Spring 5-22-2021

Bridging the Realms Between Cyber and Physical: Approaching Cyberspace with an Interdisciplinary Lens

Lena Andrea Rose

Bridging the Realms Between Cyber and Physical:

Approaching Cyberspace with an Interdisciplinary Lens

Lena Rose

lrose11@fordhdam.edu

B.A. International Studies, International Track

Fordham University – Lincoln Center

Thesis Advisor: Dr. William Akoto

Seminar Advisor: Dr. Christopher Toulouse

December 2020

Abstract

This project investigates the use of cyber technology as a political tool through the investigation of the following case studies: (1) The Sony Pictures Hack in the United States in 2014, (2) The Qatari News Hack in 2017, and (3) China's enactment of the Hong Kong National Security Law in 2020. These three case studies depict that rapid technological advancement has led to greater cyber warfare between state powers. The Sony Hack examines political coercion, the Qatari Hack examines disinformation, and the Hong Kong National Security Law examines surveillance and suppression of opposition. As a result of an increasingly complicated cyberspace, cyberwarfare and physical warfare are becoming more enmeshed. Solving cybersecurity challenges requires a diverse pool of experts who can draw from multiple different disciplines, such as sociology, political science, and public culture. The means for protecting one's data is no longer limited to code. Upon demonstrating how states use cyber technology to gain political influence, this project concludes with speculations and suggestions as to how the cybersecurity field must be addressed in the future.

Keywords: *cyber conflict, cyberspace, cyberwarfare, espionage, surveillance, national security*

Table of Contents

Introduction

Historically, only major powers—the most affluent and militarily powerful—could effectively compete in cyberspace. The field itself was defined by the few states that could afford to play. These competitive environments were understood to be where the quest for power lay in international relations. Today, cyberspace is no longer limited to the global superpowers, and it is near impossible to discuss national security without reference to cyber threats. In a digitalizing world, cybersecurity and technology are becoming more prominent in the political context.

Sometime between June 2012 and June 2013, during what Adam Segal refers to as "Year Zero," a new era of geopolitical movements in cyberspace emerged. As a result, information and communication networks became ingrained into our political, economic, and social ways of life. Since then, we have seen significant implications for security, data privacy, and cyber laws. We must conclude that cyber conflict will only become more belligerent, and the risks will be more consequential as the Internet becomes more embedded in day-to-day life. Within cyberspace, every piece of data that is put onto the Internet is of interest because of its sizable effects in the physical world. Technology is becoming more accessible and cheaper to use, which leads to greater vulnerability online and increased cyber warfare.

While some attribute the deterioration in the cybersecurity environment to investment or infrastructure, I argue that the most crucial aspect of handling cybersecurity is addressing the subject more holistically with a political and sociological background. Recent years have shown that although we continue to invest billions into cybersecurity, we still see more sophisticated cyber-attacks each year. There are two main reasons for this. First, the rules of cyberspace and cyber warfare are not the same as physical or conventional warfare. In traditional military conflict, one must consider geographical distance or state borders. The laws and concepts of the

virtual world cannot compare to the cyber realm and its infinite proximity. Second, the cybersecurity field is still evolving, and it is complicated to make sense of it. We still do not know the answers to many of the important questions, such as what is the responsibility between governments and private actors in cyber defense? What should we base international cyber norms on? What laws and policies can hold individuals, organizations, and state governments accountable across international boundaries?

The Sony Pictures Hack, Project Raven, and the Hong Kong National Security Law are explored in this thesis as three individual case studies that exemplify how cybersecurity tools are used as new methods to engage in political warfare. The Sony Hack best exemplifies how a data breach was used to coerce and threaten a corporation that mocked its ruler. The Qatari News Hack demonstrates how cyber tools are used to spy and influence regional politics. Lastly, the Hong Kong National Security Law shows how digital media acts as a new platform for protestors; additionally, this case study demonstrates the use of cybersecurity tools in censoring and surveilling anti-government opposition. In compiling this thesis, I argue that cybersecurity is a broadening interdisciplinary field that needs to consider behavioral approaches to best define the nature of cyberspace challenges. In completing this thesis, my findings support prior research that concluded that increased digitalization, technological advancement, and developing cyber-enabled information warfare have led to greater competition in cyberspace.

Methodology

Importance of Case Studies – Significance

The case studies that I have chosen for this project explore how state powers employ cyber technology to influence and sway regional and international politics. These case studies also explore the effects of digitization in international relations. My case studies on North Korea and the United Arab Emirates demonstrate how the emerging cyberspace permits small states to compete on the same playing field as global superpowers such as the U.S., China, and Russia. Additionally, the Hong Kong National Security Law case study investigates digital media as a mechanism to publicize domestic affairs to a global audience, as well as how that mechanism can be censored by digital suppression. All three case studies share the common trait of employing their respective technologies to pursue geopolitical aims. Due to the ongoing fluctuations in cybersecurity developments, I found it most useful to gather data from sources from 2014 and onward. More importantly, I would like to use my thesis as an opportunity to suggest ways to move forward in the cyber realm.

A scientific or technical approach to handling cybersecurity challenges could help enrich an understanding of how intrusions occur. This paradigm alone, however, does not encompass the political or sociological motives for hacking, espionage, and disinformation, which I argue is the most crucial aspect to understanding cyberspace. In other words, the problem is not always a weak code or poor security, but what provoked the attack or action in the first place. I believe that North Korea, the UAE, and Hong Kong best exemplify this argument because they highlight the critical theme of a desire to protect state reputation. International Studies challenges us to critique the human actors, whether they are individuals, hacker groups, or entire nation-states. I find this the most useful way to approach cybersecurity challenges. Aside from investing in

security development, cybersecurity requires understanding the human context in its political and social atmosphere.

Method of Organization

This paper will first outline the previous scholarly work on conflict in cyberspace. The literature review will develop a theoretical framework to make sense of the case studies presented in this project. More importantly, this literature review will strengthen my claims as to why there is a need to research this specific topic. Afterward, the case studies of The Sony Hack, the Qatari News Hack, and the Hong Kong National Security Law will be discussed with graphics to guide in telling each story. For each country, a background of the case study will be outlined, and key themes will be explored. Next, the analysis section will be broken into three subsections: reputation as a motivator for cyber warfare, establishing political influence through the use of technology, and the impact of the ongoing coronavirus pandemic on cybersecurity. Finally, the conclusion will summarize the arguments discussed and outline future questions to be researched in cybersecurity and political science.

Limitations

The first and the most pressing limitation is that most of the sources concerning the case studies do not focus on human weaknesses when discussing the foundations of the event. Many cybersecurity experts only point out the fatal flaw of human error in not safeguarding their electronic devices or security infrastructure. As stated, cybersecurity tends to be dominated by programmers with experience only in technology and engineering, despite many cyber-attacks having a political or social motive. This can make it difficult to recognize the real reasons behind particular hacks, as sometimes the issue is not the security element but the action that prompts it. Indeed, one can install and implement all the necessary security protocols, but there is not, nor will there never be, a 100% hack-free device in this world. Data breaches are like cybersecurity's Kryptonite. Research that discusses the complicated relationship between cybersecurity, international relations, and political science does not yet seem to be a major focus in the field. I hope to shed more light on conflict in cyberspace and offer speculation as to how to improve the cybersecurity environment in the future.

This research refers to digital censorship, disinformation, and political propaganda. It is possible that I have not uncovered all parts of my case studies if any material was concealed from the public domain. Certain countries with state-run media, such as North Korea and the UAE, have different reporting frameworks than independent media outlets. Adding to my previous statement, another limitation of this thesis is that some of the cited sources were pro-Western. For example, one of the books that I mainly used in this research is Adam Segal's book *A Hacked World Order*. Segal does an excellent job at laying out the relationship between geopolitics and international relations but spends a good majority of his book critiquing the lack of freedom of digital privacy in non-democratic regimes. Due to the limited time to complete this

thesis, I cannot go into depth on the regime types of each of my case studies. It would be interesting if I were to examine how regime type influences the use of cyber tools, as the three countries in this study score "low" on the Freedom Index.

My last limitation of this project is that these case studies are relatively recent and still developing. The books and research journals I found provide broad ideas of cyber warfare as it continues to evolve. The Hong Kong National Security Law is so recent from the completion of this thesis that most of the sources I could use for these two case studies are blog posts and news reports. Additionally, it was just reported as of December 2020 that there are talks of resolving the Gulf crisis with Qatar. I am hopeful that over time, especially after the COVID-19 pandemic, more works may be published on these subjects as they are still ongoing and relevant to today.

In an increasingly competitive international landscape, cybersecurity becomes harder to manage as nation-states continue to use technology for political gain. Comparisons in the cyber field are imperfect because each nation-state has its own idea of what is acceptable, which may lead to variations in international norms. Cybersecurity is often perceived as an alternative form of warfare—with the possible exception of the U.S. and China—but not a main strategic actor in international relations. This project aims to bring awareness to the great potential that cybersecurity will have, and has had already, in an increasingly digital world.

Literature Review

Contribution to Scholarship

The purpose of the literature review is to position my work in relation to what others have already done, specifically Nazli Chocuri's "Cyberpolitics in International Relations," Adam Segal's "Hacked World Order," and Fabio Rugge's chapter in "Confronting an Axis of Cyber," "An Axis Reloaded?" As there is minimal research on the intersection of political science and cyberspace, I will draw my conclusions to how cybersecurity and politics intersect with the help of few trusted scholarly sources. Building upon previous research, I collected data on each of these books and analyzed how each author's framework connects to my own research. I aim to contribute to the discussion of cyberspace conflict in international relations while demonstrating that my research addresses a gap in analyzing human behavior in cybersecurity.

Nazli Chocuri's "Cyberpolitics in International Relations"

Nazli Chocuri's book "Cyberpolitics in International Relations" explores cyberspace as a new competition field in the international landscape, one that transcends traditional territorial, governmental, social, and economic constraints of conventional or militarized warfare.[1] Chocuri is an expert in international relations and cyberpolitics; in this book, she pays special attention to the transformation in the cyber domain and the rise of digital technology. She discusses how this understanding crosses into political science, power, and influence.

> *Cyberpolitics*, a recently coined term, refers to the conjunction of two processes or realities — those pertaining to human interactions (politics) surrounding the determination of who gets *what, when, and how,* and those enabled by the uses of a virtual space (cyber) as a new arena of contention with its own modalities and realities.

[1] Nazli Chocuri, "Cyberpolitics in International Relations," 6.

The seven characteristics that Chocuri lays out in her book help to define the development of cybersecurity and growing opportunities for competition and conflict, which are crucial elements to politics and the pursuit of power. In recent years, what was initially considered a neutral sphere of open interaction—created by technological advancements flowing mainly from the West—is a tool of influence.

All three case studies connect to Chocuri's Table of Characteristics in different ways. In my first case study that discusses North Korea and the Sony Hack—a prime example of political coercion—physicality, fluidity, and accountability allow North Korea to execute its extensive hack on Sony Pictures in response to Sony's intended release of "The Interview," a film that critiques and mocks the North Korean Supreme Leader Kim Jong Un. North Korea is granted a significant advantage when carrying out offensive attacks, but this is not just because the hack was attributed to a shadow hacker group and not the North Korean government directly. North Korea's distant geographical location from its adversaries, in conjunction with the lack of communication technology within the civilian population, make it much easier for them to bypass mechanisms of responsibility and deny allegations made against them. In many ways, the physicality element of cyberspace is a defining characteristic of the Sony Pictures Hack.

The initial goal of Project Raven in the UAE was to monitor any malicious activity, such as terrorism, against the Emirati government. Today it is best known as a confidential initiative to surveil and spy on regional opponents. My second case study concerning the Emirati government's Project attack on Qatar ties into Chocuri's characteristics attribution, fluidity, and instantaneity. When the UAE hacked into the Qatari News Agency's website and planted evidence that Qatar's emir was in support of Iran, this prompted an instant response from the rest of the Gulf states to blockade Qatar. The Gulf's regional politics shifted beyond what the Arab

Spring did in ways that disrupted Middle Eastern security, redefined state sovereignty, and stirred chaos in the region. After Saudi Arabia, the UAE, and Bahrain first imposed diplomatic blockades on Qatar, Project Raven ramped up its cyber-attacks against Qatar and its media targets[2] but claimed no responsibility for the attack that helped spark the ongoing Gulf Crisis.

Hong Kong is in a unique position because it is a semi autonomous island that is connected to China under a "one state, two system" philosophy. Tying back to Chocuri's Tables of Characteristics of cyberspace, permeation and participation can be seen in this case study. Permeation is a clear characteristic to the Hong Kong case as social media has become a battleground in Hong Kong's protests, enabling activists to spread word to the rest of the world about China's anti-democratic infiltration into the region. Social and digital media in Hong Kong is being used to enhance participation in activism against the Chinese Communist Party, though the use of technology on China's part has censored this online activism in cyberspace.

Adam Segal's "The Hacked World Order"

Politics is about exerting influence and control to gain advantage. The Internet is a crucial part to the emerging global communications infrastructure, which enables actors to use digital technology for carrying out political agendas. Adam Segal identifies technology as a new form of warfare, noting that even private companies are at the forefront of cyberspace. Out of the three case studies, Segal's book only mentions the Sony Pictures hack of 2014. In "The Hacked World Order," Segal classifies the Sony Hack as "a narrative thriller and parable"[3] attributing North Korea's success on their geographic location and lack of communication technologies within the country. Segal identifies that because of the U.S. underestimating North Korea's offensive and

[2] Schetman and Bing, "Former NSA spies hacked BBC host, Al Jazeera chairman for UAE."
[3] Adam Segal, "Hacked World Order," 62.

defense cyber capabilities, the issue dragged on longer than it should have. As the Sony Pictures hack gradually unfolded during the week of Thanksgiving of 2014 and into December, North Korea became a forefront figure in international cyberspace. The Sony Hack was bold and daring, to say the least. One of the elements to cyber power that Segal identifies is "rapaciousness,"[4] which North Korea possesses. However, the attack was not meant to advance economic interest. Rather, the main motive was to embarrass and hurt Sony Pictures Entertainment from afar.

For a cyber-attack on a private corporation to receive worldwide media attention was particularly rare and alarming for that time. When Sony officially canceled the movie release of "The Interview," this prompted a direct response from former President Obama. He stated that it was wrong for Sony to back down because the attack undermined U.S. values of "freedom of expression" and national security. Segal notes that, had Sony not withdrawn the movie, Washington likely would not have made an official response against the attack, and the hack would not have been as unique. Information Security expert Mathew Schwartz also echoes the sentiment that pulling "The Interview" was exactly the wrong thing to do, since there was no credibility to the Guardians of Peace's threat. "It's the kind of response you get when you don't have a plan."[5] Instead, Sony's response only empowered the hackers to go a step further.

Fabio Rugge's "An 'Axis' Reloaded?"

A great challenge of cybersecurity is attributing cybercrime to a specific person or group, especially when it comes to state-sponsored hacks. Cyber-attacks allow high-ranking officials in government as well as intelligence agencies to masquerade as common cybercriminals. In other

[4] Adam Segal, "Hacked World Order," 42-43.
[5] Schwartz, "Sony's 7 Breach Response Mistakes."

words, it is difficult to figure out who is really behind a virtual attack. Fabio Rugge writes the introductory chapter titled "An Axis' Reloaded?" in the book "Confronting an Axis of Cyber" on cyberspace behavior, values, norms. He highlights that the current confrontation in cyberspace is translating, at the international level, into a massive "security paradox." This is because cyber strategies differ by state and are sometimes perceived as aggressive or offensive, or the results of using such technologies can have detrimental effects in real world politics.

Defining rules and international cyber laws for a state's cyber behavior is an absolute priority, especially when it comes to the use of force and coercion in cyberspace. This suggestion is brought up by Rugge, arguing that that the low level of public awareness of cyber-enabled information warfare (CEIW) is "understandable but worrisome."[6] He discusses the 2016 U.S. Presidential Election as an example; when Russia meddled in the 2016 Presidential elections' debate, the massive data leaks catalyzed a DNC scandal that eroded trust in American institutions. However, despite the hack's severity in altering the course of American politics, it still failed to raise the public's understanding of "the true nature of cyber threats and of the potential impact on international security." [7] This is because cyberspace is the "domain of ambiguity," where it is impossible to anticipate the scope of a virtual campaign without considering strategic, political, or social contexts.

Rugge marks 2008 as a critical year, where the first use of cyber-attacks in military operations were used during the Georgian War. Since then, various cyber-attacks have been carried out in the ongoing presence of international crises. The Qatari News Hack—a case study in this thesis– is mentioned as one of these cyber-attacks; the ongoing Gulf dispute in the Middle East quickly escalated after the alleged false statements from the UAE were planted on the

[6] Cyber-enabled information warfare describes the overlap of cyberspace into traditional and conventional strategic warfare and operations.
[7] Fabio Rugge, "Confronting an Axis of Cyber?", 14.

Qatari news website. As a result of Qatar being blockaded by Saudi Arabia, the UAE, Bahrain, and Egypt, tensions rose when Qatar ultimately sought out Iran and Turkey for assistance, the enemies of the U.S.-led Middle Eastern coalition against the Islamic State.

Rugge's key point is that technological innovation is transforming societies at a rapid rate that public opinions and foreign policymakers are unable to keep up with. If we are to effectively manage cyber challenges in the political context, then we must recognize the cyber realm and the "real world" are growing more interconnected and what the consequences of using technology can have.

Case Studies

The Sony Pictures Entertainment Hack

On November 24, 2014, Sony employees who logged onto their desktops that morning were greeted with the sound of digital gunfire and a sinister image of a red skeleton with the title "Hacked By #GOP." Below the title read a grim message:

> We've already warned you, and this is just a beginning. We continue till our request be met. We've obtained all your Internal data including your secrets and top secrets. If you don't obey us, we'll release the data to the world. Determine what will you do till November of the 24th, 11:00 PM (GMT).

A shadow hacker group, claiming themselves as the "Guardians of Peace" (GOP), carried out one of the most devastating cyber-attacks on an American private institution by sabotaging the system's computers and stealing over 100 terabytes of data using wiper malware[8] and releasing that sensitive information to the general public. Though politically motivated attacks and theft of intellectual property are not new, this case study stands out amongst others because it drew an unprecedented U.S. response. What was first seen as an amateur cyber hack ultimately catalyzed a series of actions for U.S. national security.

The GOP demanded that Sony cancel its then-upcoming political satire film, "The Interview." The film, which stars James Franco and Seth Rogen, is about two journalists hired by the CIA who attempt to assassinate Kim Jong-un, who is parodied by actor and comedian Randall Park. When the film was still being made in the summer of 2014 by Columbia Pictures, Korean officials expressed disdain over the movie as releasing such a film would constitute an act of "the most undisguised sponsoring of terrorism as well as an act of war." A spokesman

[8] Malware is malicious software intended to infiltrate another user's computer to leak, steal, or manipulate data.

from the North Korean Ministry of Foreign Affairs commented that "if the United States administration tacitly approves or supports the release of this film, we will take a decisive and merciless countermeasure."[9] The spokesman did not elaborate on this statement but noted that Washington was guilty of "provocative insanity" and tainting the North Korean supreme leader's image. Pyongyang also wrote a letter of complaint to the Secretary-General of the United Nations to stop the production. Michael Lynton, then Sony's chief executive, said when Sony officials called the State Department, they were told it was just more "bluster."[10]

GOP hackers reportedly gained access to Sony's networks from the inside by stealing a key password from an employee in Sony's IT department, likely a system administrator who had broad access to the computer systems. The GOP's technique of gaining the password is not entirely certain. Still, many speculate it was shared through a spear-phishing attack, a social engineering tactic intended to steal data. After the Sony hack was publicized later in November, several American journalists requested comment from the GOP. One GOP member, who called themselves "Lena," told a CSO Magazine reporter that "Sony left their doors unlocked, and it bit them." Lena added that "[Sony] doesn't do physical security anymore,"[11] which made it much easier for the GOP to plant the malware.

Although Sony's security systems were already weak, it is clear that the Sony hack was carefully executed and well thought out. The release of the stolen data came out gradually by week. On November 27, three days after employees found the message on their computer screens, five Sony films—four of which had not been released—were uploaded to an online file-sharing hub for free streaming to the public[12]. Following the release of these films on

[9] Sang-hun, "North Korea Warns U.S. Over Film Mocking Its Leader."
[10] Sanger, "The World Once Laughed at North Korean Cyberpower. No More."
[11] Bort, "How the Hackers Broke into Sony And Why It Could Happen to Any Company."
[12] Risk Based Security, "A Breakdown and Analysis of the December, 2014 Sony Hack."

December 1, the pre-bonus salaries of Sony's top 17 executives were leaked, as well as personal information of more than 47,000 former and current Sony employees. The information uncovered from the data itself caused major upset as the numbers indicated a sizable gender pay gap between male and female employees and actors. Sony hired the FBI's cybersecurity firm, SealMandiant, to investigate, but stolen data—from celebrity aliases, Sony workplace complaints, to passport and visa information—was still being released day by day in batches.

On December 5, the GOP emailed Sony employees threatening to harm them and their families if they did not sign a statement renouncing the company. As word of this message got out to the public media, people began to panic. Despite the paranoia, however, it should be understood that the length of the Sony Hack can be attributed to the poor responses. James Franco, who hosted *Saturday Night Live* the night after the threat, mocked the hackers in an opening monologue:

> Something pretty crazy happened this week. I have this movie called 'The Interview' coming out at Sony and this week Sony Studios got all their computers hacked. This is true. These hackers have leaked real personal information about everybody that works at Sony. Social security numbers, e-mails, and I know eventually they're going to start leaking out stuff about me. So, before you hear it from someone else, I thought it would be better if you hear it from me. Soon you'll know that my e-mail is CuterThanDaveFranco@AOL.com. My password is 'LittleJamesyCutiePie' — and this is all just a real violation of my personal life.

The Christmas release of "The Interview" was canceled, following another email sent on December 16, 2014 from the GOP that contained terroristic threats. "The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the [theaters] at the time. (If your house is nearby, you'd better leave)." While many thought that

it was a relief to pull the plug on the movie premiere, others, specifically President Barack Obama, were disappointed that Sony listened to the GOP's commands. "I'm sympathetic to the concerns they faced. Having said all that, I think they made a mistake."[13]

On December 19, 2014, the FBI's cybersecurity firm, SealMandiant, linked[14] the Sony Hack to North Korea. Though they claimed they could not share all details concerning the report for confidential reasons, they laid out three points asserting their argument: (1) Technical analysis of the data deletion malware was linked to other malwares that the FBI can confirm were used by North Korea; (2) The IP addresses[15] were associated with North Korean infrastructure; (3) The tools used in the hack were similar to the South Korean bank and media hacks made by North Korea in March of 2014. Although the North Korean government continually denied the allegations that they were behind the attack, the U.S. Department of the Treasury imposed economic sanctions on North Korea in January of 2015, which further intensified tension between the U.S. and North Korea.

The severity of the hack was not realized at first. As Buchanan puts it, "Sony executives apparently talked to United States officials after the North Korean saber-rattling, but neither side seemed overly concerned about the possibility of North Korean escalation."[16] The BBC also quotes a tech expert wrongly predicting that the Sony hack would be less detrimental than the 2011 hack on Sony's PlayStation. Wee Teck Loo, head of consumer electronics research at Euromonitor, told the BBC: "This time around, I don't believe that there will be massive damage, save for Sony's ego, even if the hack is real." While there was clear significant financial loss to the studio, what made the breach so catastrophic wasn't the hack itself but the series of

[13] Diamond, "Washington Outraged Over Sony Decision."
[14] Federal Bureau of Investigation, "Update on Sony Investigation"
[15] IP address stands for Internet Protocol address, which is a numerical label associated with a computer that identifies a user on the Internet.
[16] Ben Buchanan, "The Hacker and the State," 167.

events that unfolded. The breach of confidentiality and failure to secure information led to dozens of lawsuits against Sony Pictures. Below is a graph that demonstrates the data leaks and the data destruction were the two most damaging aspects.

The embarrassing secrets and of a successful multibillion-dollar entertainment company were exposed, which led to financial and legal issues that lasted for years. As the focus of the attack was centered on the public gossip about the film industry, the Sony Hack became a worldwide phenomenon. Backlash was particularly directed towards Sony producer Scott Rudin, when emails exchanges between Rudin and co-chair of Sony Amy Pascal were released. In the emails, Rudin described famous actress and activist Angelina Jolie as a "minimally talented spoiled little brat" after Jolie wanted David Fincher to direct Jolie's film, "Cleopatra". "YOU BETTER SHUT ANGIE DOWN BEFORE SHE MAKES IT VERY HARD FOR DAVID TO DO JOBS," Rudin said in one email, referring to Jolie.[17] Rudin also took aim at actress Megan Ellison when he referred to Ellison as a "bipolar 28-year old lunatic" who needed to take her meds. The Sony hack also showed emails disclosing racially insensitive remarks against former President Barack Obama, which caused mass criticism from high-profile celebrities like Kevin Hart and Shonda Rhimes. Pascal—while discussing breakfast at which she would be meeting President Obama—jokingly asked[18] Rudin if Obama likes the movies "DJANGO" and "The Butler," two movies centered around black men.

The Sony Hack was the start of an era where digital technologies became a choice of weapon for political coercion. Given the relative weakness of its military, and its distant geography from its Western adversaries, North Korea chose to instigate and carry out irregular cyber operations as part of their strategic objectives to steal data. "While we have yet to witness

[17] Stedman, "Leaked Sony Emails Reveal Nasty Exchanges and Insults."
[18] Holpuch, "Sony Email Hack: What We've Learned about Greed, Racism, and Sexism."

the extremes of cyberwar, the more subtle danger since 2016 is the way states like Russia and North Korea use cyber-strategies as a form of political warfare."[19] When cyberwar becomes the normal state of affairs on the Internet, states must determine what the proper response to these attacks are since they are virtual and not physical. For the U.S. to retaliate in any way to a cybersecurity breach on a private institution is alarming and can be traced back to a merge between the cyber realm and the physical realm.

In hindsight, the Sony Pictures Hack demonstrated that some of the most aggressive cyber attacks were not driven by military, security, or financial motive but by an intent to coerce another power into doing what they want. The relative easiness and inexpensiveness of technology has helped in aiding this process. "You don't need that much money to invest in cyber warfare," says Martin Libicki, senior management scientist with the Rand Corporation. "It is really a people thing, not a money thing," he adds.[20] North Korea only has a small GDP and a thousand or so specialists dedicated to cyber warfare. Cyber-attacks are easier to perpetrate and send messages. The aftermath of the data breach left us with chilling concerns about the long-cherished right to free speech, and whether that right would have its consequences. The breach was a turning point in cyber that even a renowned global entertainment corporation could be the victim of a cyber-attack.

Qatari News Agency Hack

In the Sony Hack case study, I examined how cyber tools are used for (political) coercion. In this second case study, I will look at the use of Project Raven in the UAE's hack of

[19] Valeriano, et.al., "Analysis: Cyberwarfare Has Taken a New Turn. Yes, It's Time to Worry."
[20] Suciu, "Why Cyber Warfare Is So Attractive to Small Nations."

the Qatari News Agency. This case study primarily demonstrates how cyber tools are used to spread disinformation[21] and conduct espionage on state adversaries.

When news broke that the Qatari emir vocalized support for Iran and the Islamic state, it caused a frenzy in the Middle East. On May 24 of 2017, a post was found on the Qatari News Agency (QNA) website, Qatar's official government media outlet, with a statement claiming to be attributed to the Qatari Emir, Sheikh Tamim bin Hamad Al Thani. The statement, officially calling Iran an Islamic power and speaking positively about the Palestinian militant group, Hamas, was allegedly planted by hackers from the United Arab Emirates. The "fake news" that was posted in this state-sponsored hack whipped anger against its smaller Gulf neighbors and catalyzed an ongoing Gulf Crisis. The hack occurred just three days after President Donald J. Trump visited Riyadh during his tour of the Middle East.

On June 5, 2017, Saudi Arabia, Bahrain, Egypt, and the UAE cut all diplomatic and transport ties with Qatar, accusing the state of financing Islamist militant groups, supporting terrorism, and allying with its Shiite rival, Iran—the Gulf states' regional adversary. The Qatari government said its emir had never given the statement and that QNA was hacked. Despite Qatar's protests, its neighbors—already suspicious of Qatar for supporting terrorism—quickly acted by blocking Qatar from the rest of the Gulf. When ties were officially severed, the blockading countries demanded Qatar to call back all diplomats and cancel all means of transportation, communication, and trade with them. The reports about the alleged statement were broadcasted all over Saudi Arabian government outlets. Additionally, the UAE shut down all Qatari media broadcasts inside its borders, including Al Jazeera, the most-watched satellite network in the Arab region. The day after diplomatic relations in the Gulf were severed, U.S.

[21] Disinformation is different from misinformation in that disinformation typically refers to political or government propaganda.

Defense Secretary Jim Mattis called for negotiations between the Gulf states to resolve the situation, however this was not successful.

On July 16, 2017, the Washington Post released an article asserting that the UAE was responsible for orchestrating the hacking of QNA and attributing the false statement to the Qatari emir.[22] U.S. intelligence agencies, including the FBI and the CIA, and British law enforcement officials found that members of the Emirati government discussed the disinformation plan and its implementation with Egypt and Saudi Arabia. Yousef al-Otaiba, the UAE Ambassador to the United States, stated to the Post that the article was false. "The UAE had no role whatsoever in the alleged hacking described in the article," the statement said. "What is true is Qatar's behavior. Funding, supporting, and enabling extremists from the Taliban to Hamas and Qadafi. Inciting violence, encouraging radicalization, and undermining the stability of its neighbors."[23]

In a separate Reuters report, investigators uncovered that Project Raven operatives sprang quickly into action and launched operations to break into the Apple iPhones of at least ten journalists and media executives they believed were colluding with Qatar or the Muslim Brotherhood. "The goal, the former Raven operatives said, was to find material showing that Qatar's royal family had influenced the coverage of Al Jazeera and other media outlets, and uncover any ties between the influential TV network and the Muslim Brotherhood."[24] BBC host Giselle Khoury, the chairman of Al Jazeera, Hamad bin Thamer Al Thani, and other prominent Arab media figures were reportedly spied on by Raven operatives. The UAE's security officials used a surveillance tool called Karma to surveil and steal information from the intended targets. Karma was dangerous because hackers could obtain personal information by uploading phone

[22] Al Jazeera, "UAE arranged hacking of Qatari media: Washington Post."
[23] DeYoung and Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials."
[24] Schetman and Bing, "Special Report: U.S. hackers helped spy on Al Jazeera chairman, BBC host."

numbers or email accounts into an automated targeting system. The UAE purchased Karma from an unknown source.

The UAE and Qatar have been engaged in a "tit-for-tat hack-and-leak"[25] operation for years. Tensions between the UAE and Qatar can be traced back to 2013 during a power struggle in Egypt. When Qatar allied with the Egyptian Islamist movement after the Arab Spring, the UAE backed a military takeover that cast the Islamists into prison. Each side has been accusing the other of cyber espionage for years, leading to multiple lawsuits and strained Gulf relations. Perhaps the UAE and its allies needed to find a legitimate reason to cut ties with Qatar and were willing to plant false information to carry this out. A few months after the rift began, U.S. Secretary of State Rex Tillerson intervened to stop Saudi Arabia and the UAE from invading Qatar militarily.[26] Though the U.S. is allied with the blockading countries, it has strong relations with Qatar.

The UAE hack on Qatar signaled a broader transformation in cyber espionage. It is a clear sign that cyberattacks and disinformation campaigns are no longer the exclusive domain of sophisticated powers of Russia, China, and the U.S. Like North Korea and the Sony Hack, cyber-attacks are no longer limited to Western or first-world countries because technology is becoming more accessible and affordable as the digital era becomes more present in everyday life. The rapid advancement of this technology creates an increasingly competitive cyberspace where small states such as the United Arab Emirates hold power to sway Middle Eastern politics to the point where the U.S. steps in to mediate. Many small states, especially in areas where hiring hackers is easy, find that cyber war provides a greater return than actual investment in conventional weapons. Amy Chang, a research associate in the technology and national security

[25] A tit-for-tat hack-and-leak is used to characterize actions and reactions in arms race contexts. In the context of international relations, it is a retaliation against a state to punish them for wronging them.
[26] Asmar and Hasaj, "Just How Important Is the Rift Between Qatar and the Saudi-Arabia Led Quartet?"

program at the Center for New American Security, states that cyber warfare is an excellent alternative to conventional weapons because it is cheaper and far more accessible, especially for small nation-states. Essentially, it allows these countries to pull off attacks without the risk of retaliation or getting caught.[27]

This news hack is not the first time where the UAE attempted to meddle in other state's affairs. In 2016, Reuters uncovered documents that revealed that the UAE had been using cyber tools to monitor other targets aside from the Qatari emir. These included a senior Turkish official Deputy Prime Minister Mehmet Simsek, Oman's head of foreign affairs Yusuf bin Alawi bin Abdullah, the Saudi Prince, and even American citizens from abroad. Ex-NSA Lori Stroud confirmed as a former Project Raven operative that foreign adversaries such as Iran, Qatar, Turkey, and individuals who criticized the monarchy, were the main targets.[28] According to documents reviewed by Reuters, Raven was largely staffed by U.S. intelligence community veterans who were paid through an Emirati cybersecurity firm named DarkMatter.[29] DarkMatter did not respond to the numerous emails and phone calls requesting comment. The NSA also declined to comment on Project Raven.[30]

Besides Israel, the UAE has developed a reputation as a tech hub in the Arab world, attracting investments in computing from large tech corporations such as Microsoft. The UAE is a prime example of how Gulf monarchies are increasingly outsourcing defense and security work. The fact that the UAE was able to garner support from former NSA methods, knowledge, and tools for use by their own intelligence purposes is alarming. The UAE also recruited

[27] Suciu, "Why Cyber Warfare Is So Attractive to Small Nations."
[28] Schetman and Bing, "Inside the UAE's secret hacking team of mercenaries."
[29] In 2016, DarkMatter replaced CyberPoint as a contractor for Project Raven, the Emirati government's confidential initiative to surveil adversaries.
[30] Schetman and Bing, "UAE used cyber super weapon to spy on iPhones of foes."

graduates of the Israeli military's cyber unit, offering lavish salaries and properties to the individuals.

The Qatari News Hack case study demonstrates the power of disinformation. The Emirati government's use of cyber technology enabled them to sanction off and isolate Qatar from the rest of the Gulf states. The planting of fake statements engineered what would be one of the greatest modern Gulf crisis. "The Emiratis needed a trigger to spark the crisis and this was it."[31] A hack of the QNA is also a striking example of a cyber-attack in shaping Middle Eastern politics. The UAE readily denies the allegations that they attacked the Qatari news site to this day, despite evidence that the Emirati government has been spying on Qatar since 2016 and had prior political tensions dating back to the formation of Al Jazeera.

Hong Kong National Security Law

The Sony Hack and Qatari News Hack case studies were examples of security breaches. They examined how technology and digital media enable small powers to sway domestic and international politics through hacking. It was clear who the perpetrators of the hack were and who the victims were. In this third case study, I will examine Hong Kong's national security law to discuss how the People's Republic of China uses cyber technology to carry out political and economic initiatives over Hong Kong through censorship and surveillance.

In 1984, thirteen years before the handover of Hong Kong, China and Britain signed a treaty that declared China and Hong Kong would be under the principle of "one country, two systems," otherwise known officially as the Sino-British Joint Declaration of 1984. Since the Hong Kong Special Administrative Region of the People's Republic of China's (HKSAR) handover from British rule in 1997, they thrived under the authority of China but in a "one

[31] Hardwood, "Qatar Hack: Middle East Is the Worst Place in the World for Fake News."

country, two system" concept that was implemented in Basic Law, Hong Kong's de-facto establishment. The declaration enshrined the city's capitalist system and granted it a high degree of autonomy. It also helps them to reintegrate Taiwan, Hong Kong, and Macau with mainland China while preserving their own political and economic systems.[32] During this time, Hong Kong had been trying for years to pass a security law; it was unsuccessful due to an inability to reach a consensus. However, the semi autonomous region's standing as a stable international financial center and gateway for global capital has risen above China, making it a populous city for multinational corporations and foreign investors.

On June 30, 2020, the Standing Committee of China's National People's Congress imposed a security law at 11:00 PM, just an hour before the 23rd anniversary of the city's handover to China from the British. With little input from local Hong Kong officials, this new security law established a wide-reaching security apparatus with the power to crack down on a range of political actions deemed harmful to the Chinese government and the Chinese Communist Party (CCP). The law is now incorporated into Hong Kong's "mini-constitution," the Basic Law, but the details of the law's sixty-six articles were not revealed until after it was passed. The Hong Kong democracy campaigner Joshua Wong spoke out in a series of tweets[33] after his political party, Demosisto, was disbanding:

> [The security law] marks the end of Hong Kong that the world knew before. From now on, #HongKong enters a new era of terror, just like #Taiwan's White Terror period in history, with arbitrary prosecutions, black jails, secret trials, forced confessions, media clampdowns and political censorship. With sweeping powers and ill-defined law, the city will turn into a #secretpolicestate.

[32] Albert and Maizland, "Democracy in Hong Kong."
[33] Wong, Joshua. Twitter Post. June 29, 2020, 10:41 PM.

The new Hong Kong law criminalizes secession, subversion, terrorism, or collusion with foreign forces with maximum life sentences in prison, resembling mainland China's own laws. Both Chinese and Hong Kong laws include punishments for people "suspected" of inciting hatred against the government, with no elaboration. Roger Creemers of Leiden University in the Netherlands says that "vagueness is a governing tactic"[34] for China's authoritarian regime. Strict punishments, which acted as a deterrent, are core to China's control over Hong Kong. Beijing will establish a new security office in Hong Kong with its own Chinese law enforcement personnel. Under the new law, Chinese officials can arrest any protestor and sentence them to life and without bail. Additionally, the law would allow for new Chinese national security agencies and formal secret police authority. Hong Kong can establish its own national security commission but with a Beijing-appointed advisor. The city has long cherished the independent judiciary, a remnant of the British colonial rule that stood in stark contrast to China's secretive, party-controlled courts. Now, Hong Kong must address its cases according to mainland Chinese law, where the penalties for violation are often harsh. There are now questions as to whether Hong Kong will be permanently stripped of free speech and public communication.

Hong Kong's civil unrest began when talk of plans—which did not end up happening—that would allow extradition from Hong Kong to mainland China had spread to the public. What started as a single peaceful demonstration has snowballed into a wider pro-democracy movement, demanding state autonomy and self-rule. The urge to push for democratic reform and investigate alleged cases of police brutality followed through city-wide protests which, in turn, sparked mass upheaval for a fight to protect democratic institutions. Last year in 2019, anti-government demonstrators in Hong Kong bombarded police stations and surrounded Chinese government buildings. Some Hong Kong protesters have called upon the

[34] Cadell, "In Hong Kong National Security Law, Echoes of China's Own Cyber Crackdown."

U.S. in their support for democracy and freedom by waving American flags to symbolize pro-democracy and free speech. A stronger pro-democracy protest presence would also empower the U.S. government to impose sanctions on Chinese or Hong Kong officials deemed to be undermining that autonomy or committing human rights abuses.

On May 22, 2020, an explanation of the National People's Congress' (NPCSC) request for authorization to create new national security legislation for Hong Kong was released. NPC Vice Chairman Wang Chen cited growing risks to China's national security in the city since the outbreak of the anti-extradition bill protests in June 2019. Wang stated that the forces that were "anti-China" were calling for Hong Kong's independence from China, self-determination, and for a referendum on Hong Kong's future.[35] When explaining China's decision to establish a national security law, he accused that the protesters:

> …openly insulted and defaced the national flag and emblem, incited Hong Kong people to be anti-China and anti-Communist Party, besieged the Central People's Government's institutions stationed in Hong Kong, discriminated against and excluded people from mainland China in Hong Kong; deliberately undermined social order in Hong Kong, violently confronted police enforcing the law, damaged public facilities and public property, and paralyzed the governance of the government and the operation of the Legislative Council.

The Hong Kong national security law raises questions as to how China is using cyber technology to censor and surveil Hong Kong, as well as how technology might be used to sway Chinese politics. Many are afraid that Hong Kong's judicial independence will be trampled and that the city's legal system will soon resemble one of China's, one with no right to free expression. "It is clear that the law will have a severe impact on freedom of expression, if not personal security, on the people of Hong Kong," notes Professor Johannes Chan, a legal scholar

[35] Lawrence and Martin, "China's National Security Law for Hong Kong: Issues for Congress."

at the University of Hong Kong.[36] The law blurs the line between software developed for national security and for individual or personal use.

Donald Trump and the White House did not say too much on the new Hong Kong law, but there have been actions to address it. On November 22, President Trump made a comment on "Fox & Friends" where he signaled support of the protestors but also pointed out his trade deal with China. In fact, Trump also spoke warmly about Xi, calling him "an incredible guy" and "a friend of mine,"[37] while also crediting his trade negotiation as the reason why Hong Kong was not already obliterated. Eventually, on November 28, 2019, Trump signed the Hong Kong Human Rights and Democracy bill, which requires the U.S. government to impose sanctions against mainland China and Hong Kong officials responsible for human rights abuses against protestors. The bill received bipartisan support in the Senate and the House of Representatives—signaling support for self-determination in Hong Kong. In the eyes of the Trump administration, the Hong Kong matter is a second-tier issue compared to trade with China and North Korean and Iranian nuclear threats. However, China has and continues to repeatedly blame the protestors on foreign interference in the city.[38] In an indirect way, this case study exemplifies China's attack on Western ideology.

Hong Kong's protesters are using their available tools to bring heightened awareness not just to cybersecurity but to Chinese-Hong Kong relations. This has allowed us to recognize how unique and so far-fetched in that the law can apply to anyone, anywhere in the world. The law's expansive scope will especially make it difficult for data and tech companies to conduct business. Donald Clarke, a law professor at the George Washington University, noted that the

[36] Cheung and Hughes, "Why Are There Protests in Hong Kong? All the Context You Need."
[37] Swanson and Crowley, "Trump Says He's 'Standing with Xi (and With Hong Kong's Protestors)."
[38] Baker, "China is set to pass a draconian new law in Hong Kong that would effectively stifle all dissent. Here's what could happen to the people in the city."

law claims "extraterritorial jurisdiction" over every person on the planet.[39] Essentially, the law is broader in scope than China's own criminal law. So, how willing are technology and financial platforms to stand up to the Chinese government, particularly when their assets are at stake? Companies like Google and Facebook halted accepting requests for data from Hong Kong authorities, while TikTok, a Chinese-owned platform, has already decided to entirely pull out of the region. "If companies like Google and Facebook refuse to comply, they could be fined thousands of dollars, and their local employees may be sent to prison for up to six months."[40] Since the rules also extend beyond Hong Kong's borders, Facebook could be compelled to produce information about a user in the U.S. if Hong Kong authorities deemed their posts a threat to China's national security.

While China uses its resources to keep eyes on the citizens of Hong Kong, citizens in Hong Kong are fighting back by using technology to galvanize international support, hide organizer's identities, and mobilize demonstrations. In a CNBC article, Tracy Loh, senior lecturer of communication management at Singapore Management University, stated: "what has changed now is that social media is used to win the hearts and minds of the people. Both sides are using images of police brutality and/or protester brutality to further their own agendas."[41]

The case study of Hong Kong asks a crucial question: what is the balance between individual rights and state interests in the digital age? Looking at the consequences of this new law, the latter seems to outweigh the former. The use of digital technology to suppress and control flow of information is a common theme throughout Chinese cyber realm. Enforcing the 2017 Chinese Cybersecurity Law onto Hong Kong would be illegitimate; however, this law—in addition to many others related to digital technology— could be slowly introduced by starting

[39] Clarke, "Hong Kong's National Security Law: A First Look."
[40] Chan, "The One Element of Hong Kong's New Security Law That Concerns Business the Most."
[41] Shao, "Social Media Has Become a Battleground in Hong Kong's Protests."

with access to data, security and localization requirements for citizens' and organizations' data, and critical infrastructure protection measures. When President Xi assumed the presidency, he focused on consolidating his power through an anti-corruption campaign that would continue to this day. As more people had access to the Internet in China. Xi responded by creating small interest groups dedicated to cybersecurity policy issues, a key instrument for Xi to exercise greater control over the huge Chinese bureaucracy.

Discussion and Analysis

The discussion and analysis portion of my thesis will offer speculations and suggestions for each of the case studies. In conducting research for this thesis, I would like to argue how much International Studies has to offer; not just to the computer science and cybersecurity fields but to all academic disciplines. International Studies offers a new way of critical thinking. The application of the International Studies lens to cybersecurity allows one to take a step back to see a bigger picture, which, in turn, can unveil the true nature of modern cyber challenges.

International Studies Interdisciplinary Table

Economics	History
Sociology	Political Science

Your Reputation Precedes You

Max Weber defined power as the chances that an individual in a social relationship can achieve their own will in spite of resistance.[42] Those with limited or diminishing power may act to gain control over certain resources. Weber's theory certainly applies to this thesis as power and reputation were the driving forces in each case study examined. I argue that aside from proper practice, one should consider the reputational risks which come from two essential factors: the speaker and the status. One must also consider the consequences that can follow from the use of technology in the context of societal engagement and public engagement. North

[42] Warren, "Max Weber's Nietzchean conception of power," Vol. 5 No. 3, 19.

Korea's rage against Sony was caused by Sony's intention to tarnish North Korea's image as a country not to be messed with. The wrong thing to do was to make a movie mocking North Korea in the first place. The Kim family's cult of personality, which only began after Kim II-sung took power in 1948, shows this; if one does not show "proper" respect for the regime, there would be consequences. In regards to the UAE case study, demonstrates the extent to which the UAE, alongside Saudi Arabia, were unwilling to tolerate any deviation from its vision for this region and the lengths to which they would go to. After the election of former U.S. President Donald Trump, the UAE likely saw the new American presidency as an opportunity to start asserting power in the Middle East. With the momentum of paranoia and panic in the Gulf, it started the hashtag trend "القطع العالقات مع قتر," or "cut relations with Qatar," bringing more attention to Qatar's fake statement. Similar to the UAE, China wanted to maintain a secure grasp of their domestic security, and the way to do this was through a security law that would limit any anti-government protest. With the overthrow of the Qings in 1912 and the Chinese Civil War, the Chinese are especially keen on keeping control of the population.

North Korea, the UAE, and China all share a characteristic of going to great lengths to maintain their reputation from foreign adversaries. North Korea's method was coercion; the UAE employed a disinformation tactic; and China used digital surveillance and oppression on the semi autonomous region of Hong Kong. All three countries used cybersecurity tools as a means for political purpose which, in turn, has created a new and murkier cyberspace. Based on the findings of this research, I conclude that cybersecurity must be viewed holistically or with an interdisciplinary lens outside of computer science for solving issues that cannot be solved with a simple code. Cybersecurity is only perceived as a technical field that is dominated by computer scientists and engineers with limited knowledge of public culture or social dynamics. The

hackers and spies behind the cyber tools learn to adapt and improve their techniques for the future, so it is important to understand where the root causes for cyber conflict are coming from.

Controlling the Media Narrative

In the 1930s, the U.S. welcomed the radio, which quickly became a golden phenomenon. By the start of World War II during 1939, nearly 28 million American households owned radios to receive their news. Eventually, this shifted when the 1960s and 1970s ushered in a new era of digital technology. Both technologies had such large attraction because it was an excellent way of uniting communities, especially during WWII, The Cold War, and the Vietnam War. What should be noted from this is that people could only really receive their news in one form; unlike today, where we can choose where we get our information from, the spectacle of news was pretty uniform. In "Confronting an Axis of Cyber" James Lewis' chapter "Defining Rules of Behavior for Force and Coercion in Cyberspace" states part of the reason why it was easier for nation-states to come together in earlier times was because the world was recovering from various world wars that overwhelmed the international system. "This is not 1945 when there was widespread consensus on the need for stabilising institutions, nor is it 1975, when Cold War opponents were ready to reach accommodations to increase stability."[43]

The technological advancements in the 40 years between the 1930s and the 1970s is astonishingly different from those between the 1970s and the 2010s. Today, anyone with a device has the ability to control "the minds of the masses," in the words of Malcom X. Media scholars classify the press as "the fourth estate" [44] exemplifying the considerable influence that the press had on public affairs. In England, this term was first used in Parliament as a group to be

[43] James Lewis, "Defining Rules of Behaviour for Force and Coercion in Cyberspace," 174.
[44] Poklandik, "How the Media Controls the Narrative and Us."

added alongside the nobility, the clergy, and the commoners. Essentially, what makes the Internet so unique in this case is that online processes functioned as a mode for narrative control, which differs from conventional or military warfare in that it is much more abstract.

The idea that media is one of the most potent entities proves absolutely true in this thesis. Seeing Sony suffer horribly while controlling what the world saw was far more rewarding for North Korea than hacking the multinational entertainment corporation itself. North Korea's goal of preventing the movie from being shown had not followed as planned, but the hack's outcome almost certainly exceeded their expectations. The same can be said for the UAE and the planting of statements on the Qatari News Agency's website. The UAE case study shows us a declining hierarchy of knowledge; one message brought an entire region into chaos, unveiling the underlying issues that the Middle Eastern already had in the Gulf coast. With the Sony Hack and Project Raven, these examples show that cyberspace allows diplomats and state governments to masquerade as cybercriminals. Lastly, Hong Kong's use of technology, both on the protestor and the police force side, is the best example of technology being used to narrate the battle for public opinion. The Internet has become a token of political geography where online participation was crucial to the success of the Hong Kong protests. China's live news feeds, action information, and "intelligence" collected through cybersecurity surveillance have also shown us China's attempts to uphold societal discipline and unity.

COVID-19 Pandemic and Moving Forward

This year, the world navigated the stress and devastation of a deadly COVID-19 pandemic. The pandemic inevitably interrupted a normal way of life and led to months of lockdown in all fifty U.S. states. As we continue to stay at home and limit ourselves from large

social gatherings and other grand events, the use of communication platforms, such as Zoom and Google Hangouts, has risen exponentially. COVID-19 has also contributed to e-commerce with the adoption of online shopping and increased social media usage. With a greater reliance on digital technology to conduct everyday tasks, we have also become increasingly vulnerable to cybercrime.

Cybersecurity threats are estimated to double from $3 trillion to $6 trillion (USD) a year by 2021, and the number of cyber-attacks has increased five times worldwide after the COVID-19 outbreak.[45] With the heightened emotional states, individuals are more susceptible to falling for email scams such as ransomware attacks and phishing scams. On a much larger scale, there have been multiple cases of cyber hacks from Russia and China on the U.S.'s COVID-19 research. The pandemic has ultimately created a new set of practices in cyberspace, both domestically and internationally, which will ultimately have an impact on the ongoing Gulf Crisis and Hong Kong Security Law.

Out of all the three case studies, the COVID-19 pandemic is most relevant to the Hong Kong National Security Law. The Hong Kong law came amidst the coronavirus pandemic, and during the time of its announcement, the U.S. was very much distracted in handling their rising COVID-19 cases. With China's desire to draw out foreign influence from Hong Kong, the timing of the national security law actually makes a lot of sense since their adversary, the U.S., was distracted by a global health crisis. The impeccable timing on China's part makes it more difficult to undo and much harder for Hong Kong to gain back their state sovereignty. Combatting any form of Chinese human rights abuses will require more than just the declaration of the Hong Kong Human Rights Bill. Given the U.S.' relationship with China, and depending

[45] See the 2020 Official Annual Cybercrime Report.

on the new presidency of the U.S. come inauguration of Joe Biden in 2021, strict economic sanctions actually may be the most effective method.

Conclusion

Three teachable lessons can be learned from these case studies. Time, effort, and finances that are spent on information security should be increased; second, risk analysts should consider the social and political repercussions; lastly, do not put anything on your computer that would want others reading. Sony especially received this wakeup call too late and could not resolve their errors. Common computer hygiene and security practices such as updated software and security patches, avoiding phishing scams, and using anti-virus software, can and should be supported. However, these practices are inadequate to avert persistent and sophisticated attacks, such as those from North Korean hackers.[46] Cybersecurity is a dynamic process involving human attackers who continue to adapt and quickly learn from their mistakes. Attacks can be endlessly inventive when motivated. As a result, cybersecurity needs people better versed in public culture and social dynamics. The history of cyberspace is relatively short, but the pace of history is rapidly accelerating as technologies, and more importantly the hackers, improve and develop.

The cyberspace grants a new way to achieve strategic advantage, particularly for small and developing powers. Whereas in the physical realm there are threats of nuclear catastrophe and warfighting, the cyber realm offers the ability to manipulate flow of information without risk of physical warfare, at least not quite as much. In one instance, the Israeli Defense Forces bombed the Palestinian cyber headquarters in Hamas in 2019 after a brutal fight between Hamas in Gaza and Israel.[47] The number of events that show merging between cyberspace and the physical realm will continue to increase. Simple and static approaches are not well suited to deal with continued technological advancement, increased access to technology, and changing cyberspace norms.

---

[46] Daniel Pinkston, "North Korean Cyber Threats," 118.
[47] Read Israel Responds to Cyber Attack with Bombs for more details.

Every global power is caught in what the late diplomat George Kennan calls a "perpetual rhythm of struggle," that is, a non-stop conflict between states. The increased access to technology has enabled cyberspace as a new competitive playing field in international relations for smaller powers. However, cyberspace is difficult to navigate because of how increasingly enmeshed it is becoming in international politics and security. Emmy-winning journalist Bruce Sussman describes it best: "…we, as a society, were on a two-lane road. The left lane was the physical world, and the right lane was the cyber world. Now, here we are, passing a sign that says 'Lanes Merge Ahead.'"[48] Alongside further research, international and domestic communities must address the non-technical approaches to cybersecurity. The best way to do this is to employ people in non-technical roles to assist in analyzing cybercrime and risk analysis. While there have been meetings to discuss, cyberspace will still be evolving.

[48] Sussman, "Cyber War vs. Traditional War: The Difference is Fading."

Bibliography

Albert, Eleanor, and Lindsay Maizland. "Democracy in Hong Kong." *Council on Foreign Relations*, Council on Foreign Relations, 30 June 2020.

Asmar, Amir, and Gabriela Hasaj. "Just How Important Is the Rift Between Qatar and the Saudi Arabia-Led Quartet?" *Council on Foreign Relations*, Council on Foreign Relations, 22 June 2020.

Baker, Sinéad. "China Is Set to Pass a Draconian New Law in Hong Kong That Would Effectively Stifle All Dissent. Here's What Could Happen to People in the City." *Business Insider*, Business Insider, 27 May 2020.

Bort, Julie. "How the Hackers Broke Into Sony And Why It Could Happen To Any Company." *Business Insider*, Business Insider, 19 Dec. 2014.

Buchanan, Ben. "Hacker and the State: Cyber Attacks and the New Normal of Geopolitics." Harvard University Press, 2020.

Cadell, Cate. "In Hong Kong National Security Law, Echoes of China's Own Cyber Crackdown." *Reuters*, Thomson Reuters, 7 July 2020.

Center for a New American Security. "Sony Hack Case Example." *The Nextware Sessions*, 2015.

Chan, Veta. "The One Element of Hong Kong's New Security Law That Concerns Business the Most." *Fortune*, Fortune, 16 July 2020.

Cheung, Helier and Roland Hughes. "Why Are There Protests in Hong Kong? All the Context You Need." *BBC News*, BBC, 21 May 2020.

Clarke, Donald. "Hong Kong's National Security Law: a First Look." *The China Collection*, 3 July 2020.

Council on Foreign Relations. "Virtual Meeting: Hong Kong Update-Autonomy and National Security." *Council on Foreign Relations*, Council on Foreign Relations, 12 Aug. 2020.

DeYoung, Karen, and Ellen Nakashima. "UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials." *The Washington Post*, WP Company, 16 July 2017.

Diamond, Jeremy. "Washington Outraged over Sony Decision." *CNN*, Cable News Network, 19 Dec. 2014.

Holpuch, Amanda. "Sony Email Hack: What We've Learned about Greed, Racism and Sexism." *The Guardian*, Guardian News and Media, 15 Dec. 2014.

Lawrence, Susan V, and Michael F Martin. "China's National Security Law for Hong Kong: Issues for Congress." *Congressional Research Service*, 3 Aug. 2020.

Leff, Alex and Emliy Feng. "Trump Angers China by Signing Law Backing Hong Kong Protestors." *NPR*. 28 Nov. 2019.

Lewis, James A. "Defining Rules of Behaviour for Force and Coercion in Cyberspace." *Confronting an Axis of Cyber?: China, Iran, North Korea, Russia in Cyberspace*, edited by Fabio Rugge, Ledizioni LediPublishing, 2018, pp. 161–176.

Pinkston, Daniel A. "North Korean Cyber Threats." *Confronting an Axis of Cyber?: China, Iran, North Korea, Russia in Cyberspace*, edited by Fabio Rugge, Ledizioni LediPublishing, 2018, pp. 89–120.

Pokladnik, Randi. "How the Media Controls the Narrative and Us." *Ohio Valley Environmental Coalition*, 5 July 2019.

Reuters Staff. "UAE Arranged for Hacking of Qatar Government Sites, Sparking Diplomatic Row: Washington Post." *Reuters*, Thomson Reuters, 16 July 2017.

Risk Based Security. "A Breakdown and Analysis of the December, 2014 Sony Hack." *RBS*, Risk Based Security, 5 Dec. 2014.

Rugge, Fabio. "An 'Axis' Reloaded?" *Confronting an Axis of Cyber?: China, Iran, North Korea, Russia in Cyberspace*, edited by Fabio Rugge, Ledizioni LediPublishing, 2018, pp.13-39.

Sanger, David E, et al. "The World Once Laughed at North Korean Cyberpower. No More." *The New York Times*, The New York Times, 15 Oct. 2017.

Sang-hun, Choe. "North Korea Warns U.S. Over Film Mocking Its Leader." *The New York Times*, The New York Times, 25 June 2014.

Schetman, Joel and Christopher Bing. "Former NSA Spies Hacked BBC Host, Al Jazeera Chairman for UAE." *Reuters*, Thomson Reuters, 1 Apr. 2019.

Schetman, Joel and Christopher Bing. "Inside the UAE's Secret Hacking Team of American Mercenaries: Ex-NSA Cyberspies Reveal How They Helped Hack Foes of UAE." *Reuters Investigates*, Thomson Reuters, 30 Jan. 2019.

Schetman, Joel and Christopher Bing. "'Karma': Inside the Hack Used by the UAE to Break into iPhones of Foes." *Reuters*, Thomson Reuters, 30 Jan. 2019.

Schwartz, Mathew J. "Sony's 7 Breach Response Mistakes." *Bank Information Security*, Information Security Media Group, 23 Dec. 2014.

Segal, Adam. “The Hacked World Order”. New York: Public Affairs, 2017.

Shao, Grace. “Social Media Has Become a Battleground in Hong Kong’s Protests.” *CNBC*, CNBC, 15 Aug. 2019.

Suciu, Peter. “Why Cyber Warfare Is So Attractive to Small Nations.” *Fortune*, Fortune, 22 Dec. 2014.

Sussman, Bruce. “Cyber War vs. Traditional War: The Difference Is Fading.” *Cybersecurity Conferences & News*, Seguro World Inc., 27 Dec. 2019.

Stedman, Alex. “Leaked Sony Emails Reveal Nasty Exchanges and Insults.” *Variety*, Variety Media, LLC, 9 Dec. 2014.

Swanson, Ana, and Michael Crowley. “Trump Says He’s ‘Standing’ With Xi (and with Hong Kong’s Protesters).” *The New York Times*, The New York Times, 22 Nov. 2019.

The Associated Press. “List of Demands on Qatar by Saudi Arabia, Other Arab Nations.” *AP NEWS*, The Associated Press, 23 June 2017.

U.S. Federal Bureau of Investigation. “Update on Sony Investigation.” Washington, DC: *FBI*, 19 Dec. 2014.

Valeriano, Brandon, et al. “Analysis: Cyberwarfare Has Taken a New Turn. Yes, It’s Time to Worry.” *The Washington Post*, WP Company, 13 July 2017.

Warren, Mark E. “Max Weber’s Nietzschean conception of power.” *History of the Human Sciences*. 1992;5(3):19-37. doi:10.1177/095269519200500303.

Wong, Joshua. Twitter Post. 29, June 2020, 10:41 PM.