Trouble in Silicon Valley: Cyber Attack Hits the US

Chair: Anna Nguyen
Letter from the Chair

Dear Delegates,

Thank you for taking part in the 2019 Stanford Model United Nations Conference and for getting involved in the key issues of our time: peace, climate action, cyber security, global security, sustainable development and human rights. It is my honour to chair the Cyber Security Committee this year and we will go deep into the relationship between cyber policy and cyber security in relations with national and global security.

Before elaborating further, I would like to make a quick introduction to my background. My name is Anna Nguyen Thuy An. I am currently working on my Master of International Policy under the Freeman Spogli Institute of International Studies at Stanford University. I am also a fellow at the Asia-Pacific Scholars Fund. Prior to joining Stanford, I was working as a
management consultant with a strong focus on digital technology, the Internet of Things, digital transformation and innovation. Therefore, cyber security has always been an important topic in my work. My professional experience spanned over 4 continents: Asia, North America, South America and Europe. I take pride in being a global citizen with exposure to various parts of the world. I earned a bachelor’s degree in Business Administration, Financial Risk Management, from the National University of Singapore where I was a Temasek Foundation scholar.

Our world is changing with an unprecedented pace with ever more complex and interconnected networks of systems and data. This brings an enormous amount of potential applications for the advancement of humanity, and at the same time, immense risk and vulnerability for malicious forces to abuse and misuse. This means, now more than ever, we need the next generation of world leaders and policy makers to not only be familiar with international policy, but also to be well-versed about the intricacies and nuances of the digital world that we are living in right now. Current global leaders have a lot of wisdom and lessons to pass on in terms of international politics and global history, but they are counting on us, the next generation, to push on radical changes to existing policies so as to adapt to the incredible rate of change that we are witnessing every day.

It is exhilarating to think about the vast potential that we, the next generation, are holding in our hands. The speed of development and innovation is unparalleled. I witness new technologies being developed and applied towards the improvement of human lives every single day – it is tough to stay on top and most-updated with all of them. And that is exactly why I am excited to welcome you into the committee to tap on the power of our collective knowledge, to
brainstorm and debate, and to innovate together. On the other hand, with great power comes great responsibility as Stan Lee once said. While I am optimistic about the future that we are building together as an international community, it is also of utmost importance that we prepare ourselves for scenarios that will interfere with the development of humanity as a whole – one of such is the potential misuse of the power of the interconnectedness – people, machines, systems, data – that we have developed. Cyber security is, therefore, one of the most important topics that we, future leaders and policy makers, need to focus on, research and develop a good grasp of.

Given the importance and complexity of the topic of cyber security, I hope you will join me with prior research, foundation knowledge, and your own standpoints and perspectives on the topic. As I mentioned above, given the fast pace of development, no one has all the knowledge in this area, and we are here to tap on our collective knowledge and innovative thinking. I am looking forward to collaborating, debating, and learning from every single one of you; as much as I hope you will learn from the whole committee, from our debates, and that you will be able to obtain meaningful insights that will be useful and crucial for your future career.

You will learn more about the procedure and the details of the Conference from the organising committee directly. Do not hesitate to reach out to them if you have any administrative question.

Remember, the success of this conference is in your hand. And I will see you soon.

Yours sincerely,

Anna Nguyen Thuy An

Email: anna0505@stanford.edu
Note on the Guide & Committee

Welcome to Trouble in Silicon Valley! This committee promises to be one of constant excitement and action, particularly if you as a delegate come in with both knowledge of the general topic and an idea of the role you would like your character to play. Since the realm of cyber war, terrorism, and policy is one that can just as easily focus on the intricacies in hacking and development of technology as it can policy to prevent an attack, I wanted to take a moment to emphasize that you do not need to have a comprehensive grasp of the science behind cyber attacks, nor recognize all of the different types of attacks that can occur. Rather, it would be helpful to use this guide as a primer on such topics, and then as a framework for future research more geared toward strategy and policy. This guide is short for a reason -- it should provide just enough information for you to get a basic grasp of the subject, but it will also leave you wanting to learn more in order to take full advantage of your personal powers as a delegate. In addition, the timeline of the committee will begin by emulating the real world; thus, the start of the committee (and the initial crisis) is Nov. 8, 2019.

In addition, I want to be clear that although there are moments of humor in this guide, and likely interspersed throughout the committee, this topic is quite serious and deals with somber subject material. In attempting to emulate real life, the situations you may encounter throughout the committee may be upsetting for some. We strive to make this conference realistic in order to envision the true consequences of our actions, and work to challenge delegates to step out of their comfort zone and empathize with others who carry vastly different beliefs and opinions. Yet, learning is the key goal, and environments need to feel safe for learning to take place. If you feel at any way uncomfortable during the committee, please reach out to the Dais
staff and we will do everything in our power to help. As a reminder, please be courteous and kind to your fellow delegates; SMUNC has a zero-tolerance policy for any sort of bullying or hate speech.

The Crisis Hits

The date is Nov. 8, 2019. It is 8:30 pm in Washington, D.C. President Trump has just retired to the residence of the White House, applauding himself for a slew of amusing Tweets he’d rattled off throughout his last meeting -- an evening national security update. Not unusually, his habit of sipping a Coke while writing said Tweets meant that he failed to listen to much of the presentation by his various security advisors. Thus, he didn’t notice when Gina Haspel, Director of the CIA, noted that there had been increased chatter on a site within the dark web that was known to be a hub for terrorists interested in cyber crimes. Nor did he notice when Secretary of State Mike Pompeo presented a recent message from President Recep Tayyip Erdogan. Secretary Pompeo noted his confusion as to the many spelling errors Erdogan’s email had, an unusual mistake for the Turkish leader.

Sitting down in front of his flat screen television, President Trump unmutes the perennially-playing Fox News and unwraps a Big Mac graciously left for him on the sparkling Reagan china plate. As he lifts the burger to his mouth, however, he notices the TV has gone blank. Attempts to change channels result in the same slate-gray screen, before a message in cardinal red fills the screen:

“Ready for a game?”

Trump thinks for a beat. Sure, it’s a Friday night; what else is happening?
“Good, so are we. We play like this: you -- the United States, government and citizens -- agree to our terms, or there’s a consequence. The terms? Simple. Remove all US troops stationed outside of the United States. Bring them home quickly, and you win. Take your time, however, and the game gets complicated. For each day that the US government avoids action, we’ll initiate another cyber attack. Power grids, water filtration centers, hospitals, banks, social media -- everything’s up for grabs if you’ve got the right intelligence. And that, we do. You have 24 hours before the next attack…

Good luck!”

It’s not long before advisors are at his door, on his phone, and blowing up his Twitter mentions. The threat has been broadcast throughout every nation-wide television network, and is now getting its third and fourth plays as the anchors who were interrupted by the announcement immediately begin analyzing its content and implications. The video is spreading even quicker through Facebook and Twitter. These same feeds, though, are soon filled with messages of hate and accusation; conspiracy theories mutate and multiply -- was it Iran? Russia? North Korea? A terrorist organization? Incited by Trump himself? More importantly, did the group tamper with anything else? When will the next attack hit?

Soon, further evidence of the group’s capabilities are uncovered. It becomes clear that many of these hateful messages, churning out fake news, haven’t been posted by Americans themselves; accounts across the US have been hacked, with everyone from kindergarten teachers to Bill Gates supposedly Tweeting out calls to violence against minority populations within the country. While those whose accounts have been hacked attempt to shut down their accounts, the messages and their screenshots spread quickly and efficiently. A cacophony of shouts and sirens
careens toward 1600 Pennsylvania; parents begin to take their teens’ phones, fearful of the messages being spread; bottled water and canned goods disappear off of shelves in minutes.

President Trump’s Big Mac, like a Stanford student in 60 degree weather, has gone cold.

**History of the Problem**

Cyber security is, indisputably, integral to the wars of the future; yet, the extent of its influence on international and domestic policy, as well as the day to day lives of everyday citizens, remains to be seen. Even so, the threat’s definition as the key national security challenge of the United States has not translated to abundant discourse on the subject, nor a basic understanding by the civilian population as to what cyber warfare would truly entail.

There are three main categories that are used to describe information attacks using technology: cyber warfare, cyber terrorism, and cyber crime. Although these phrases are often used interchangeably in popular discourse and even by the global media, it is important to recognize the different risks that each of these attacks poses to various populations and infrastructures.

While cyber warfare has gone through multiple shifts in definition, a 1993 RAND study presents one of the earliest analyses of the future of the then-burgeoning technology. It describes the use of improved cyber systems in military operations, noting the potential to improve reconnaissance and intelligence gathering while also infiltrating and disrupting computers that control critical technologies.¹ As access to -- and fundamental reliance on -- computers has grown, this power has only increased; individual people, companies, cities, and federal

---

governments are all susceptible to cyber attacks. As of February 2019, 74% of US adults own a desktop or laptop computer,² while 81% own some form of smartphone.³

A case study of Estonia provides a prime example of the catastrophic consequences of such reliance on technology without proper security measures in place. In 2007, the country was hit with a series of distributed denial of service, or DDoS, attacks. DDoS attacks are some of the most common and highest-profile attacks because they can use only a few tools to take down entire websites or servers. In Estonia, the attacks mirrored intense internet traffic, prompting Estonian banks, government websites, and media outlets to be a few among many of the online sites to be taken down. The attack did its job: meant to provoke confusion and panic, yet remain below the marker of an armed attack, Russian forces fostered a sense of insecurity within Estonia and the larger region -- a response to Estonia’s removal of a Soviet-era statue out of the capital. The Russian government has been linked to similar attacks since 2007, including attacks on the nation of Georgia as a hybrid with traditional military forces.

The more recent use of cyber warfare against Ukraine, in fact, provides a lens into future conflicts. Russia has managed to trigger blackouts in central cities like Kiev, delete government documents, and render the railway companies’ booking systems useless at the high point of the holidays. Most destructive, however, has been the release of an automated worm virus called NotPetya. The worm spread to roughly ten percent of Ukrainian computers and incapacitated Ukrainian society; encrypting documents and demanding ransoms, the attack caused massive shutdowns of institutions like banks and airports, disarray of hospitals, and a massive

immobilization of government agencies. Even more, due to the nature of cyber warfare, it spread beyond Ukraine and infiltrated networks across the world, including the United States and France. In fact, the United States has estimated that NotPetya cost a total of $10 billion in total damages.⁴

Today, most definitions of cyber warfare cite it as a conflict in cyber space between two nations. However, it’s become increasingly clear that non-state powers also maintain the capacity to inflict massive harm on governments. Moreover, hacking and cyberwarfare represent more than just a threat to state security. Private companies, from Twitter to Sony⁵, have been hacked, resulting in varying degrees of damage. While presenting a threat to the security of information, these attacks also present a severe financial cost to the targeted companies and governments. Water distribution systems, oil refineries, hospitals, tech companies -- all are vulnerable, to various degrees, to devastating attacks by state and non-state actors.

All of the above risks are even greater magnified when it comes to cyberterrorism. With terrorism defined as “the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change,” cyber terrorism represents the same end goal through different means.⁶ The “pursuit of political change” here is key to the difference between cyber terrorism and cyber warfare, in addition to the emphasis on threats of violence. While there

is still debate as to if an act of cyber terrorism has even taken place as of 2019, potential future situations could include:

- Attacking air traffic control systems to collide multiple civilian planes;
- Changing formulas for prescriptions at pharmaceutical companies;\(^7\)
- Targeting certain populations and stealing money and personal information, fomenting distrust and instability throughout communities.

This list is not nearly comprehensive, but merely provides an idea of the route that such acts of cyberterrorism could take in the future.

**Policy and Protection**

As evidenced above, prominent public and private institutions now face the threat of cyber attacks on a daily basis. As such, both sectors are increasingly raising concerns regarding cybersecurity and how international policy can be utilized to protect countries and citizens against these attacks. Microsoft President and Chief Legal Officer Brad Smith has pioneered the creation of a “Digital Geneva Convention,” which he claims would consist of a “legally binding agreement that will ensure a stable and secure cyberspace.” The company’s 2017 policy paper calls for public-private partnerships between governments, the technology sector, and civil society groups to pave a way for the creation of such a convention. While the idea has been embraced by many in the humanitarian action realm, there remain key questions as to how the convention would jive with current standards of international law, which are largely based on 20th-century notions of state sovereignty and borders. Since cyberspace has few true “borders,”

protection from and retribution for attacks under international human rights law would be complicated at best.

The potential convention also brings into conversation the current US strategy to combat cyber warfare. In its annual “Worldwide Threat Assessment of the US Intelligence Community,” the Office of the Director of National Intelligence notes cyber threats as the primary threat for 2019. Listed as the first threat under “Global Threats,” it reads:

“Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.

At present, China and Russia pose the greatest espionage and cyber attack threats, but we anticipate that all our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence US policies and advance their own national security interests. In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely. For years, they have conducted cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk. They are now becoming more adept at using social media to alter how we think, behave, and decide. As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic
competitors almost certainly will gain greater insight into and access to our protected information."

The report also notes the prevalence of unattributed and nonstate actors increasing attacks and weaponizing technology. Since the countries mentioned above are not likely to claim responsibility for attacks, the use of cyber tools by these unattributed actors also escalates the risk of misattribution and misdirected responses. Such responses can come from national governments as well as targeted companies within the private sector, potentially provoking conflict through mere miscommunication or confusion.  

As technology continues to develop, the main question has become one of defense -- is it possible to defend against a cyber attack? A few options for possible defense may include:

- Deterrence + cyber security: One option is to use a combination of deterrence of an attack, while improving cybersecurity measures in place. Methods of deterrence include imposing sanctions against international actors that commit such crimes, in addition to issuing condemnations in coalition with other allied governments. Both President Obama and President Trump have taken such actions, although it is unclear whether their deterrence theory has been successful.

- Development of cyber peace treaties: It’s clear that many governments are struggling to keep up with the rise of weaponized technology, as finding a loophole in a protecting mechanism is generally much simpler than creating the protection itself. The rapid devastation that an attack could have, and correlating destabilizing effect on cities and

---


9 Ibid 7.
national governments, is a horrifying, yet foreseeable, future. Thus, many major world powers may be open to discussing cyber peace treaties, similar to the arms control treaties established during and after the Cold War between the Soviet Union (and later Russia) and the United States. And yet, risks and drawbacks loom large with this strategy. First, diplomacy may only limit action by state actors, meaning that non-state actors such as terrorist organizations would not face the same implications with their relations with the international community. Such actors may be deterred from action if laws were put in place punishing these acts, both domestically and in terms of international law. Second, many governments have restrained from being the first to negotiate a peace treaty in fear of being taken advantage of by actors who have yet to declare peace or “disarm.” The sheer magnitude of actors with cyber capabilities is a unique threat to cyberspace, as major powers tend to have a substantial edge in conventional weaponry and thus negotiate with fewer actors.

Questions to consider in response to the crisis:

● How will you determine who is behind these attacks? What resources can you use?
● How will you keep the general population from descending into chaos?
● Is it possible to stop future attacks? To mitigate further damage?

Works Cited


Zetter, Kim. “Sony Got Hacked Hard: What We Know and Don't Know So Far.”