knew from the start that the U.S. response would be limited to retorsions, something North Korea has dealt with for decades. It is already the most sanctioned state in the world, which means it has very little to lose when carrying out operations like the Sony breach (Korgun et al., 2022). For the United States, escalating a cyber incident into an international armed conflict makes no strategic sense. A more realistic long-term approach would be strengthening economic intelligence on North Korea to improve the accuracy and effectiveness of imposed sanctions (Greitens et al., 2019).

As a closing note, international law and the Tallinn Manual set extremely strict conditions for when a forceful countermeasure would be lawful, and all of them require either a use of force or a cyber operation with clear kinetic-level effects (critical infrastructure targeting or loss of human life, for example). The Sony attack does not meet that threshold (Schmitt, 2017). With these legal and strategic boundaries in place, escalation was never a rational option, and the DPRK almost certainly understood this before penetrating Sony's network (National Security Archive, 2017).

References

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

Fleming, C. (2025). *The peacetime legal framework for cyber operations: Internationally wrongful acts in cyber & lawful state responses*. NYU School of Professional Studies.

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

Greitens, S. C., & Brazinsky, G. (2019). Explaining economic order in North Korea. *Korea and the World: New Frontiers in Korean Studies*, 129-156.

Korgun, I., & Toloraya, G. (2022). On the question of effectiveness of sanctions against DPRK. *Polis. Political Studies*, *32*(3), 80-95.

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

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

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

Sullivan, C. (2015). The 2014 Sony Hack and the Role of International Law. *J. Nat'l Sec. L. & Pol'y*, *8*, 437.

The White House. (2015). *Executive Order—Imposing additional sanctions with respect to North Korea*. The White House, Office of the Press Secretary.

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.