How Has Cyber Operations Impacted American Citizens?

Eric Tran

Old Dominion University IDS 300W

The world has seen a boom in technology in the few recent years. From the construction and improvement of the internet to the advancement of cellphone and computer technology, Cybersecurity has gone from an after thought to a national security crisis. Throughout the years, prolific breaches and cyber operations against the United States has opened the eyes of many, and showing how devastating cyber weapons and cyber operations are. Russia's information campaign, China's penetration into classified networks, and Iran's cyber attacks have all costed the United States a lot in terms of information, money, and personnel information. With the spotlight on cyber and how it has impacted America in so many ways, exploring the impacts through multiple disciplines will reveal the true nature of this looming threat. Through multidisciplinary lenses, consisting of economics, political science, and psychology, how has cyber operations impacted American society? No doubt when breaches happen, companies can lose the trust, investments, and monetary value of their company, along with money to secure their system and fix whatever damage was caused. When it comes to politics, cyber operations against a sovereign nation can yield either no blow back or can evolve into a political mess. Lastly, psychology and the impact of cyber activity on victims is now being looked into by researchers, where once it was never mentioned. Many in government and private industries can argue that one of the disciplines is more of a priority, but together they paint the overall picture of cyber operations and once they come together, the common ground shows how each out can explain the impacts cyber attacks will have on American citizens and the United States as a whole. However in order to see the common ground, each discipline will need to be explained, and how cyber impacts them.

It has been said by many analysts that the next Pearl Harbor will involve a massive scale cyber attack on critical US infrastructure. Economic infrastructure which is the backbone of the United States promotes economic activity through banks, financial markets, transportation, and telecommunication. Even smaller scale attacks on government agencies and private companies can cost millions or even

billions to repair and rebuild. From nation state sponsored attacks to cybercriminals looking for a payday, cyber attacks can and will cause severe damage to any system. A statistic written in the Harvard Business Review by Paul Mee and Til Schuermann, “Cybercrime alone costs nations more than $1 trillion globally, far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. We ranked cyber attacks as the biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.” It is very easy and cheap to set up a computer to be able to attack a network, and it is much more effective than planning a terrorist bombing or even war. Additionally, the writers from the Harvard Business Review painted a picture as to how a financial crisis might be triggered from a cyber attack. The writers suggested that a rogue nation, terrorist group, or script kiddies could compromise financial institutions and cause a snowball effect, which will make various banking and payment options unavailable. American society will be halted, although temporary, but still the damage will be done. Such actions, need to be counteracted whether it be through the strengthening of cyber defenses or renewal of old infrastructure. Economic infrastructures aren’t the only vulnerable aspect, but also America’s national security strategy involving cyber and the politics behind cyber attacks.

“It is legitimate to say that the United States has a national security problem rather than a cybersecurity problem and to say that as things stand at present the American government is steering the United States toward a cyber-9/11” (Gagnon, 2004, p.1). There are parallels that can be drawn between pre-9/11 and current cybersecurity environment. Firstly, in both situations, there was knowledge that people were actively working to hurt the United States through physical or cyber means. Second, the US government did not respond to this knowledge with adequate measures nor handled the threat before it became a problem. An exercise titled “Eligible Receiver” which was conducted by the National Security Agency (NSA) and Department of Defense (DoD) consisted of 35

agents and a couple thousand dollars. They were to travel around the world and acquire legal means to attack the United States information grid. The end result was astounding, in less than two weeks, they successfully took over 911 systems and attacked 41,000 of the 100,000 Pentagon computers. This exercise only highlighted a portion of what could be done on American infrastructure. Several measures have been enacted by different administrations to better US cyberstrategy. The Clinton administration issued Presidential Decision Directive (PDD) 63 and the Bush administration issued the National Strategy to secure Cyberspace (NSSC). Critics of both of these documents say that they were late in coming and were both incoherent policies. The policies also inhibited an inability to evolve with the growing tech industry, failed to analyze hacking trends, did not account for citizen's role in protecting the information system, and failed to support the private sector. This is a snippet of the overall inability of the government to create a defining cyberstrategy and ensure the safety of critical infrastructure, while not responding to cyber attacks effectively. With politics and nation security, there are unknowns that still need to be addressed, parallel to cyberpsychology and the emerging interest in what happens to victims of cyber attacks psychologically.

"Depending on who the attackers and the victims are, the psychological effects of cyber threats may even rival those of traditional terrorism. Victims of online attacks and crime can suffer emotional trauma which can lead to depression" (Bada, Maria, and Jason R. C. Nurse, 2019, p.17). Depression, stress, heightened threat perception, and victimization are all psychological causes from cyber attacks. Maria Bada and Jason Nurse suggests that the public response to malicious cyber attacks center around the public not perceiving the attacks as a threat onto themselves, and if they do, they believe they have no power to stop it. Instead, the public responds to the loss of service or interruption of their application, rather than the attack itself. The Protection Motivation Theory (PMT) states that there are two cognitive processes: threat appraisal and coping appraisal. Threat appraisal is how susceptible

someone is to a threat. An example of this is how vulnerable someone is to a phishing attack. Coping appraisal is when someone engages in a recommended action that is preventative in nature. An example of coping appraisal is not opening an email sent by an untrustworthy email address. PMT is able to explain how people end up being targets and also explains how people can prevent from being targets of a cyber attack. US society also responds to attacks differently depending on several variables. The first variable is the identity of the attacker and target identity. Since most criminals and terrorists do not reveal who they are, the public usually will usually not react severely. Similarly, fraud and phishing attacks cause less panic, whereas attacks against national finance or health institutions may cause mass panic. Secondly, the scale of the attack is another influential point. The full impact of an attack is not known immediately, but once it has been disclosed, society will react accordingly, like in the case of the Equifax breach. Third and last, the disclosure method of communicating an attack will influence how society will react. Communication to the public will usually come from either the government, the company that was attacked, or the attacker themselves. Maria Bada and Jason Nurse highlighted the psychological impact with a case study of the WannaCry ransomware in 2017.

The WannaCry ransomware was a computer worm that spread across Windows computer networks. The reason why this worm in particular was so devastating was because the hackers utilized a zero-day vulnerability which was not yet patched by Microsoft. With over 200,000 victims in over 150 countries, the disruption caused social outcry since it impacted health systems, car manufacturers, delivery services, education sectors, and telecom companies. As stated by Maria Bada and Jason Nurse, “The psychological impact of WannaCry was also significant. For many it resulted in worry, anguish, disbelief, and a sense of helplessness… Psychologically, there was also the realization by many that cyber-attacks could now cause the loss of life.” Due to the WannaCry ransomware gripping health systems tight in its hands, one patient who was scheduled for heart surgery had to postpone until this

crisis was averted. The inconvenience, stress, and frustration of this event led to the patient and his family members questioning as to why the attackers would target a hospital. This event also showed that an attack like this could also result in loss of life due to unavailability of health systems and health infrastructure, furthering the psychologically impact of citizens and victims.

With the background of each of the three disciplines explained, one major question arises once more, why explore cyber attacks through a multidisciplinary lens rather than focusing in on one major discipline? Many can argue that an economics view has proponents of psychology and national security and vice versa. The advantages of going about answering this question through a multidisciplinary perspective is bringing the expertise together and develop common ground, where each discipline melds together to tackle the complex issue of cyber attacks and their impact on American citizens and society as a whole.

"You bring me 10 hackers and within 90 days I'll bring this country to its knees. Jim Settle, former head of the FBI" (Gagnon, 2004, p.2). This profound quote from the former head of FBI paints a grim picture of the current landscape of American infrastructure and cyber defense. The blend of the three disciplines, political science (national security), economics, and psychology (cognitive) can reveal a complex issue and point the way to a solution. Since the passage of the NSSC under the Clinton administration, Benoit Gagnon states that "cyberattacks have risen by approximately 55 per cent each year. In 2003 alone, the year in which the NSSC was initiated, the number of attacks rose by about 60 percent." One of the many criticism of the NSSC and many policies in general is the public-private relationship. Under the National Cyberspace Security Response System (NCSRS), the Department of Homeland Security (DHS) was supposed to organize the private sector to adopt cybersecurity measures in order to secure private industry. However, with little legislation, this plan failed. With over 80

percent of critical infrastructure in the hands of private industry, and with their three top goals: profit, customer satisfaction, and innovation, cybersecurity is not on their list of priorities. Because of this, infrastructures like banks and other financial institutions are prone to attack.

The financial sector is a combination of human psychology and economics. Confidence in knowing that a payment will go through or a bank will have the money a person need, keeps the system stable. However, throughout the years, it has been evident that banks are vulnerable to cyber threats, and if a catastrophe were to happen, the confidence will erode and will cause a ripple throughout the world. Written in the *Economics and Business Review Vol. 5,* Piotr Lis and Jacob Mendel gave a chilling statistic:

> "Cybercrime costs the global economy up to $575 billion annually. The rise of disruptive technologies, such as the Internet of Things (IoT), and more than 50 billion devices connected to the Internet by 2020 means that the world is facing an increasing risk of cyberattacks. Estimates show that cybercrime extracts up to 20% of the value created by the Internet meaning that as much as $3 trillion of global economic value could be at risk by 2020."

Over 50 billion devices are expected to be connected to the internet by 2020, paving way for more opportunity for hackers. Because of this growing threat, another criticism of the NSSC was their inadequacy of identifying threat vectors that could potentially shutdown critical banking systems and in turn impact the American financial system. Another issue with America's cyberstrategy is the inability to keep up with technological advancements and evolve with hacking trends. Referencing back to the exercise "Eligible Receiver" conducted by the NSA, criminals and state sponsored hackers are nimble and can acquire the materials needed for an attack from anywhere. Because of this, nations throughout the world has taken their war fighting and intelligence gathering into the cyber domain. One strong example is Russia, who has conducted numerous cyber operations on their neighboring countries and

conducted full scale cyber operations in support of kinetic attacks in Ukraine. More recently, they have performed a massive disinformation and influence campaign in the United States, which resulted in a divided and broken United States. In the end, while Russian GRU officers receive medals in the Kremlin, American society ate up all of the misinformation and started to in fight. This highlights a weak national security and cyberstrategy that failed to strengthen the US society and the government failed to predict such an event from happening. What happened to the Unites States during the 2016 election time-frame was tested on Ukraine during the Crimea conflict, and although the US was observing, they failed to see the what Russia was doing in the cyber domain.

Parallel to what Russia is capable of, everyday someone is attacked either by phishing emails, fraud, virus attacks, identity theft, or social engineering attacks. Although the attackers who are mostly going after companies and citizens are not doing it for war, they are still interested in monetary gain and disrupting daily norms. Like Maria Bada and Jason Nurse stated earlier, the Protection Motivation Theory or PMT shows how people are vulnerable and how they can prevent such attacks from bearing fruit. Through the unsuccessful attempts by DHS and the government as a whole, private industry has been left to self regulate and self defend against cyber threats. Recently with the creation of the Cybersecurity and Infrastructure Security Agency (CISA) steps have been taken to strengthen and provide resources for private companies, it is still too late. Because of this self reliance, many companies have poor training or personnel and outer layer defense. Therefore the threat appraisal of the situation states that an employee is bound to be a victim of a cyber attack, most likely due to social engineering attacks which will then lead to a more sophisticated technical attack. Many researchers and analysts look at an attack and ponder how much money is lost or what is the blow back resulting from poor defense. Few look at the attack and wonder what psychological impact it has on the victims and how it might open them up to more vulnerabilities and emotional stress. Maria Bada and Jason Nurse

describes how identity theft might impact a person, “the impact of identity theft on a victim at an emotional level can lead the person becoming distressed and be left feeling violated, betrayed, vulnerable, angry and powerless.” Some victims may even go through the stages of grief and further become depressed or gain a heightened sense of danger. A study done by Dr. Daphna Canetti and her colleagues on personal insecurity after a cyberattack was one of the first psychological studies. The researchers simulated an attack and measured salivary cortisol. In the study, salivary cortisol is the measure of stress response and it was taken from 100 college aged participants. After simulating the participants to a cyber attack, the results show that cortisol levels rose significantly. As a result, if the cyber attacks were real, the participants would have experienced feelings of personal insecurity, elevated stress, and vulnerability. Even though no psychical harm was experienced, psychologically, victims suffer far after the incident.

Cybersecurity has been and always will be a complex problem facing America today and in the future. By looking at this problem with disciplines like economics, political science, and psychology, solutions can be found. America has a big problem, which is the outdated infrastructure and policies that are not evolving with the technology. Combining all disciplines, a solution can be solved through an improved policy, improved infrastructure, and improved society that can weather any cyber attacks. First and for most, the solution must come from the top, which is policy. Developing a comprehensive cyberstrategy that can address current issues and future issues like quantum computing is key. Also, bridging the gap between public-private partnership is key to solidifying the defensive posture of America against any cyber threat. Once policy has been implemented and enforced, the effects will trickle down and businesses, as well as infrastructures will be improved and there will be resources to implement better cybersecurity practices. Banks and other private companies must also take it upon themselves to invest in a more comprehensive cyber defense structure, as well as train their employees

to be more preventative to cyber attacks, such as phishing, whaling, scams, frauds, or any type of social engineering attacks. Since billions are lost each year, improvments in defense will decrease tragedies such as breaches and other types of successful attacks since there will be defenses in place and humans won't be walking vulnerabilities. Psychologcial impact will always be inevitable in cyber attacks, but with the improvements of policy and infrastructure, the likelihood of people being impacted individually will be reduced. Awareness of such psychological impact will also help victims seek the necessary aid they need post attack.

Cyber is an ever evolving and growing field with billions of devices capable of being turned into a weapon. It only takes a few hackers and some laptops to potentially cripple the US economy and infrastructure. That is why answering the complex issue of "how has cyber operations impacted American society" needs a multidisciplinary. Through explaining how economics, political science, and psychology can come together and create a common ground to solve this issue, many disciplines are represented. It is evident with proof from researchers, analysts, and experts, policy and cyberstrategy is a crucial foundation before being able to secure the infrastructure and ensure citizens are safe psychologically. Cyber attacks will always occur, but by reducing the chances of it recurring, the US can propel itself into a new age of technology and ensure the country is safe from the next "9/11." However, it will be a grim future if the US can not grapple with the evolving landscape of cyber, and the picture painted by former head of FBI, Jim Settle will very much be in our near future, if not now.

References

Bada, Maria, and Jason R. C. Nurse. “The Social and Psychological Impact of Cyber-Attacks.” 2019.

Canetti, Daphna, et al. “How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks.” CyberPsychology, Behavior & Social Networking, vol. 20, no. 2, Feb. 2017, pp. 72–77. EBSCOhost, doi:10.1089/cyber.2016.0338.

Gagnon, Benoît. “Are We Headed For a Cyber-09/11? The American Failure in Cyberstrategy.” Conference Papers -- International Studies Association, Mar. 2004, pp. 1–20. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=poh&AN=16050639&scope=site.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics & Business Review*, *5*(2), 24–47. https://doi-org.proxy.lib.odu.edu/10.18559/ebr.2019.2.2

R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," in IEEE Technology and Society Magazine, vol. 30, no. 1, pp. 28-38, Spring 2011.