Cite as Sullivan, 8 J. NAT'L SECURITY L. & POL'Y ___ (forthcoming 2016)

# THE 2014 SONY HACK AND THE ROLE OF INTERNATIONAL LAW

*Clare Sullivan*[*]

## INTRODUCTION

2014 has been dubbed "the year of the hack" because of the number of hacks reported by the U.S. federal government and major U.S. corporations in businesses ranging from retail to banking and communications. According to one report there were 1,541 incidents resulting in the breach of 1,023,108,267 records, a 78 percent increase in the number of personal data records compromised compared to 2013.[1] However, the 2014 hack of Sony Pictures Entertainment Inc. (Sony) was unique in nature and in the way it was orchestrated and its effects.

Based in Culver City, California, Sony is the movie making and entertainment unit of Sony Corporation of America,[2] the U.S. arm of Japanese electronics company Sony Corporation.[3] The hack, discovered in November 2014, did not follow the usual pattern of hackers attempting illicit activities against a business. It did not specifically target credit card and banking information, nor did the hackers appear to have the usual motive of personal financial gain. The nature of the wrong and the harm inflicted was more wide ranging and their motivation was apparently ideological.

Identifying the source and nature of the wrong and harm is crucial for the allocation of legal consequences. Analysis of the wrong and the harm show that the 2014 Sony hack[4] was more than a breach of privacy and a criminal act. If, as the United States maintains, the Democratic People's Republic of Korea (hereinafter North Korea) was behind the Sony hack, the incident is governed by international law.

The argument presented in this paper is that assuming North Korea is responsible, the 2014 Sony hack at least breached U.S. sovereignty. When viewed in its entirety, arguably it constituted an orchestrated attack on the United States, although the target, adversary, method of attack and the notions of territory and damage appear very different from those in traditional warfare. This article raises the question whether this type of cyber operation is the next evolution of modern warfare. The author asserts that new thinking is needed on these

---

[*] LLM, MBA, PhD. Fellow, Center on National Security and the Law, Georgetown University Law Center, Georgetown University, Washington DC, USA.

[1] Arjun Kharpal, *Year of the hack? A billion records compromised in 2014*, CNBC (Feb. 12, 2015), http://www.cnbc.com/id/102420088.

[2] Other holdings include Columbia TriStar Motion Picture Group (which includes Columbia Pictures, Screen Gems, and Sony Pictures Classics), marketing and acquisitions unit TriStar Pictures, Sony Pictures Television, Sony Pictures Home Entertainment, Sony Digital Production, and Crackle online video.

[3] Sony is the only movie studio currently owned by the Japanese company. In Tokyo, Sony's chief executive, Kazuo Hirai, president and CEO of the parent Sony Corporation, was "very much concerned "about *The Interview* according to leaked internal emails. Hirai believed the movie could enrage North Korea. The relationship between Japan and North Korea is tense and has been so since the Japanese occupation of Korea from 1910 to 1945. See, Mark Seal, An *Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 4, 2015), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

[4] This paper refers to the cyber operation which was discovered at Sony Pictures Entertainment Inc. in November 2014 as "the 2014 Sony hack" because that is how it came to be known, but bear in mind that the operation was more than just a hack.

issues so that countries like the United States, and the international community generally, can adequately defend and deter attacks of this nature.

## I. THE SONY HACK - THE SUMMARIZED SEQUENCE OF EVENTS

The 2014 Sony hack has been described as the most devastating attack on a U.S. company to date.[5] It was a deliberate, sustained attack against the corporation and individuals, primarily employees and contractors – civilian targets. It involved threats, unauthorized obtaining of data including data relating to individuals, and operational damage to Sony systems. The intrusion may have begun more than a year before it was discovered in November 2014.[6] Its origins have been traced back to June that year.[7]

On June 11, 2014 in a letter to UN Secretary-General Ban Ki-moon, the North Korean government denounced the Sony film *The Interview,* a comedy about a fictional CIA plot to assassinate Kim Jong Un, as "undisguised sponsoring of terrorism, as well as an act of war."[8] The letter promised "decisive and merciless countermeasure [if] the U.S. administration tacitly approves or supports" the movie.[9] On June 27, the North Korean ambassador to the United Nations, Ja Song-nam, unsuccessfully requested that the Security Council adopt the statement of the Democratic People's Republic of Korea against the film.[10]

On June 25, the Korean Central News Agency posted a statement from the country's foreign minister criticizing the U.S. for "bribing a rogue movie maker" to produce a "film on insulting and assassinating the supreme leadership." The release of the movie was described as "intolerable," "terrorism," and "a war action." The minister threatened decisive and merciless countermeasures if the movie was released.[11]

On November 21, "God'sApstls" sent an email to Michael Lynton and Amy Pascal, co-chairs of Sony stating, "[W]e've got great damage by Sony Pictures. The compensation for it, monetary compensation we want. Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely." Three days later the image of a skull and long skeletal fingers appeared on the computer screens of employees at Sony headquarters in Culver City, California with the message: "This is just the beginning… [W]e've obtained all your internal data." Identifying themselves as "Guardians of Peace" (GOP), they stated that they would release Sony's "top secrets" unless the company agreed to "obey" their demands.

On November 29, Kevin Roose, a senior editor at Fusion.net, was one of several journalists who received an email stating: "Hi, I am the boss of G.O.P. A few days ago, we told you the fact that we had released Sony Pictures films including Annie, Fury and Still Alice to the web. Those can be easily obtained through internet search. For this time, we are

---

[5] Ronald Grover, Mark Hosenball & Jim Finkle, *Sony Suffered The Most Devastating Hack Of A Major US Company Ever*, REUTERS (Dec. 3, 2014), http://www.businessinsider.com/the-size-and-scope-of-the-sony-hack-is-incredible-2014-12.
[6] Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014), http://www.wired.com/2014/12/Sony-hack-what-we-know.
[7] *See* Gary Leupp, *A Chronology of the Sony Hacking Incident*, COUNTERPUNCH (Dec. 29, 2014), http://www.counterpunch.org/2014/12/29/a-chronology-of-the-Sony-hacking-incident.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Mark Seal, An *Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 4, 2015), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

about to release Sony Pictures data to the web. The volume of the data is under 100 Terabytes**."**[12]

The email contained links to data that had been posted on Pastebin, and a password, "diespe123." Roose is reported to have used the password and found labelled folders containing what he described as an "insane" amount of Sony internal information. [13]

A series of eight data dumps of an estimated 38 million files followed. The hackers used the media, emailing alerts to journalists and writers at various websites including Gawker, BuzzFeed, Mashable, the Verge, Re/code, the Daily Beast, and others to direct them to the file-sharing sites from which they could download information from the latest file dump.[14]

The full content of the data dumps is still not known, but reportedly they contained previously unpublished pilot scripts and detailed financial data, including revenues and budget costs and invoice facsimiles, for all of Sony's recent films. There were comparisons of movies' financial performance, and projected performance of films yet to be released, confidential movie release dates for Sony and Sony-owned Columbia Pictures, and information about promotion activities and costs including gifts. Five Sony, movies including four which were previously unreleased, were posted to file-sharing networks.

The data included information about corporate and personal bank accounts, wire transfer confirmations, and receipts. There were also copies of passports and visas of cast and crew members and personal email addresses[15] and aliases used by celebrities,[16] phone numbers of assistants to stars,[17] and in one case a home address,[18] as well as employee passwords. There were also Human Resources spreadsheets containing employee names, birth dates, social security numbers, health conditions and medical costs of Sony employees and their families; and information about salaries and performance. One file contained correspondence over several years, apparently of Amy Pascal, which proved to be both revealing and embarrassing and led to her later resignation.

There were reports that Sony employees were the victims of fraudulent credit card and banking transactions, as their credit card and banking details became public.[19] Sony assisted employees with credit protection and fraud alerts, as well as setting up new email and

---

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] Reportedly Seth Rogen and Emma Stone's personal email addresses as well as email addresses of lesser known celebrities were in the information. See, Stan Schroader,"*The Damage Done, Sony Pictures Hack Reveals More Embarrassing Details*" MASHABLE (Dec.9, 2014), http://mashable.com/2014/12/09/sony-hack-details/#a0r3lNrbu5qt.
[16] Natalie Portman is "Lauren Brown." Daniel Craig is "Olwen Williams." See, Stan Schroader,"*The Damage Done, Sony Pictures Hack Reveals More Embarrassing Details*" MASHABLE (Dec.9, 2014), http://mashable.com/2014/12/09/sony-hack-details/#a0r3lNrbu5qt.
[17] There were reports that Brad Pitt's phone number was listed but the number appears to be that of his assistant.
[18] Jesse Eisenberg's home address was reportedly included. See, Stan Schroader,"*The Damage Done, Sony Pictures Hack Reveals More Embarrassing Details*" MASHABLE (Dec.9, 2014), http://mashable.com/2014/12/09/sony-hack-details/#a0r3lNrbu5qt.
[19] *Id.*

phone accounts. The FBI reportedly provided victim counselling and presented seminars on identity theft.[20]

On December 5, a message claiming to be from GOP was emailed to Sony employees stating: "Many things beyond imagination will happen at many places of the world. Our agents find themselves act in necessary places. Please sign your name to object the false of the company at the email address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger."[21]

On December 7, North Korea denied involvement but called the hacking a "righteous deed." On December 8, the GOP warned Sony to "[S]top immediately showing the movie of terrorism which can break regional peace and cause the War!"[22]

On December 16, reporters received an email purporting to be from the GOP stating:

> "We will clearly show it to you at the very time and places The Interview be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time."[23]

The next day Sony cancelled the planned Christmas Day release of *The Interview* and the hackers contacted Sony, praising this as a "wise decision."[24]

On December 18, White House Press Secretary Josh Earnest stated, "I can tell you that, consistent with the president's previous statements about how we will protect against, monitor and respond to cyber incidents, this is something that's being treated as a serious national security issue."[25] On December 19, the FBI announced, "[A]s a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions…. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves."[26]

At a press conference on December 19, President Obama repeated the FBI's allegation and criticized Sony's decision not to proceed to release *The Interview*. The next day, North Korea again denied responsibility and demanded that the United States agree to a joint investigation, a demand which was rejected by the United States in a statement by the Department of State on December 22:

---

[20] *Id.*
[21] *Id.*
[22] On December 15, 2014, Sony Pictures CEO Michael Lynton announced that the ongoing investigation is being handled at the "highest level" of the FBI, and on December 16, 2014, the FBI stated, "We are aware of the threat." David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.* Some commentators have disputed the involvement of North Korea, maintaining that the hackers were posing as North Korea and that the hackers may have been Sony insiders. For the purposes of the analysis of the legal issues, this paper does not enter into this debate but does later address the issue of attribution.

> "[T]he government of North Korea has a long history of denying responsibility for its destructive and provocative actions, and if they want to help here, they can admit their culpability and compensate Sony for the damage they caused." [27]

That day the Internet in North Korean reportedly shut down for nine hours, and connectivity was intermittent for the following two days.[28] The U.S. State Department refused to comment about U.S. involvement, stating "[T]he president has spoken to what our potential response is, separate and apart from what we've seen over the last 24 hours." State Department deputy spokeswoman Marie Harf said, "I leave it to North Koreans to talk about if their Internet was up, if it wasn't, and why."

On December 23, Sony announced that it would proceed with release of *The Interview* on Christmas Day. President Obama praised the decision. [29] The movie opened to limited screening in selected cinemas.

## II. WHY THE 2014 SONY HACK IS MORE THAN A BREACH OF PRIVACY AND A CRIMINAL ACT

The hackers took terabytes of private data and facilitated its public disclosure. They deleted the original files from Sony computers, left messages threatening the company and individuals, and installed malware to cover their tracks (which rendered most of the Sony network inoperable). The effects were felt well into 2015. The hack was a wrong in all these respects, and while the full impact is not yet known, harm has clearly been done to Sony (as well as to other companies and individuals involved in the hack) in the form of data destruction and information disclosure.

The key issues are: how the wrong and harm should be legally characterized; and who is responsible. Attribution determines whether the wrong and the harm are governed by private law or international public law.[30]

From a legal perspective, there is considerable doubt about the effectiveness of private law in addressing the wrongs done and harm inflicted by the 2014 Sony hack. This is apparent when the privacy and criminal law implications are considered. Section II A of this paper considers the privacy implications, particularly from Sony's perspective. The practical limitations in applying U.S. criminal law to the Sony hack are examined in Section II B and attribution and what constitutes an attack are examined in Section III. Sections IV, V, and VII analyze the hack under applicable principles on international law and Section VIII raises the question whether the Sony hack is the next evolution of modern warfare. Section IX discusses lawful countermeasures.

### *A. The 2014 Sony Hack and the Privacy Implications*

---

[27] *Id.*

[28] Francesca Chambers, Lucy Crossley & Alexandra Klausner, *North Korea's internet is shut down AGAIN after losing connectivity for nine hours yesterday*, DAILY MAIL (Dec. 24, 2014), http://www.dailymail.co.uk/news/article-2885359/North-Korea-s-internet-shut-losing-connectivity-nine-hours-yesterday.html.

[29] *See* Leupp, *supra* note 7.

[30] "It is the element of attributability – the reciprocal ability to say 'who did it'– that makes law work." Michael J. Glennon, *The Road Ahead: Gaps, Leaks and Drips*, 89 INT'L L. STUD. 362, 380 (2013).

While the hackers accessed the Sony network without authority and breached privacy,[31] their primary objective seems to have been to facilitate a breach of privacy by others, in order to make selected information available to the general public.

The hackers periodically loaded Sony data files onto anonymous file sharing sites, but ultimately, the decision as to what to report to the public was left to those with this password access. Most news organizations concluded that at least some of the information in the data dumps was newsworthy and reported it. Selected information was also posted and reposted online. As a result, on December 14, Sony demanded that media organizations stop reporting on the leaked documents and delete any copies in their possession.

However, the reporting of information found in the Sony data dumps is not unlawful. As long as the reporter and news organization have not participated in the Sony attack itself, they have a First Amendment right to report on newsworthy information found in the documents. The information reported was newsworthy and, as the Supreme Court observed in *Bartnicki v. Vopper aka Williams,* "[I]n these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance."[32] Media organizations did not participate in the hack, and as part of freedom of speech they have a right, and many would say a duty, to report newsworthy aspects, even if the information was made available through illegal means. This was made clear in *Bartnicki v. Vopper aka Williams* where the Court ruled that a radio station could not be held responsible for broadcasting the contents of newsworthy audio recordings which were originally made in violation of wiretapping laws. The same principle can apply to information obtained from the 2014 Sony hack data dumps.

While there are options for Sony to take action for breach of its privacy, the corporation is facing a class action lawsuit by current and former Sony employees and family members whose private information was disclosed. The action alleges that Sony was negligent for leaving its computer systems insufficiently protected. The complainants also allege Sony violated California state law that requires employers to protect employees' medical records, as well as California and Virginia state laws requiring companies to notify consumers of data breaches.

While some experts believe that Sony could not have guarded against the type of attack that occurred in late 2014, there is a counterargument that the Sony PlayStation network hack in 2011[33] put Sony on notice that its system was vulnerable. Reports that files were descriptively labelled, enabling the hackers to easily find sensitive information, strengthen the argument that Sony could have done more.[34]

However, the plaintiffs in the class action face a significant threshold issue before the substantive security issues can be addressed. For the class action, the complainants must

---

[31] In reading the list of files, the hackers breached privacy. They similarly breached privacy if they accessed file contents, but there are reports that the Sony files were clearly labelled so it may not have been necessary for the hackers to actually access files to know their contents. *See, e.g.*, Tom Fox-Brewster, *Sony needed to have basic digital protection. It failed*, THE GUARDIAN (Dec. 21, 2014), http://www.theguardian.com/commentisfree/2014/dec/21/sony-hacking-north-korea-cyber-security.

[32] 532 U.S. 514, 534 (2001).

[33] For more information on this hack, see Emily Chung, *PlayStation data breach deemed in 'top 5 ever'*, CBC NEWS (Apr. 27, 2011), http://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548.

[34] *See* Fox-Brewster, *supra* note 31.

show that they've actually been harmed by the release of their personal information or will suffer "certainly impending" harm. The U.S. Constitution's provision on standing to sue in federal court requires that condition be met, according to *Clapper v. Amnesty International.*[35] *Clapper v. Amnesty International* concerned a challenge to wiretapping by the NSA. It has since been argued as a threshold issue for defendants in cases against retailers whose customer information was hacked,[36] and federal judges have ruled that consumers could not sue because they had not suffered actual injury as required under *Clapper v. Amnesty International*.[37] The threat or prospect of a threat of injury is not sufficient to establish cause. Justice Samuel Alito's opinion held that standing depends on an actual injury or "certainly impending" injury which cannot be satisfied by "a highly attenuated chain of possibilities"; spending money to ward off feared injury is not sufficient.[38] "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."[39]

Justice Alito explained earlier that "(Plaintiffs) cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[40] While this view is open to criticism in the era of digital identity on the basis that the injury actually occurs at the moment of unauthorized disclosure, *Clapper v. Amnesty International* currently presents a hurdle for the class action against Sony.

The irony, of course, is that the class action for breach of privacy is against Sony. Irrespective of the eventual outcome, Sony has to deal with this, and future law suits, and the ongoing publicity they will bring – thus increasing the harm suffered by the company as a consequence of the 2014 hack.

### *B. The 2014 Sony Hack and the Wrong and Harm*

---

[35] 133 S.Ct. 1138, 1147 (2013).

[36] Counsel for the class action against Sony, are reported to have said however that Sony shouldn't even attempt to contest their clients' constitutional standing to sue. "Are they really going to claim that the disclosure of personnel files and medication information is not a harm?" Lynn Sarko said. "I would be shocked if a judge were to find no injury. ... And I think the public would be outraged." Alison Frankel, *Do Sony employees have the right to sue over data breach?*, REUTERS (Dec. 16, 2014), http://blogs.reuters.com/alison-frankel/2014/12/16/do-sony-employees-have-the-right-to-sue-over-data-breach.

[37] This is a significant issue. *Clapper v. Amnesty International* is open to criticism on the basis that injury has been suffered by the data exposure per se. In December 2014, U.S. District Judge Paul Magnuson in St. Paul, Minnesota rejected Target's argument that the consumers lacked standing to sue because they could not establish any injury. *In re* Target Corp. Customer Data Security Breach Litigation, 64 F. Supp. 3d 1304 (D. Minn. 2014). Despite Target not having a direct relationship with financial institutions issuing credit and debit cards to customers affected by the data breach, the court found that Target's conduct created an increased risk of harm such that the banks, as foreseeable victims, had standing to sue. *Id.* at 1309. Earlier in 2014, U.S. District Judge Lucy Koh found that Adobe customers whose data was exposed by hackers suffered actual injury from the risk their information would be misused. *In re* Adobe Systems Privacy Litigation, 66 F. Supp. 3d 1197 (N.D. Cal. 2014). Judge Koh found that the customers had constitutional standing to sue by virtue of the money they spent to mitigate the potential harm – a holding that other judges have found to be barred under *Clapper v. Amnesty International*. According to Judge Koh, the appropriate precedent in the 9th Circuit is the 2010 decision in *Krottner v. Starbucks*, which involved the theft of a laptop containing unencrypted information on nearly 100,000 Starbucks employees. Krottner v. Starbucks, 628 F.3d 1139 (9th Cir. 2010). In *Krottner*, the court found that because the theft posed a "credible threat of real and immediate harm" to a class of Starbucks employees, those employees met constitutional requirements for standing. *Id.* at 1143. The case was dismissed on other grounds.

[38] Amnesty Int'l, 133 S.Ct. at 1148.

[39] *Id.*

[40] *Id.*

The 2014 Sony hack exposed virtually every aspect of Sony's business and its business practices. The information dumps were found to include audits, budgets, budget averages, bank accounts, wire transfers, invoices, financial forecasts, legal documents, personal notes and emails, strategic documents, plans and presentations. When this information was made public, it was of course also available to Sony's competitors and rivals and others who could use the information to their advantage.[41]

Following the breach, the hackers installed Wiper, malware which erases data from the servers. Reportedly, this is the first time a major U.S. company has been subjected to this type of destructive software which is designed to make computer networks inoperable.[42] Sony was forced to shut down its internal computer network to prevent further damage,[43] and the impact was still being felt months afterwards. In January 2015, Sony announced the delay in submission of its third-quarter results because of the impact of the 2014 hack on its network. The company said then that most financial and accounting applications would not be working until early February, and announced that financial regulators had been asked to extend the filing of Sony's report to March 31, 2015.[44]

It is now known that Sony incurred significant direct costs in investigating the breach which included operational losses as a result of system shut-down, costs of increasing its security,[45] and legal costs from the class action lawsuit in California for allegedly failing to adequately protect the personal information of its employees and contractors.[46] On February 4, 2015 during provisional announcement of its financial results, Sony reported that the 2014 hack had a predicted direct cost of approximately $15 million, much of which will be covered by insurance. That figure has now been confirmed.[47] However, this is only the quantifiable cost. Sony admits that the full extent of the hack is still not known. As a result, the extent of the harm is also not known. No one knows how the information obtained will be used and the consequences for Sony, and other companies and individuals caught up in the situation.

In addition to the impact on individuals, the information released impacts Sony's present and future projects, negotiations (including pay disputes), and general dealings with employees and contractors. It also exposes the company to further lawsuits beyond the present data breach class action. With only a small portion of the data dumps released, revelations could continue into the future. The overall result is a general undermining of Sony's standing and its competitive advantage in an industry which depends on relationships, confidentiality and public image.

---

[41] The information included personal data for employees at Sony and partner companies. While there is no evidence that the Sony hackers used this information for personal fraud, the data dumps made it available to others with opportunity and motive.

[42] Ronald Grover, Mark Hosenball & Jim Finkle, *Sony Pictures struggles to recover eight days after Cyber Attack*, REUTERS (Dec. 3, 2014), http://www.reuters.com/article/2014/12/03/us-Sony-cybersecurity-investigation-idUSKCN0JG27B20141203. The data-wiping virus had made computers using Microsoft Windows software inoperable.

[43] Zetter, *supra* note 6.

[44] Ritsuko Ando, *Sony to delay official submission of third quarter results after hacking*, REUTERS (Jan. 23, 2015), http://www.reuters.com/article/2015/01/23/us-Sony-results-delay-idUSKBN0KW0Q520150123.

[45] Seal, *supra* note 11.

[46] It has been reported that personal information including social security numbers and medical information of employees and their family members was not encrypted or password protected. It has also been reported that passwords for computer and social media accounts were stored in a folder labeled "password," making it easy for the hackers to locate sensitive information. *See, e.g.*, Fox-Brewster, *supra* note 31.

[47] Sam Frizell, *Sony Is Spending $15 Million to Deal With the Big Hack*, TIME (Feb. 4, 2015), http://time.com/3695118/sony-hack-the-interview-costs.

The 2014 Sony hack highlights the essentially intangible nature of this type of operation and the widespread, on-going harm it can cause. The hack also showcases the increasingly important dual role of information[48] as both a target and a highly effective weapon capable of causing considerable damage.

While acts by non-state actors have traditionally been regarded as crimes, the 2014 Sony hack shows the overall ineffectiveness of the criminal law in addressing the wrong and harm and in deterring future attacks. The hackers breached federal and state criminal law in entering the Sony network without authorization. They also caused malicious damage in rendering the Sony system inoperable by planting malware.[49] But bringing the hackers to justice is difficult in the absence of an extradition treaty and cooperation at the state level.[50] The effectiveness of the criminal law in punishing offenders and in providing deterrence is highly questionable when hackers are apparently motivated by ideology and are, in effect, encouraged and protected by a rogue state like North Korea.

State-to-state countermeasures can be much more effective in their short- and long-term impact, particularly in de-escalating conflict and deterring its recurrence. The type of countermeasure that can be legitimately used depends on how the wrongful act is characterized under international law and whether it can be attributed to a state (in this case North Korea).

## III. ATTRIBUTION AND STATE RESPONSIBILITY FOR CYBER OPERATIONS

Recall that at the United Nations, North Korea declared *The Interview* an act of war. Subsequently, a cyberattack attributed to North Korea was launched against Sony, a U.S. corporation based in California. The 2014 Sony hack was described by White House spokesman Josh Earnest as an example of "destructive activity with malicious intent that was initiated by a sophisticated actor."[51]

---

[48] In this article, "information" includes data and vice versa, unless specified otherwise.

[49] Many criminal damage offense provisions still require tangible damage, however. See, for example, CAL. PENAL CODE § 594 (West 2008).

[50] Those involved in the 2014 Sony hack risk prosecution under U.S. law in much the same way that the five Chinese military hackers who were indicted in May 2014 for computer hacking, economic espionage and other offenses. But there are significant legal and practical challenges in bringing them to justice, especially in bringing them to trial in the United States in a timely manner. Often the only option is to wait until the alleged perpetrators travel to another jurisdiction with which the United States has an extradition treaty. The perpetrators may well leave North Korea eventually, but it can be a long wait to bring them to justice, and that can impact on the quality of the evidence produced by the prosecution.

[51] David Brunnstrom & Jim Finkle, *U.S. considers 'proportional' response to Sony hacking attack*, REUTERS (Dec. 18, 2014), http://www.reuters.com/article/2014/12/18/us-Sony-cybersecurity-northkorea-iduskbn0jw24z20141218. The FBI attributed the 2014 hack to North Korea: "While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following: Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks." Press Release, Fed. Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. The FBI observed "significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack." *Id.* The FBI stated that separately, the tools used in the Sony hack attack have similarities to a cyberattack in March 2014 against South Korean banks and media outlets, which was carried out by North Korea. *Id.*

International public law governs state responsibility for harm to another state in the cyber domain.[52] If, for example, North Korea's Bureau 21 mounted the 2014 Sony hack, there is no doubt as to state responsibility. Actions of state "organs" are recognized in Article 4 of the International Law Commission (ILC)[53] Articles on Responsibility of States for Internationally Wrongful Acts 2001[54] (ILC Articles) as attributable to the state. This is so even if the actions are *ultra vires*.

If the 2014 Sony hack was conducted by a group which is not designated as a state organization, under Article 8 of the ILC Articles,[55] attribution traditionally attaches to the state only if North Korea directed and controlled the operation or later acknowledged and adopted it as North Korean action under Article 11.[56] This is the traditional approach, though it should be noted that these rules (as codified in the ILC Articles) were developed for a vastly different era.

The ILC Articles "seek to formulate, by way of codification and progressive development, the basic rules of international law concerning the responsibility of States for their internationally wrongful acts."[57] Whilst they are not binding, the ILC Articles are highly influential and have been cited by the International Court of Justice (ICJ).[58] The ILC Articles codify customary international law. However, they are the product of fifty years of work by the ILC which culminated in 2001, well before the world was aware of operations like the Sony hack. The principles of international law were developed to deal with kinetic attack and, understandably, are concerned to limit its use and escalation. For this reason, international law has traditionally defined state responsibility narrowly.

For example, Article 8 of the ILC Articles which is entitled "Conduct directed or controlled by a State," states that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." It is not clear how much control is required, and the law in this area is highly coloured by traditional military operations and kinetic attack. This is evident in the "effective control" test adopted by the International Court of Justice in *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*,[59] (*Nicaragua* case). The Court held that in a military context, for a state to be responsible for the acts of a non-state actor, the former must have effective control over the latter. As Peter Margulies observes in his recent

---

[52] The White House view is that "the development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace." THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (2011).

[53] The ILC was created by the United Nations General Assembly in 1947 to codify and progressively develop international law. The ILC has become the most influential body in the development of international law.

[54] G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts, art. 4 (Dec. 12, 2001).

[55] "[T]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." *Id.* art. 8.

[56] "[C]onduct acknowledged and adopted by a State as its own Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own." *Id.* art. 11.

[57] Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 31 (2001).

[58] For example, the ICJ cited the views of the ILC in conforming that the United Nations Charter prohibition on the use of force "constitutes a conspicuous example of a rule in international law having the character of *jus cogens*." Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 190 (June 27).

[59] *Id.* ¶ 392.

scholarship on sovereignty and cyberattacks, "[W]hile to American ears 'effective control' may connote practical control, the ICJ's use of the term is something closer to "specific, comprehensive control."[60]

In *Prosecutor v. Tadić* [61] the International Criminal Tribunal for the former Yugoslavia used the "overall control" test for criminal proceeding against an individual. This test was formulated for the purpose of determining the nature of armed conflict and in a later case, the ICJ distinguished the evaluation of the nature of armed conflict from state responsibility.[62] "Overall control" is considered a lower threshold than the control required in the *Nicaragua* case, but the International Criminal Tribunal determined that the necessary level of control still required more than "the mere financing and equipping of such forces."[63] The tribunal held that "effective control" involves "'coordinating or helping in the general planning of [the group's] military activity."[64] Mere financing, training, equipping and providing operational assistance was not considered sufficient.

The traditional approach is reflected in the ILC Articles which, in turn, influence legal scholarship on cyberattacks – in particular the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual or the Manual).[65] The Tallinn Manual is, in effect, the collected views of an International Group of Experts (IGE) as to the legal principles applicable to cyberattacks and cyberwarfare. The manual does not represent official views of states, nor of international bodies such as NATO. It is nevertheless influential especially in states' interpretation and practical application of principles of international law in the cyber realm. This is especially so because at present there is no specific guidance from bodies such as the ICJ as to the application of international law to cyberattacks like the 2014 Sony hack. The Tallinn Manual, which was published in 2013, is presently the only systematic effort to adapt the law of armed conflict (LOAC) to cyber.

The Manual deals with what it calls "cyber warfare," which Professor Schmitt says generally encompasses "both the *jus ad bellum*, the international law governing the resort to force by States as an instrument of their national policy, and the *jus in bello*, the international law regulating the conduct of armed conflict (also labelled the law of war, or international humanitarian law)."[66]

The Tallinn Manual follows the approach of the ILC and where possible the ICJ, on state responsibility. However, both the ILC and decisions of the ICJ were developed for traditional military operations which involve tangible damage. The strong influence of this tradition is evident in the key provisions of the Tallinn Manual.

A notable example is Rule 30 which defines cyberattack as "… a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to

---

[60] Peter Margulies, *Sovereignty And Cyber Attacks: Technology's Challenge To The Law Of State Responsibility Sovereignty & Cyber Attacks*, 14 MELBOURNE J. INT'L L. 1, 11 (2013). Peter Margulies is a Professor at Roger Williams University School of Law, Rhode Island.
[61] Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 120 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
[62] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 404-407 (Feb. 26).
[63] *Tadić*, *supra* note 61, ¶ 145.
[64] *Id.* ¶ 131. *See also* Margulies, *supra* note 60, at 11-12.
[65] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).
[66] *Id.* at 18.

persons or damage or destruction to objects."[67] This definition envisages cyber being used, but to deploy traditional weapons which are designed to inflict tangible damage. The commentary states that "the word 'cause' in this Rule is not limited to effects on the targeted cyber system. Rather, it encompasses any reasonably foreseeable consequential damage, destruction, injury, or death."[68] However, this notion of damage is still tied to tangible, physical impact. As a result, it does not apply to an attack like that inflicted on Sony in 2014.

The Tallinn Manual notes that "although the Rule is limited to operations against individuals or physical objects, the limitation should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack."[69] However, rather than acknowledging the new importance of data and the need to protect it, the commentary again returns to the ensuing physical consequences of cyber operations against data. "[W]henever an attack on data results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack' and the operation therefore qualifies as an attack."[70]

The IGE differ in their views on many key points including what constitutes an attack. The divergent views illustrate the inherent difficulty in applying principles developed for a past era, to new and very different issues. For example,

> "[W]ithin the International Group of Experts, there was extensive discussion about whether interference by cyber means with the functionality of an object constitutes damage or destruction for the purposes of this Rule. Although some Experts were of the opinion that it does not, the majority were of the view that interference with functionality qualifies as damage but only if restoration of functionality requires replacement of physical components."[71]

Again, the link with the physical world, and with the familiar, is evident in the views of the IGE. In this regard it should be noted that extensive experience and expertise of the IGE is in the traditional LOAC and international law, the principles of which were developed for an era when there was a sharper distinction between military and civilian targets, and armed conflict used traditional weapons and inflicted tangible damage.

The commentary considers "a cyber-operation that is directed against the computer based control system of an electrical distribution grid. The operation causes the grid to cease

---

[67] *Id.* at 106. A possible way forward using the exiting terminology of Rule 30 is for the definition of "objects" in the rule to include digital data and information. Data exists and occupies space in a physical sense, on the network, for example, in a storage device. An effects-based definition needs to be included in the definition of an attack on an object to include secondary and tertiary effects.

[68] TALLINN MANUAL, *supra* note 65, at 93. The commentary recognizes that considerable harm can be inflicted by cyber means and draws the analogy between using cyber to open a dam waters and destructive waters being released as a result of the dam being attacked with explosives. "The word "cause" in this Rule is not limited to effects on the targeted cyber system. Rather, it encompasses any reasonably foreseeable consequential damage, destruction, injury, or death. Cyberattacks seldom involve the release of direct physical force against the targeted cyber system; yet, they can result in great harm to individuals or objects. For example, the release of dam waters by manipulating a SCADA system could cause massive downstream destruction without damaging the SCADA system. Were this operation to be conducted using kinetic means, like bombing the dam, there is no question that it would be regarded as an attack. No rationale exists for arriving at a different conclusion in the cyber context." *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

operating. In order to restore distribution, either the control system or vital components thereof must be replaced. The cyber operation is an attack."[72] The manual states that "[T]hose experts taking this position were split over the issue of whether the 'damage' requirement is met in situations where functionality can be restored by re-installing the operating system."[73] Yet this is precisely the new nature of cyberattack and cyberwarfare. Significantly, however, "few Experts went so far as to suggest that interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack. For these Experts, it is immaterial how an object is disabled; the object's loss of usability constitutes the requisite damage."[74] This is precisely the point: the new challenge is the type of attack exemplified by the 2014 Sony hack which is not classified as an armed attack in its traditional sense because of its intangible rather than physical consequences.

In the Manual, the IGE discuss the characterization of a cyber operation that does not cause physical damage but which results in large-scale adverse consequences.[75] The majority "took the position that, although there might be logic in characterising such activities as an attack, the law of armed conflict does not presently extend this far."[76] Again, this is the point. The fact that a court or international tribunal or even that most international law scholars have not yet considered this issue does not mean that the law is incapable of this extension. International law is based on norms of conduct which evolve to adapt to new challenges and new standards of conduct within the international community. This is a defining characteristic of public international law. Unlike common law, for example, which is based on the doctrine of precedent, international law is established through international acceptance. Acceptance can of course be evinced through treaty (i.e. agreement), but most often norms are initially established through conduct.

The 2014 Sony hack illustrates that international law developed for a completely different time is no longer adequate or effective. This shortcoming of the original Tallinn manual has now been acknowledged by the IGE.[77] Reportedly, this type of malevolent cyberattack, which does not rise to the level of armed attack in its traditional sense,[78] will be addressed in the second version Tallinn. Tallinn 2.0, which is currently being developed and is planned for publication in 2016, will follow the original manual but expand its scope.[79] While the precise contents of Tallinn 2.0 are as yet undeveloped and therefore unknown, the IGE will examine the international legal framework that applies to cyber operations that do not rise to the level of an armed attack as it is traditionally defined in international law and under the LOAC on the basis of tangible consequences.[80]

## IV. A New Type of International Conflict and the Role of Public International Law

[72] *Id.*
[73] *Id.*
[74] *Id.* at 94.
[75] *Id.* The example provided in the manual is "blocking email communications throughout the country (as distinct from damaging the system on which transmission relies)." *Id.*
[76] "[T]he minority took the position that should an armed conflict involving such cyber operations break out, the international community would generally regard them as an attack." *Id.* Significantly, "[A]ll Experts agreed, however, that relevant provisions of the law of armed conflict that address situations others than attack, such as the prohibition on collective punishment (Rule 85), apply to these operations." *Id.*
[77] Paul Rosenzweig, *Tallinn 2.0*, LAWFARE (Apr. 27, 2015), https://www.lawfareblog.com/tallinn-20.
[78] Because it does not result in tangible damage.
[79] TALLINN MANUAL, *supra* note 65, at 94.
[80] *Id.*

The target, ostensible perpetrator, method of attack, and the notions of territory and damage appear very different from those of traditional warfare, but the 2014 Sony hack exemplifies a new type of international conflict.[81]

It presents new challenges for international law, particularly in defining sovereignty and state responsibility, and the determining the right to legitimately take effective countermeasures including invoking the right to self-defense. Responding to these new challenges is the purpose and role of public international law. International law evolves over time to establish new standards of conduct. Customary international law, for example, is based on the concept that a rule or principle has evolved over time to become a norm. The principles of international law, including those codified in the ILC Articles which now influence the Tallinn Manual, have evolved over time.[82] However, evolution over many years is not necessary, and in the cyber realm is not appropriate. The ICJ has acknowledged that new norms can form quickly and has specifically referred to technological advances prompting new rules.[83] While established principles can provide a baseline, the argument presented in this paper is that new thinking is needed to effectively address the new issues presented by cyberattacks like the 2014 Sony hack.

The fundamental concern of modern international law as particularly demonstrated since the world wars is to avoid, and if necessary, contain international conflict.[84] The approach to a cyberattack like that perpetrated against Sony as currently presented in the ILC Articles and as reflected in the Tallinn Manual, however, now can have the opposite effect. This approach encourages conflict by categorizing cyberattacks based on their physical consequences. In not recognizing the true nature of the 2014 Sony cyberattack, the right of a law-abiding injured state to legitimately take effective counter measures is uncertain and therefore limited.

While denying involvement, North Korea praised the 2014 Sony hack as a "righteous deed," thereby fomenting or at least tolerating subversive activity aimed at causing civil strife. State responsibility is framed in terms of control, and in the context of the North Korean regime, can it really be said that North Korea has not exercised control? At the very

[81] This century has been notable for the changing nature of warfare. It has been characterized by the rise of terrorism, the use of state-backed actors, the rise of non-state actors like ISIS, and new forms of attack such as the use of commercial airlines to attack new civilian targets such as the World Trade Center and the Pentagon on September 11, 2001, for example. This change includes recognition by governments, including the U.S. government, that warfare now extends to the cyber domain.

[82] The major multilateral conventions governing war date back to the Declaration of Paris of 1856. Other milestones include the Geneva Convention of 1864 which was revised in 1906, the Hague Conventions of 1899 and 1907, and the Geneva Conventions of 1929 and 1949 which, together, helped codify humane treatment for the wounded in the field, acceptable practices of land warfare, the rights and duties of the parties to a conflict and of neutral states and persons, and rules governing the treatment of prisoners and the protection of civilians.

[83] Technological advances in the capacity to exploit the continental shelf prompted re-negotiation of the definition in Act 76 of 1982 United Nations Convention on the Law of the Sea. In the *North Sea Continental Shelf* cases, the ICJ observed that, "[A]s regards the time element, … [a]lthough the passage of only a short period of time [was] not necessarily … a bar to the formation of a new rule of customary international law on the basis of what was originally a purely conventional rule," it was indispensable that "State practice" during that period, "including that of States whose interests [were] specially affected, should have been both extensive and virtually uniform in the sense of the provision invoked;— and should have occurred in such a way as to show a general recognition that a rule of law was involved." North Sea Continental Shelf Cases (Fed. Republic of Ger./Den.; Fed. Republic of Ger./Neth.), Judgment, 1969 I.C.J. Rep. 3, ¶ 74 (Feb. 20).

[84] This objective is especially clear in the United Nations Charter. *See* U.N. Charter art. 1 (stating the purposes of the United Nations).

least, there is now a concept of state due diligence recognized under international law by which a state must not harbor those who engage in subversion and terrorism and is required to have domestic laws punishing these acts.[85] That due diligence is now expected as part of a state's responsibility as a member of the international community and arguably is now established as a norm under customary law.[86]

A state also clearly has an obligation to ensure that operations emanating from its territory do not cause harm to another state. Violation of this obligation of due diligence provides a separate basis for countermeasures by an injured state. This right is presently framed in traditional terms in terms of territory. This traditional approach limits its effective application now because a cyber operation like the Sony hack may be carried out with North Korean acquiescence and even support, but not necessarily from North Korean territory. A cyber operation may be routed through a number of locations to disguise its origin. The Sony hack was reportedly traced back to Thailand.[87] While cyber operations present challenges in determining attribution, those challenges are not insurmountable. The existing obligation under public international law could now be more broadly and realistically framed in terms of its basic premise (i.e. state responsibility), rather than remaining moored to traditional notions of territory.[88]

In the cyber context, the due diligence should be expanded to include state toleration of subversion. While this approach may be criticized on the basis that a state can only control activity within its boundaries, there is a precedent for a broader interpretation. The Declaration on the Principles of International Law (the Declaration),[89] the key interpreter of the United Nations Charter (U.N. Charter), distinguishes "armed intervention" and "*all other forms of interference* or attempted threats against the personality of the State or *against its political, economic and cultural elements*, are in violation of international law"[90] (emphasis added). The Declaration extends to state toleration of subversion by providing that "no State shall organize, assist*, foment*, finance, incite *or tolerate subversive*, terrorist or armed

[85] The September 11, 2001 attacks were the catalyst of for this development whereby greater attention was given by the international community to states' obligations to disrupt networks of non-state terrorist groups operating from their territory. The obligation included not harboring these groups and having domestic law to address their activities.

[86] This responsibility developed largely as a consequence of the rise of terrorism particularly after the September 11 attacks, and it is broad in nature, extending from enactment of protective law such as anti-moneylaundering and counterterrorism financing legislation to international obligations not to harbor terrorists.

[87] Jordan Robertson, Dune Lawrence & Chris Strohm, *Sony's Breach Stretched from Thai Hotel to Hollywood*, BLOOMBERG (Dec. 8, 2014), http://www.bloomberg.com/news/articles/2014-12-07/sony-s-darkseoul-breach-stretched-from-thai-hotel-to-hollywood.

[88] Cyberspace consists of three layers: the physical layer, the logical layer, and the persona. Geographical boundaries may apply to some portions of the physical infrastructure in the physical layer. However, the logical layer and persona are not necessary bound by geography. Warfare in the cyber domain may not have a physical boundary.

[89] G.A. Res. 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970).

[90] The full text is "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law." *Id.* The provision goes on to preserve state sovereignty by providing that: "No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind." *Id.*

activities directed towards the violent overthrow of the regime of another State, *or interfere in civil strife in another State*" (emphasis added).[91]

This provision can be broadly interpreted to apply to the 2014 Sony hack and its political motivation. Viewing state responsibility in this way widens state responsibility for the non-state groups or individuals through which a state like North Korea can operate. Most importantly, it discourages a rogue state from hiding behind the actions of seemingly non-state actors.[92] It provides an injured state with a legal basis for proportional countermeasures and retorsion;[93] and international law imposes crucial limitations on countermeasures in these circumstances. For example, even though the 2014 Sony hack may be considered to have involved use of force, countermeasures by the United States against North Korea for lack of due diligence must not involve use of force, even if it is proportionate. Far from escalating conflict, the right to take proportional countermeasures can balance what is at present a very uneven arena.[94]

Sections 6, 7, 8, and 9 examine how the Sony hack is currently categorized and how it should now be categorized under international law. Section 10 considers the type of countermeasures a state like the United States can lawfully take, depending on how the hack is categorized.

## V. THE 2014 SONY HACK AS A BREACH OF SOVEREIGNTY AND A WRONGFUL ACT UNDER INTERNATIONAL PUBLIC LAW

As stated in *Island of Palmas* (*Neth. v. U.S.*) the principle of "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[95] That independence includes territorial integrity and political independence.[96] The

[91] Nicar. v. U.S., 1986 I.C.J. at ¶ 191.

[92] There is another option for state response to harmful cyber operations when the instigator is a non-state actor or is unknown. A plea of necessity, a notion reflected in Article 25 of the Articles of State Responsibility, is available when harmful cyber operations affect the state's "essential interest" and the action is the only means to address "a grave and imminent peril." *See* G.A. Res. 56/83, *supra* note 54, at art. 25. That state may then take necessary action that would otherwise be unlawful. There is no requirement in such situations that there be an initial "internationally wrongful act" or that, as in the case of countermeasures, the internationally wrongful act be attributable to a State. The 2016 Sony hack cannot be said to involve an essential U.S. interest but if the target had been the power grid or banking system, there may be legal basis to resort to the plea of necessity.

[93] Acts of retorsion are acts that are unfriendly but lawful, such as a state closing its cyber infrastructure to transmissions from the rogue state.

[94] Peter Margulies refers to this as "attribution asymmetry." Margulies, *supra* note 60, at 11-12. Margulies makes the point that "[C]yber is relatively easy to direct, given a sophisticated commander, but very difficult to detect. While it is difficult to direct a group of armed personnel located hundreds or thousands of miles away from the funder of the group, an entity that wishes to control cyberweapons can control their use from a remote location by requiring groups with state cybertools to submit to periodic virtual accounting. On the other hand, unlike conventional kinetic action where effects are manifest within a short time after the weapon is used, cyberweapons can take months to detect, lying dormant for significant periods or secretly altering data to clandestinely compromise a network's operation. This ability to engage in more precise direction while avoiding detection distinguishes cyber from kinetic weapons." *Id.* He also makes the point that at "cyberattacks require far less in the way of personnel." *Id.*

[95] Island of Palmas (U.S. v. Neth.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928). The current notion of state sovereignty has four aspects: territory, population, authority, and recognition. Thomas J. Biersteker & Cynthia Weber, STATE SOVEREIGNTY AS SOCIAL CONSTRUCT (1996).

[96] This is reflected in Article 2 (4) of the U.N. Charter, which provides that: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2(4)

Declaration[97] provides more insight. Significantly, it ties state sovereignty to the rights of subjects, specifically to the rights to self-determination, freedom and independence. These rights lie at the heart of democracy, are recognized and protected under U.S. law, and are of particular relevance to the 2014 Sony hack, which affected so many individuals and other companies.[98] The right to self-determination, for example, is closely tied to the right to privacy; and freedom of expression protects free speech, including the making, screening and viewing of political satire like *The Interview.*

The 2014 Sony hack breached U.S. sovereignty in all aspects: territorial integrity, political independence and the rights of subjects. Nevertheless, the IGE in the original Tallinn Manual still felt that there must be physical damage, not just harm to data, to constitute a breach of sovereignty. However there seems to be a re-thinking of this, and Michael Schmitt has since commented that "it would seem reasonable to characterize a cyber operation involving a State's manipulation of cyber infrastructure in another State's territory, or the emplacement of malware within systems located there, as a violation of the latter's sovereignty."[99] Professor Schmitt has also stated that "[T]he substantive criteria for breach of sovereignty by cyber means has been the subject of extensive examination in the Tallinn 2.0 process."[100] It is to be hoped that this aspect is addressed in Tallinn 2.0 so that a breach of sovereignty encompasses the type of malevolent cyberattack that was perpetrated against Sony in 2014.

State sovereignty exists in cyberspace as it does in the other domains of air, land, and sea; and a state has sovereign control over cyber infrastructure and cyber operations within its territory.[101] The Sony hackers breached U.S. territorial sovereignty when they infiltrated, commandeered, manipulated and interfered with Sony's cyber operations in the United States. The hackers also breached U.S. political independence and rights of U.S. citizens when they threatened U.S. subjects and interfered with their fundamental rights as U.S. citizens to self-determination and to the freedoms protected under U.S. law, particularly under the U.S. Constitution. In all these respects, the hack constituted international wrongful acts under international law.

The question then is how the 2014 Sony hack should be characterized because its character determines the type of response permitted under international law. There are three

---

(emphasis added). Sovereignty, territorial integrity and political independence is also reflected in Article 1 of the Definition of Aggression, for example, which states that: "Aggression is the use of armed force by a State against the *sovereignty, territorial integrity or political independence of another State,* or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition." (emphasis added) G.A. Res. 3314 (XXIX), annex, Definition of Aggression, art. 1 (Dec. 14, 1974).

[97] G.A. Res. 2625 (XXV), *supra* note 89.

[98] The full text is "Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of their right to self-determination and freedom and independence." *Id.*

[99] Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea.

[100] *Id.*

[101] The ICJ has confirmed that a state has the right of control over its territory and other states cannot interfere in that state's freedom to maintain exclusive and independent control over its territory. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, at 36 (Apr. 9). There is general consensus that international law governs activities in cyberspace. For example, the International Group of Experts unanimously concluded that the general principles of international law apply to cyberspace. See TALLINN MANUAL, *supra* note 65, at 13. *Cf.* Secretary-General's High-level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility*, 11, U.N. Doc. A/59/565 (Dec. 2, 2004).

established categories. As outlined in Section 7 below, the two most familiar categories are "threat or use of force" under Article 2(4),[102] or an "armed attack" under Article 51[103]of the UN Charter. However, there is a third well-established category – intervention – which is often overlooked. As discussed in Section 7, interference or attempted threats against the personality of the State or against its political, economic and cultural elements, is a violation of international law.

## VI. THE 2014 SONY HACK IS AN INTERVENTION UNDER INTERNATIONAL PUBLIC LAW

Depending on its "scale and effect," a cyber operation, as is the case in the other domains, may constitute a "threat or use of force" under Article 2(4),[104] or an "armed attack" under Article 51[105] of the UN Charter. The precise meaning of these terms and the distinction between them is not clear. Their relation to "aggression," which is used in a number of UN declarations, most notably in the UN General Assembly's Definition of Aggression,[106] is also not clear. This general lack of clarity makes the application of these provisions to cyber even less certain.

Nevertheless, the wording of Articles 2(4)[107] and 51 and the Definition of Aggression have some scope for application to an event like the 2014 Sony hack. Article 3 of the Definition of Aggression,[108] for example, sets out acts that are considered acts of aggression. While those examples are essentially military acts, part (g) specifically includes "[T]he sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above,[109] or its substantial involvement therein."[110] Article 4 also provides that "[T]he acts numerated…*are not exhaustive* and the Security Council may determine that other acts constitute aggression under the provisions of the Charter" (emphasis added).[111]

"Force" is not defined in the UN Charter but has generally been regarded as requiring military force and not mere economic or political coercion, for example. This is generally confirmed by the Declaration,[112] which also refers to military force. However, both the UN Charter and the Declaration were drafted in a vastly different era, when military force meant armed force in its traditional kinetic sense, not the type of new cyber operation exemplified by the 2014 Sony hack.

---

[102] "All Members shall refrain in their international relations from *the threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2(4) (emphasis added).
[103] U.N. Charter Article 2(4) prohibits use of force and intervention and Article 51 recognizes the right of self-defense in response to armed attack. *Id.*
[104] *Id.*
[105] *Id.*
[106] G.A. Res. 3314 (XXIX), *supra* note 96.
[107] Article 2(4) states that "[A]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2(4).
[108] G.A. Res. 3314 (XXIX), *supra* note 96.
[109] The acts specified above in parts (a) – (f) of Article 3 of the Definition of Aggression include attack, invasion and a state allowing its territory being used by another state to perpetrate an act of aggression against a third state. *Id.* at art.3.
[110] *Id.*
[111] G.A. Res. 3314 (XXIX), *supra* note 96.
[112] G.A. Res. 2625 (XXV), *supra* note 89.

The Declaration does, however, expressly recognize indirect intervention. Distinction is also made between "armed intervention" and "all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."[113] Also, as mentioned earlier in relation to state responsibility, the Declaration extends to state toleration of subversion.[114] In line with this extension, one of the most significant provisions of the Declaration is of particular relevance to the Sony hack and the involvement of North Korea: "[E]very State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force." The ICJ in the *Nicaragua* case affirmed that this formulation of indirect force is included in the prohibition of the threat or use of force in Article 2 (4) of the UN Charter.[115]

The ICJ also provided some guidance on what constitutes an intervention and use of force in the kinetic context in the *Nicaragua* case. The court drew a distinction between "the most grave forms of the use of force (those constituting an armed attack)" and "other less grave forms."[116] The court found that while providing arms and training to the contras were acts amounting to the threat or use of force, mere funding was not.[117] The Court found however, that the funding did constitute an intervention.

The court explained that the non-intervention principle prohibits intervention in a state's "political, economic, social and cultural system, and the formulation of foreign policy."[118] This reasoning can readily be applied to the Sony hack to support the argument that it amounted to an intervention. In relation to the impact on free speech, it was an intervention in U.S. social and cultural values. On a deeper and longer lasting basis, it was an intervention in the U.S. economic system. If the reasoning of the ICJ in the Nicaragua case is applied, North Korea breached its obligation under international law not to "intervene in matters within the domestic jurisdiction of a State" [119]and is responsible for the harm done.[120]

---

[113] The full text is "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law." *Id.* The provision goes on to preserve state sovereignty by providing that: "No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind." *Id.*

[114] Nicar. v. U.S., 1986 I.C.J. at ¶ 191.

[115] *Id.* ¶ 195**.** *See also* JAMES A GREEN, THE INTERNATIONAL COURT OF JUSTICE AND SELF-DEFENSE IN INTERNATIONAL LAW 111–28 (2009); TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 53–68 (2010).

[116] While all use of force is unlawful and can entitle the injured state to a declaration to that effect and to reparation, this finding limits the right to self-defense under Article 51 of the UN Charter to armed attack. In *Oil Platforms (Iran v. U.S.*), Judgment, 2003 I.C.J. Rep. 161, ¶ 51 (Nov. 6), the ICJ drew the same distinction between a use of force and an armed attack as it did in the *Nicaragua* case i.e. based on gravity. This approach has been criticized on the basis that "[The] requirement that an attack reach a certain level of gravity before triggering a right of self-defense would make the use of force more rather than less likely, because it would encourage states to engage in a series of small-scale military attacks, in the hope that they could do so without being subjected to defensive responses. William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 295 (2004). Although Taft made this observation many years ago now, it still rings true, especially in relation to cyber- attacks.

[117] *See* Nicar. v. U.S., 1986 I.C.J. at ¶ 228.

[118] *Id.* ¶ 205.

[119] *Id.* ¶ 41.

## VII. THE 2014 SONY HACK AS A THREAT OR USE OF FORCE PROHIBITED UNDER INTERNATIONAL PUBLIC LAW

A cyber event that violates international law in this way need not rise to the level of an armed attack in order for a state to respond. However, the Sony hack also included threat of force, with a specific threat of violence if Sony did not meet the hackers' demands to withdraw *The Interview*. A key question is whether the hack amounted to a threat or use of force under international law. If so, the question then is whether that threat or use of force was at a level that can be classified as an armed attack under Article 2(4) of the UN Charter and customary international law. As Michael Schmitt correctly states, "[T]he prevailing view in international law is that 'use of force' is a lower threshold than 'armed attack'; all armed attacks are uses of force, but the reverse is not true."[121]

The original Tallinn Manual does not provide further insight on use of force in the cyber context. Michael Schmitt observes, "[U]nfortunately, after three years of discussion, the International Group of Experts (IGE) could arrive at no black letter definition of a cyber use of force."[122] The IGE only agreed that states would make a case-by-case assessment of non-injurious or destructive cyber operations, considering such factors as severity, immediacy of effect, invasiveness, and military character.[123]

The law in relation to threat of force is even less developed that the law relating to use of force. However, it is interesting that Ian Brownlie's explanation of threat of force as "an express or implied promise by a Government to resort to force conditional on the non-acceptance of certain demands of that Government"[124] aptly describes the threat made by the Sony hackers.

Romana Sadurska makes another point relevant to the 2014 Sony hack and which ties in with the view of the Sony hack as an intervention in a state's "political, economic, social and cultural system, and the formulation of foreign policy" as discussed by the ICJ in the *Nicaragua* case.[125] He says that the key aspect is not the kind of force applied or threatened, but the object and purpose of the threat. More specifically, the key question according to Sadurska is whether the threat genuinely reduces the range of options available to the state?[126] In the Sony hack, the object and purpose of the threat was ostensibly to stifle freedom of speech in a country where freedom of speech is protected as a constitutional right,[127] but there was also deeper purpose: commercial harm.

When considered in its entirety, there is an argument that the Sony hack involved "use of force" under Article 2(4), perhaps even to "armed attack" level under Article 51 of the UN Charter, though traditional weapons and methods were not used and there was no physical damage as currently required by the IGE. Characterizing the hack in these terms has

---

[120] Just as the United States was held responsible by the ICJ in the *Nicaragua* case. *See id.* at ¶ 41.
[121] Schmitt, *supra* note 99.
[122] *Id.*
[123] *Id.*
[124] Ian Brownlie, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 364 (1963).
[125] Nicar. v. U.S., 1986 I.C.J. at ¶ 205.
[126] *See* Romana Sadurska, *Threats of Force*, 82 AM. J. OF INT'L L. 239 (1988).
[127] The object of the threat in the Sony hack was ostensibly *The Interview*, and the ostensible purpose of the threat was to prevent it from being seen by the general public, and for a time the threat had the desired outcome.

generally been avoided by commentators, because of concerns that to do so could result in escalation[128] and/or unwanted repercussions.[129] There is however, a counterargument which is advanced in this paper: that correct characterization of the hack can lead to de-escalation.[130] Rogue states like North Korea (and non-state actors which operate with their tolerance and tacit support) exploit the present lack of clarity and the uncertainty which exists in the application of international law to cyber. In the meantime, law-abiding states are targets for cyber operations like the 2014 Sony hack. The hackers count on the fact that they will not be quickly brought to account by North Korea or the United States; and North Korea counts on the United States not being able lawfully to take effective countermeasures.

As to the scale and effect of the operation, the hackers inflicted damage and the initial damage was as serious as if Sony's U.S. headquarters had been subject to a kinetic attack. The attack involved the use of destructive malware which fundamentally disrupted the corporation's operations. It shut down the Sony system for a week and caused disruption for months. Threats were made to the company and its employees. Data was taken and made available to the public and as a consequence, it harmed Sony, its employees, contractors and others mentioned in the files. The on-going damage to individuals and to Sony through the data revelations, current and future lawsuits, and the overall impact on the business, is the cyber equivalent of timed devices detonating after the initial explosion. The third component of the hack is perhaps the most destructive because it is unknown – how will the information obtained be used against Sony, its employees, contractors and others mentioned in Sony's data files? To use a kinetic analogy, this is the minefield with which Sony, U.S. nationals, and the United States generally, will have to contend for years. No one knows where, when or how they will activate or what damage will be inflicted. This is an important point because Article 51(2) of the *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts,*[131] prohibits "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."[132]

---

[128] *See* Danny Yadron, Devlin Barrett & Julian E. Barnes, *U.S. Struggles for Response to Sony Hack White House Walks Fine Line to Find Way to Retaliate for North Korea's Apparent Attack*, WALL STREET J. (Dec. 18, 2014), http://www.wsj.com/articles/u-s-struggles-for-response-to-sony-hack-1418950806. Reportedly a "former U.S. official said policy makers remain squeamish about deploying cyber weapons against foreign targets." *Id.* "[A]lthough the use of force threshold remains ambiguous, it seems highly unlikely that the international community will characterize operations like that against Sony as such. This hesitancy will be driven in part by concern over the U.S. position (a distinctly minority one) that all uses of force are also armed attacks that allow forceful responses. Some States view the premise as potentially destabilizing in that it allows for an earlier use of force than would otherwise be the case. They will accordingly be extremely reticent about characterizing cyber operations as having crossed that threshold." Schmitt, *supra* note 99. However these comments are coloured by traditional notions of weapons and warfare. As discussed in Section 10, *infra*, the legal requirement of proportionality limits the type of countermeasures that can be legitimately invoked, including those used by a state in self-defense. To be considered proportional and lawful, the response to cyberattacks like the 2014 Sony hack must not have physical consequences even if the Sony hack is considered to be at 'armed' level under international law.

[129] Yadron et al., *supra* note 128.

[130] A similar point has been made by John Norton Moore, though in the context of secret warfare. Moore argues that the ICJ's *jus ad bellum* decisions have "adopted a minimalist approach undermining the Charter and encouraging aggression, particularly aggression in the 'secret warfare' spectrum." John Norton Moore, Jus Ad Bellum *Before the International Court of Justice*, 52 VA. J. INT'L L. 903, 905, 918 (2012).

[131] Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.

[132] The IGE also acknowledge that "[W]hile the notion of attack extends to injuries and death caused to individuals, it is, in light of the law of armed conflict's underlying humanitarian purposes, reasonable to extend

Using the case-by-case assessment agreed by the IGE shows that the 2014 hack was severe, invasive, and its effects were both immediate and are ongoing.[133] The hack does not have a military character in its traditional sense, but this may be because it is unfamiliar. Section 9 below raises the question whether this is the first example of a new type of state-sponsored cyberwarfare.

The observation has been made that the United States expected this type of operation in relation to national resources such as water and electricity but did not anticipate a major U.S. corporation to be a target.[134] This type of activity nevertheless has the potential to undermine the nation's systems including its economy and its national security. Cyber is changing the nature of warfare, including its targets and the type of damage which can inflict harm. The hack does not *appear* to be a military operation, and that gives the adversary the initial tactical advantage of surprise and then uncertainty as the target tries to determine the legal nature of the operation and its lawful response.

## VIII. THE 2014 SONY HACK AS THE NEW FORM OF 'ARMED ATTACK' UNDER INTERNATIONAL PUBLIC LAW

Michael Schmitt maintains that although the Sony hack was "…highly disruptive and costly, such effects are not at the level most experts would consider an armed attack." [135] But is that really the case or does the Sony hack just not look like an armed attack as we know it?

If Sony had been attacked by North Korea using traditional weapons like explosives, there would have been no doubt that it was an attack on the United States, and it would have been condemned by the international community. In this age, digitally stored data and information is just as significant to a country like the United States as its physical infrastructure, probably more so in view of the country's reliance on information technology. When the 2014 hack is viewed in this way, there is no doubt about its seriousness and its destructive power and that it is much more than just a breach of data security and of corporate and individual privacy or that it is an espionage or intelligence gathering operation.

In determining the true nature and extent of the 2014 Sony hack, analogy is made to a kinetic attack as discussed above in Section 8. It is illustrative to consider the 2014 Sony hack in that context, for two reasons. First, by expressing the Sony hack in these more familiar terms, it is generally easier to grasp its true nature and effect. Secondly, because international law principles are based on the traditional LOAC and the desire to avoid it, seeing how the Sony hack fits with those traditional principles assists in correctly characterizing it.

The 2014 Sony hack has not been viewed as the cyber equivalent of a kinetic attack because the damage and injury suffered are intangible. It is a problem that pervades the law at present as it struggles to change and adapt to a new era. The conceptual difficulty is evident in the requirement under *Clapper v. Amnesty International* that "actual" injury must be suffered or impending; and it is also apparent in the application of the traditional LOAC and

---

the definition to serious illness and severe mental suffering that are tantamount to injury" (emphasis added). TALLINN MANUAL, *supra* note 65, at 108.

[133] TALLINN MANUAL, *supra* note 65, at 74.

[134] *See* Chris Strohm, *Sony Hack Signals Threat to Destroy Not Just Steal Data*, BLOOMBERG BUSINESS (Dec. 4, 2014), http://www.bloomberg.com/news/articles/2014-12-04/sony-hack-signals-emerging-threat-to-destroy-not-just-steal-data.

[135] G.A. Res. 2625 (XXV), *supra* note 89.

the Tallinn Manual to attacks where there is damage and injury, but it is not physical.[136] It is however, a leap that the law, particularly international law, can and should take to reflect the reality of the information age, and the strategic importance of all data including that stored and used by the corporate sector.

The international law as it applies to cyber is as yet unclear so states look for guidance and at present the Tallinn Manual guides state practice. The IGE agree that a cyber operation causing physical damage is a breach of sovereignty. It involves use of force and depending on the scale and effect, can amount to an armed attack.[137] However the situation is much less clear when the harm is intangible. This is because the original Tallinn Manual largely follows the ILC Articles which are mired in principles developed for another era, primarily to deal with kinetic attack.

In the original Tallinn Manual the IGE "agreed that it is not the status of an action's target that qualifies an act as an attack, but rather its consequences. Therefore, acts of violence, or those having violent effects, directed against civilians or civilian objects, or other protected persons or objects, are attacks."[138] Significantly, as mentioned above, the IGE also agree that states can make case-by-case assessments of cyber operations,[139] but at present the flexibility of this approach is undermined by the requirement for physical damage.

Considering that the Tallinn Manual is widely consulted by states – including by the United States – in dealing with cyber, the result is that an operation like the 2014 Sony hack falls into a grey area. Yet it is clear that the Sony hack is a wrong and that it caused, and continues to cause, harm. The difficulty is that the features and consequences of the hack do not apparently fit the traditional model of a kinetic attack causing physical damage.

There is a fundamental problem in trying to view cyber operations in these terms. It fails to recognize the new power and value of data and information as both a target and a weapon.

## IX. COUNTERMEASURES UNDER INTERNATIONAL PUBLIC LAW

An internationally wrongful act entitles the injured state to engage in countermeasures under international law. This right is recognized in Article 22 and Articles 49-54 of the ILC Articles. Countermeasures are actions which can be used by an injured state to persuade a rogue state to return to lawfulness. Countermeasures can only be taken by States. Sony could

[136] There is not yet consensus amongst the IGE as to the categorization of cyberattacks that do not cause physical damage.

[137] Some members of IGE went further, to focus not on the nature of the harm caused, but its severity. In their view, a sufficiently severe cyber operation, such as that resulting in a State's economic collapse, can qualify as an armed attack.

[138] TALLINN MANUAL, *supra* note 65, at 93.

[139] Considering such factors as severity, immediacy of effect, invasiveness and military character. This approach is pragmatic and is in line with modern day realities, but the IGE's view of the actions of individuals is strangely out of step. Rather than concentrating on the nature and effect of the attack, the IGE is divided over whether an individual conducted an armed attack. While some consider that if the effects of the actions met the scale and effect test then actions of individuals could rise to the level of an armed attack, others were of the view that cyberattacks conducted by individuals were only governed by the criminal law.

not have, of its own accord, lawfully responded against North Korea with its own cyber operations. That response is only available to the United States.[140]

North Korea declared release of the film *The Interview* an act of war, and this declaration was followed by a destructive cyberattack against Sony, a U.S. corporation. In these circumstances, the United States has a right under international law to respond. The United States can lawfully respond with countermeasures, subject to strict limitations which include notice,[141] proportionality[142] and necessity.[143] These principles are illustrated by the possible response of the United States in late December 2014 whereby North Korea's Internet connectivity to the outside world was progressively degraded over a period of twenty-four hours to the point where the country was completely offline.

The 2014 Sony hack is at least an intervention. Characterizing the Sony hack as an intervention dictates the type of response North Korea experienced in late December 2014. Progressive shutdown of North Korea's Internet connection was in effect 'a shot fired across the bow.' It signaled to North Korea that its actions would not be tolerated and indicated the ability of the United States to respond.

The United States has neither admitted nor denied involvement, however. The official announcement, from the State Department was, "We aren't going to discuss ... publicly, operational details about the possible response options or comment on those kind of reports in any way except to say that as we implement our responses, some will be seen, some may not be seen."[144] State Department spokeswoman Marie Harf stated that U.S. authorities agreed that North Korea was responsible for the Sony hack and should therefore pay compensation. Harf said the United States was discussing a range of options in response to the Sony hacking but would not state publicly what action was planned.[145] If, as is suspected, the United States was behind the loss of Internet connection in North Korea, it is a response which perfectly illustrates the type of countermeasure that an injured state like the United States can lawfully take in response to a cyber operation like the 2014 Sony hack. The United States complied with the requirements for lawful countermeasures. The United States gave notice that it considered North Korea to be responsible for the 2014 hack, that it was unlawful, and that the

[140] A state can outsource lawful cyber countermeasure to a private entity, but then the latter acts as an agent of the state and the state assumes legal responsibility for the act and its consequences.
[141] *See, e.g.*, Iran v. U.S., 2003 I.C.J. at ¶¶ 73–76. This requirement has been criticized however as having no basis in law in relation to the right to self-defense. *See* William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 295 (2004).
[142] Proportionality relates to the size, duration and target of the response. Proportionality is not considered to require an equivalent operation, same weapon or level of force. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 150-55 (3d ed. 2008). Only action necessary to stop the threat can be used. Self-defensive measures can be used to halt and/or repel attack but must not be retaliatory or punitive. The General Assembly has made it clear that reprisals are unlawful. *See* G.A. Res. 2625 (XXV), *supra* note 89; G.A. Res. 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, at 12 (Dec. 21, 1965).
[143] Even if proportionality indicates that an injured state can respond with force, the requirement for necessity prohibits the use of force except when the victim state determines that non-forcible measures will not effectively stop the threat.
[144] *North Korea hit by mass internet outages as debate rages over Sony Pictures hack*, ABC NEWS (Dec. 23, 2014), http://www.abc.net.au/news/2014-12-23/north-koreas-internet-totally-offline-after-sony-hack/5984580.
[145] *Id.*

United States would respond proportionally.[146] Most significantly, it signaled these aspects without use of force. This is important to satisfy U.S. obligations under international law.

Use of force is generally prohibited under international law, although there are several established exceptions. Those exceptions include force sanctioned by the U.N. Security Council under Chapter VII, Articles 39, 42 and 48, the right to self-defense under Article 51 of the U.N. Charter, and anticipatory self-defense. Anticipatory self-defense is especially important in the cyber context where time is of the essence, as it was in the 2014 Sony hack.

To legitimately invoke the right of anticipatory self-defense there must be "*necessity* of self-defense, instant, overwhelming, leaving no choice of means and no moment for deliberation in accordance with the *Caroline t*est."[147] Consequently, anticipatory self-defense cannot lawfully be used for an attack which has occurred. However, where there are a series of escalating incidents as happened in the 2014 Sony hack, the United States could have invoked this right to prevent further attacks.

Similarly, if the Sony hack is considered to constitute a "use of force" rising to the level of an "armed attack," the United States would have been entitled to respond forcefully under Article 51 of the UN Charter[148] and customary international law. In both cases, however, this does not justify use of force in its traditional form. In the case of a cyberattack which is considered to be of "armed" level, the United States lawfully could have invoked only a proportional cyber response.

What constitutes a proportional cyber response in these circumstances is, like most international law as it applies to cyber, largely undeveloped and, consequently, uncertain. Ironically, however, it is clear that to be considered proportional, a lawful response to a cyberattack like the 2014 Sony hack must not have physical consequences.[149]

## CONCLUSION

[146] President Barack Obama said the hack was not an act of war, and promised an unspecified "proportionate" response. *Obama says Sony hack was not 'an act of war,'* NEWSNET (Dec. 21, 2014), http://australia.news.net/article/2521435/obama-says-sony-hack-was-not-an-act-of-war.

[147] See note of US Secretary of State Daniel Webster dated 24 Apr. 1841, in Caroline Case, 29 British and Foreign State Papers (1841) 1137–1138, http://avalon.law.yale.edu/19th_century/br-1842d.asp. The *Caroline* test is a 19th-century formulation of customary international law. The test takes its name from the *Caroline* affair.

[148] Article 51 does not specifically require that the armed attack be committed by a state. Article 51 states that: "[N]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." This is unlike Article 2(4) which refers to a use of force by one "Member" against "any state," Article 2(4) states that "[A]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

[149] This is an important area for development by the LGE in Tallinn Manual 2.0.

The United States' 2010 *National Security Strategy* cites cyber threats as "one of the most serious national security, public safety, and economic challenges we face as a nation."[150] That view is now supported by the events in 2014, especially the 2014 Sony hack.

The pattern continued in 2015. In March of that year the State Department reported that its unclassified network was hacked. That month Anthem, one of the country's largest health insurance companies, reported a hack that exposed the data of as many as 80 million customers.[151] Most recently, the reported hack of the Office of Personnel Management (OPM) computer networks exposed the personal information of 21 million federal employees and contractors.[152] The OPM hack is particularly concerning because it exposed personal information, including biometrics, of persons who have security clearances and who are working in classified areas, as well as the personal information of their families.[153]As was the case for the 2014 Sony hack, the impact extends well beyond the impact on the privacy of an innocent individual and beyond the scope of domestic criminal law. In a country like the United States, which is now heavily dependent on digital networks, this type of activity has the potential to undermine the nation's systems and economy and its national security.[154]

Declaring cyberattacks a "national emergency" in January 2015, President Obama signed an executive order allowing for further sanctions against North Korean targets, following the 2014 Sony hack. The executive order permits the United States to impose financial penalties on those thought to be behind the attacks.[155] The order allows the secretary of the Treasury, in consultation with the Attorney General and Secretary of State, to impose financial sanctions – such as freezing of assets and prohibition of commercial trade, on individuals or groups responsible for malicious cyberattacks that "create a significant threat to U.S. national security, foreign policy, or economic health or financial stability of the United States."[156]

---

[150] This is a significant development because the information obtained goes beyond obtaining credit card numbers. Unlike a credit card number, which can be quickly changed, digital identity information—such as a person's full name, gender, and date and place of birth—is fundamental and enduring. The information stored by a health insurer enables a person's digital identity to be re-constructed and provide answers to challenge questions to get into bank and other online accounts where "forgotten password" options can be used to reset passwords. This enables a person's accounts to be taken over, for new accounts to be opened in the innocent person's name, and for the use of real identities as a cover for criminal and subversive activity.

[151] Jen A. Miller, *Health insurance companies prime targets for hackers*, CIO (Mar. 20, 2015), http://www.cio.com/article/2899488/data-breach/health-insurance-companies-prime-targets-for-hackers.html.

[152] Raya Jalabi, *OPM hack: 21 million people's personal information stolen, federal agency says*, THE GUARDIAN (July 10, 2015), http://www.theguardian.com/technology/2015/jul/09/opm-hack-21-million-personal-information-stolen.

[153] James Rogers, *Why the OPM hack is an ongoing cyber headache*, FOXNEWS (July 14, 2015), http://www.foxnews.com/tech/2015/07/14/why-opm-hack-is-ongoing-cyber-headache.

[154] There are early indications of the impact on government revenue from the Anthem hack, for example. Anthem has warned customers who may have been hacked to file their federal and state tax returns as soon as possible. Hackers could possibly file false tax returns in their victim's name using the stolen information and claim bogus refunds. The U.S. Treasury has encountered this type of activity, and in 2014 the IRS tightened its anti-fraud procedures and now shares intelligence about bogus filings with state revenue departments. However there is still potential for major impact on state revenue because there are forty-six states in which taxpayers can file an "unlinked return," meaning they can file a state return without having a file a federal return at the same time. *See* Miller, *supra* note 151.

[155] *See* Julia Edwards & Jason Lange, *U.S. slaps more sanctions on North Korea after Sony hack*, REUTERS (Jan. 5. 2015), http://www.reuters.com/article/2015/01/02/us-northkorea-cyberattack-sanctions-idUSKBN0KB16U20150102.

[156] *Id.*

While diplomacy and economic sanctions are options, alone they are unlikely to have the desired effect on a state like North Korea. International law, however, has a significant role in suppressing acts of aggression and other breaches of the peace and in maintaining national and international security. As the analysis in this paper shows, international law is capable of providing a range of lawful responses, but new thinking is needed to recognize the true nature of these attacks.

The 2014 Sony hack breached U.S. sovereignty, and it was a wrongful act under international law. The hack can certainly be categorized as an intervention in the state's "political, economic, social and cultural system, and the formulation of foreign policy."[157] The hack also involved at least the threat of force and arguably, although not in familiar form, an attack to armed level which entitled the United States to invoke the right to anticipatory self-defense.

As Professor Michael N. Schmitt, Director of the Tallinn Project, states in his Introduction in the Tallinn Manual:

> "One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent. After all, at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal regime."[158]

[157] Nicar. v. U.S., 1986 I.C.J. at ¶ 205.
[158] TALLINN MANUAL, *supra* note 65, at 17.