Bethany Abbate

World Studies: Global Politics and Information Technology in a Global Society

Why haven’t cybersecurity policies advanced in the United States?

Word Count: 3,636
Introduction: The Global Issue

Espionage has existed for thousands of years between nation states, but the modern day global cyber sphere has created a whole new set of problems regarding espionage itself. The scope of modern warfare has been changed amongst countries, enhancing vulnerabilities for nation states as they are in a more defenseless position through the means of cyber espionage. This puts at risk many crucial elements necessary for the function of a nation, such as critical infrastructure, the economy, government confidentiality, militaries, and personal privacy of citizens.

Cybersecurity is in the spotlight of international news, from a variety of sectors such as politics, international economics, national security, and law. An often cited figure is that the annual cost to the global economy from cybercrime is $400 billion (Fischer). Despite these astronomical losses and countless incidents, laws regarding international cybersecurity remain in a fairly immature state. The United Nations released a report in July 2017 stating that 50% of countries currently have no cybersecurity strategy in place (Rayome). Although the concept of cyber law has been explored to a certain degree, there have been little efforts to define a law of “cyber peace” amongst nation states in the United Nations (Russell). This brings into question what exactly are a nation’s obligations to securing their networks and to prosecuting or extraditing cyber attackers (Russell).

One of the international community's greatest challenges regarding cybersecurity is lack precedeance it is receiving by the United Nations. Addressing the problems as they occur is only half of the equation. The other half is determining what exact measures need to be taken proactively to prevent future occurrences. Thus, the scope of evaluating each incident must be
viewed in a specific context. Additionally, a predominant obstacle in the international community is that developing nations lack the resources to improve cyber protection capabilities, making them potentially more vulnerable than developed nations. The lack of partnership between developed and developing countries could lead to deeper problems, since they know that these developing countries can be taken advantage of (Cybersecurity).

Building upon this notion, geographics are also a main obstacle when assessing cyber crime (OCED). It is difficult to pinpoint exactly where an attacker is from, even if a general location can be traced. Additionally, the lack of correspondence between the legal frameworks of different nations increases the difficulty in defining global solutions to fight cybercrime and prevent the misuse of information (OCED).

One of the main concepts explored throughout this paper is how “cyber peace” is defined by different actors within the cyber sphere, and how this concept is the overarching factor as to why policies struggle to advance. A recent publicly known global cyber attack known as “Wanna Cry” took place on May 13th 2017, targeting more than 74 countries according to security firms that investigated the attacks (Perloth). This use of malicious software blockaded British hospitals from accessing patient information, and demanded a ransom before gaining access back into the system. If the users did not comply with the request, the virus threatened to destroy all of their information (Perloth). The perpetrator of the attack has yet to be discovered, which highlights exactly why this is a significant global issue with obstacles. With few policies in place, there is a vast amount of room for more increased cyber crime towards institutions such as hospitals and businesses to occur, therefore having implications on an individual society. This is not the only side to the global issue. We also face attacks aimed directly at individual citizens, who are
regularly scammed out of their money and personal information. An example of this is the 419 Nigerian hacking scam, in which a Nigerian hacking group sent “phishing” scams attached to emails. This practice was initially aimed at taking advantage of wealthy Americans, but the tactic is now used to fool citizens around the world, and Nigeria is not the country doing this.

Individuals are not the only ones at risk. Another issue that continues to arise is cyber espionage, where nation states are targeting each other’s government presence. This summer I attended a Cyber Security summer program sponsored by the United States National Security Agency, and I learned about a group of Chinese hackers lead by a man named Sun Kailiang. Kailiang and his team had incentives to steal intellectual property that would boost their own economic interests at the sacrifice of the United State’s entities. In fact, China has invested in a new “Information Security base” treated as a military unit designed to fight and win wars in cyberspace (Singer, 3). Both China and Russia have a track record of hacking into numerous governments in order to obtain information that can either benefit themselves, or be used as blackmail toward another country.

The point is that differing actors have different motivations, therefore the implications of each situation differ as well. As a result, the concept of cyber peace has become complicated and difficult to approach from a policy point of view. Additionally, we must recognize that systems are being hacked on a daily basis, often with little to no immediate impact on society. However, a successful attack on critical infrastructure of a country could have significant implications in regards to the economy, national security, and the safety of individual citizens, resulting in global chaos. The United Nations has made slight efforts to halt this issue, however there still remains a lack of policy development.
The case study chosen for this paper is specifically cybersecurity policy in the United States, with an evaluation of the obstacles preventing effective cybersecurity legislation from being advanced. The research question is “Why haven’t cybersecurity policies advanced in the United States of America?” This question was chosen because the severity of cyber risks are often evaluated, but there seems to be a lack of attention toward creating and implementing policies to deal with this growing threat, both domestically and globally. This topic falls into global politics (conflict, peace, and security) due to its direct correlation with the impact on nations worldwide, creating risks aimed at certain countries’ policies and political structures. The understanding of information technology in a global society is relevant to this topic as well, because an understanding of the internet's infrastructure is pivotal towards the development of new policies.

This past summer, I attended the IB World Student Conference in Rochester, NY, where the theme of the conference was “Defining and Defying Boundaries”. This concept ties quite well to the global issues around information technology. The internet is boundless, and provides an unprecedented interconnectedness within our world, with both positive and negative implications. The purpose of policy is to set guidelines and rules to be followed, and to assert a certain degree of control. However, the internet does not fit well with this concept precisely because it is boundless, making it extremely difficult for policy makers to grapple with. Without a doubt, there is a need for cybersecurity in the modern era, since the internet is the modern day battleground for the safety of any nation. This new battleground is broad and complex due to the nature of the internet and the IT infrastructure behind it. Along with this, the newness and complexity of the technological world have made it difficult for lawmakers and nations to define and implement policies to address the emerging cyber threat.
In this paper I intend to demonstrate various reasons why cyber security policy has not advanced in the United States, including the government's lack of partnership with corporations, the knowledge gap between eras, and differing incentives amongst lawmakers.

Cybersecurity: Policy Obstacles in The United States

You may be wondering why the United States is often recognized as one of the biggest cyber victims. Well, the answer to this goes beyond foreign adversaries simply wanting to obtain classified information. Instead, it is because these adversaries recognize that the United States has little, if any, retaliation strategy in place against such cyber attacks. As a result, nations are not afraid of holding back when it comes to striking the United States, since they know there may be no formal punishment.

After searching for recent cybersecurity legislation on the United States Congress website, it was very evident to me that cybersecurity is not of high importance to Senators and Congressman. There have been hundreds of cybersecurity related bills and resolutions introduced over the years, however only a few have passed as laws. On top of this, I also noticed something else that is slightly alarming: the bills that have been introduced are sporadic. Some are very specific, while others are too broad and seem to lump differing issues together. While some states have established their own laws to address cybersecurity, there is still no unifying federal legislation that addresses these issues. This approach to policy making could be deemed as ineffective, which is partly why congress is lacking accomplishments in this area.
In the United States, there should be a distinction between the private and public sector cyber policy, mainly because they entail different ethical constraints. There is no “one size fits all” approach to cybersecurity issues, and this is often where United States policy makers slip up. While there should be more of a distinction between the government and private sector, there should be a partnership between the two as well, especially with major technology corporations (Darrow). The United States Government invests largely in technology, therefore it should push technology companies to create more advanced protection systems (Darrow). This could also benefit the individual consumer, creating satisfaction on both ends.

Arguably, corporations have recognized the cybersecurity issue to a greater extent than the government. Not only do American companies have the responsibility towards their shareholders, but also must protect their business interests in order to survive within the competitive market. It’s when people realize they’re at risk when they take action for protection, which is why companies strive to have strong IT infrastructures. For example, the recent Equifax data breach, which potentially compromised 143 million customers’ personal information, has taken a large toll on the company's business. Equifax now faces a strong lack of consumer confidence, which is the absolute worst scenario a company can face.

Corporations are not the only American sector that need high consumer confidence to succeed. In order for political parties to gain voters, they must ensure that they have the trust from their supporters. In light of the recent 2016 United States Presidential election, the Democratic Party has substantially lost the confidence of their supporters due to the Democratic National Committee hacks to WikiLeaks, an international organization which aims to expose classified information through digital means. Researchers concluded that these hacks were
initiated by groups associated with Russian intelligence (Nance). However, prior to the 2016 election hack, American intelligence agencies had known for years that Russia is one of their most concerning adversaries in cyberspace (Gady). Though, the irony here is that until recently, Kaspersky Russian anti-virus software was used within United States Government systems.

One of the reasons behind the lack of policy advancement is the “knowledge gap” that exists between generations (Singer, 4). The current lawmakers in the United States did not grow up in a cyber world, therefore they don’t have the same technological understanding or appreciation in comparison to younger generations. If the magnitude of these threats is not fully understood, it becomes more difficult to define a clear direction towards the creation of policy. There is a common notion that in order to understand cybersecurity, you must be mathematically and technically inclined, and the jobs should be left for people who work in computer science or IT departments. However, we live in an era where these types of practices can no longer be separately distinguished, due to the intersection of technology within our everyday life. The more knowledge our lawmakers obtain in regards to the issue, clearer policies will most likely be developed, and a sense of urgency to solve the issue will be increased. It is not solely the responsibility of the older generation to inform themselves on this issue. Rather, it is also crucial that the younger generation participate in cybersecurity engagement to ensure this issue will serve of greater importance in the future.

“Threat inflation” is a term used in political science that refers to “the attempt by elites to create concern for a threat that goes beyond the scope and urgency that a disinterested analysis would justify” (Brito). Different actors have differing motivations for threat inflation, including policy experts, members of congress, and intelligence officials (Brito). This can result in
unwarranted public support for misguided policies (Brito). Therefore it is likely that many members of the United States Government who are advocating for cybersecurity advancement have their own incentives. These differing incentives are one of the main reasons policies have not advanced.

When referring to motivations behind different actors, money is a large topic of conversation. Proposed cybersecurity legislation also presents opportunities for congressional pork barrel spending (Brito). “Pork barrel” is a metaphor for the appropriation of government spending solely to bring money in. An example of this is the Cybersecurity Act of 2010, which aimed to create cybersecurity research centers across the country, which would include a large sum of money that would be donated towards these complexes (Brito).

Another form of motivation is to instill fear in the public regarding cyber attacks, often perpetrated by the media. Washington Post columnist Robert Samuelson argues that cyber threats are so “terrifying” that the internet should simply be repealed (Singer, 166). This viewpoint may seem extreme, because it would be very hard to completely strip our technologically dependent society from all internet ties, let alone the global implications would be immensely negative. However, his usage of the threat infiltration tactic does make a point that one of the biggest obstacles is the internet itself, since it is the basis for all cyber attacks. This supports the argument that lack of policy is not the issue. Rather, it’s the coordinated group of bad actors who have very sophisticated ways of going about achieving their goal of hacking (OECD). However, the argument of “repealing the internet” is lacking something. It is also important to recognize, though, that technology is not a law. Therefore, it can not be repealed or univented (Singer, 167). Thus, Samuelson’s argument is simply rhetoric.
Many United States government members are motivated to push the “secure model” (Singer, 167). Building upon this notion, former presidential cybersecurity advisor Richard A. Clarke and Council on Foreign Relations fellow Richard K. Knake make the case that the United States and its infrastructure is extremely vulnerable to military cyber attack by enemy states (Brito). They offer a set of recommendations that includes increased regulation of Internet service providers (ISPs) and electrical utilities (Brito). We are told that “America’s national security agencies are now getting worried about logic bombs, since they seem to have found them all over our electric grid,” and that “[enemies] have probably done everything short of a few keystrokes of what they would do in real cyber war” (Brito). The basis for public policy making should not be fear.

In terms of proposals and rationales for policy making, Richard Clarke, former national security coordinator of the United States, has recommended “Instead of spending money on security solutions, maybe we need to seriously think of redesigning network architecture, giving money for research into the next protocols, maybe even think about another, more secure Internet” (Brito). Essentially, this argues that the current internet and network framework was not designed with enough security to prevent today’s threats (Singer, 167). However, this argument is highly unrealistic due to the heavy dependence on the current framework of the internet. Since the internet is boundless and open, it would be difficult to suddenly regulate it, and would also be a waste of the technological progress that has already been made.

Even if some believe internet regulation would be a solution worth exploring, a significant number of in the United States Government members believe that regulation is the wrong way to approach cybersecurity (Rosenzweig). As a matter of fact, the differing views of approach
prevented the Cybersecurity Act of 2012 from becoming a law (Rosenzweig). Paul Rosenzweig of the Heritage Foundation argues that “heavy handed government regulation is a 19th century solution for a 20th century problem” (Rosenzweig). Federal regulation is known for being a lengthy, complex process. (Rosenzweig). When regulations are finally implemented, they are often very difficult to change or remove (Rosenzweig). Therefore, regulation is not an effective approach when dealing with the dynamic, fast pace of cybersecurity and technological development (Rosenzweig).

**Conclusion: How does the case study affect the global issue?**

The United States should not stand alone in developing cyber security policies. In fact, there is no excuse for why it is not leading the efforts towards cyber peace. The United States is one of the few nations strongly equipped to bring nations together in order to solve this issue. The United States has leading edge technological knowledge, in part because many of the world's top technology corporations reside in the U.S. In addition to this, the United States is committed to the safety of its citizens, which is a common interest most nations share. Moreover, the United States has much at stake as the risks of cyber security increase, threatening government, infrastructure and ultimately safety and security of its people.

In order to strive for international cyber peace, nation states must cooperate with one another in developing effective policy solutions. In addition to partnering with each other, they should partner with businesses to develop and implement cyber security technologies and policies to safeguard critical information and infrastructure. And finally, it is important to raise generational awareness to the implications and threats of cyber security issues, so that leaders will recognize
the increasing threat to safety and security, and act to put needed policies in place to guard against the very real threats we face.

To partner with other nations, countries around the world should focus on clarifying priorities and goals, ensuring a cyber framework with strong protection, but also serving benefits toward the economy and society (OECD). Strategies should strongly promote cooperation at the international level, reinforcing alliances and promoting an immediate response system so that policies can be evaluated on a consistent basis in order to mold into the newest threats and vulnerabilities. (OCED). To be effective, national cybersecurity strategies and policies should be periodically evaluated and updated so that improvements can be implemented to face new security threats (OCED). This can be performed by enacting a periodic comparison with strategies and policies of other countries (OCED). It would also be beneficial to provide periodic country reports to share information about security incidents and the level of damages created (OCED). This output could be the basis used to review the cybersecurity strategies and policies, allowing for recurring growth and development of policies throughout the world.

Earlier in the paper, I described how there is no “one size fits all” approach to cyber policies in the United States while making the point that the private and public sector should have different policy approaches. This same concept applies to the treatment of cybersecurity policy in the global community. By partnering with businesses, governments can benefit by the technical knowledge that businesses have, and by the motivation that businesses have to protect their shareholders and profits. Corporations are often labeled as the enemy from certain political perspectives, due to the large sums of money they generate. However, if the international
community wants to amplify cybersecurity measure, businesses are a strong resource that should be utilized and acknowledged.

I also pointed out how lawmakers and citizens of an earlier generation may not recognize the cyber threats we face because they did not grow up in the same technological generation that we now exist in. Therefore, it is critical that we raise awareness among the generations, past and present, to the increasing cybersecurity threats that we all face. In particular, our lawmakers need to be more aware so they can better address these threats through policy measures that protect our safety and security. Additionally, it is important that citizens are just as informed so they can encourage their lawmakers to take action as well. The younger generation needs to participate in educating older generations about the basics cyber realm, so that our society can work together to strive for a unified understanding of the issue.

As a concluding thought, I believe that by focusing on this issue, there could be a strong job market in support of securing our online data and our technological future, both in policy and technology fields. Part of the problem is the lack of research and development that is currently being devoted towards this issue. As I am in the process of searching for universities, it is very difficult to find institutions that have programs and research centers devoted to furthering the development of cybersecurity from a both the technological and policy perspectives. Academic scholars worldwide should be included in the process of cybersecurity development. The global community could be pushing the envelope in terms of cyber security jobs. There are potentially tens of thousands of jobs in this area that we simply aren't recognizing sufficiently yet to realize it. With an emphasis on education and training in the cybersecurity field, there would be a larger effort to combat cyber-related issues in society, while both raising awareness to the critical issue
and providing an income at the same time. The future highly depends on how we choose to tackle the global cybersecurity problems of today.

Works Cited


Works consulted