Government Response and Role in the Social Construction of Cybertechnologies

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Huy Huynh

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Rider W. Foley, Department of Engineering and Society

Introduction

The rate of cyberattacks have been increasing during the last decade. The first large-scale ransomware attack was called the WannaCry attack. It took place on May 17th, 2017 and it targeted old Windows computers and stole their data for ransom (Gregory, 2021). Another more recent and larger example of a cyberattack was the ransomware attack on the Colonial Pipeline, the largest American oil pipeline system, on May 7th, 2021. This attack halted the distribution of gas and had many negative effects, such as higher gas prices and gas outages around the United States. In addition, Colonial paid the ransomware of $4.4 million in bitcoin, which can further incentivize even more hacker groups to go for large scale attacks (Turton, 2021). Later the same month on May 30th, 2021, another large scale ransomware attack on JBS Foods, a worldwide meat producer, occurred. This stopped the slaughterhouse operations around the world and led to JBS Foods paying the ransomware of $11 million in bitcoin (Nair, 2021).

The US government has the power to mitigate the damage of cyberattacks by strengthening the nation's cyberdefense through legislation. They have attempted to do so in the past, but there is question whether they can do more to stop these attacks from happening in the first place. This paper used the social construction of technology to explore the government's values and actions towards cyberspace. It analyzed the government's role and actions involving cybersecurity throughout recent years of presidency starting from President George W. Bush to President Joe Biden. Several cybersecurity policies are examined to see if any positive effects came from them. Lastly, direct government actions through legislation are discussed to determine if the government has created any actual change in cyberspace.

Research Design

What role does the US government play in the development of cyber technologies? This paper aimed to research what the US government has done in the past involving cyber technologies and cybersecurity and determine how effective the government legislation and actions involving cyber technologies were in the past and the present. This paper will focus on the policies and actions made by the government starting from the George W. Bush-era to the current Joe Biden-era. The Bush era was chosen because the issue of cybersecurity and security in general became a topic of national importance after the events of the terrorists attack on September 11th, 2001, which was during the Bush-era. The most notable actions involving cybersecurity from each presidency up to the current Biden presidency is analyzed to see the outcomes and effects of each action. These actions are picked subjectively based on how large the action and effect was on the social group of the public. A conclusion of what the government's role is in cybersecurity is made based on the effects of these policies on cybersecurity. This evidence was then analyzed to answer the research question to find the government's actions regarding cybersecurity.

STS Framework

The social construction of technology (SCOT) framework is about how a certain piece of technology is shaped by human society. The basic concepts of SCOT include four main components, including interpretive flexibility, relevant social group, closure and stabilization, and wider context (Klein & Kleinman, 2002). SCOT itself is an "open process that can produce different outcomes depending on the social circumstances of development" (Klein & Kleinman, 2002). Looking at cyber technologies through the lens of SCOT, there exists interpretive

flexibility as social groups such as modern companies and the government can manifest what cyber technologies truly mean. Currently, it is still in the closure and stabilization phase because it is still developing and growing more important by the day.

Semire Yekta wrote a doctorate thesis mentioning the use of SCOT in regards to cyberspace. They talked about online fraud and said that "one of the most important characteristics of cyberspace is the construction of a unique form of connectivity" (Yekta, 2019). Yekta quoted another scholar, Mlambo, and their belief about the Internet is a network of networks, and these networks are interconnected to each other in different configurations" (Yekta, 2019). Yekta also stated that it "in turns creates a unique environment and engenders challenges that cannot be solved through traditional crime prevention and detection methods", which shows how common practices of fighting against crime will not work in this new social construction of cyberspace (Yekta, 2019). Through their research, they emphasized that cyberspace and cybersecurity alike are both new, developing, and unfinished constructs of technology through their analysis of online fraud and crime.

Furthermore, Myriam Dunn Cavelty, an International Relations Scholar has analyzed SCOT of cybersecurity in the government. She stated in her article that "cyber technologies are treated like any other tool of power projection and coercion" (Cavelty, 2018). This implies when cyberattacks became more prevalent, the government began to view cyber technologies as not just a piece of digital technology, but more of a political issue in general. This changed cybersecurity to be more relevant to current politics in the government. The social construction of cyber technologies is becoming something of more importance because of the growing rate of cyberattacks. This undeveloped cyberspace and cybersecurity forces the government to determine how to handle the growing importance of these social constructs.

Case Context

The government is heavily affected by the growing rate of cyberattacks because of the plethora of sensitive information within the government. Cyberattacks could lead to that sensitive information being stolen. Even with the potential consequences of the leaked data, the government has not done a great job with cybersecurity throughout the last decade. There are several reasons that this could be the case. One is that it is currently a new and developing social construct of technology, so it will take some time before the government will be able to secure their sensitive information optimally. There are many different social groups affecting the development of cyber technologies, including government agencies, hacker groups, corporations, and the public. Hacker groups will keep developing new hacks to create cyber attacks. Government agencies and corporations will need to adapt and create a stronger cybersecurity to defend against those attacks. The public can be affected by these cyber attacks too and can pressure the government and corporations to take more action against cyber attacks. These social groups are still currently developing cyber technologies.

There are many entry points of attack and it will be hard in general to defend against these cyberattacks. The government will need the help of smaller scale companies in the fight against cyberattacks. In a McKinsey & Company's book on the transformation of cybersecurity, they mentioned the government must take initiative in the fight against cyberattacks by creating legislation enforcing certain cybersecurity requirements (Digital, 2019, p. 21). The government hasn't really enforced any strong legislation on cybersecurity, until only recently. On May 12, 2021, Joe Biden issued an executive order regarding the nation's cybersecurity (The United States Government, 2021). This executive order is a strong case of the government beginning to adapt to this new social construct of cybersecurity after the recent large-scale attacks on big

companies, such as the Colonial Pipeline attack and the JBS Foods attack. The government is beginning to view cyberspace as being an important factor in their system. However, there is still a question on what more the government should do in terms of cyberspace.

Results

The US government tried to play a major role in cybersecurity, but most of their efforts did not result in anything substantial for the cybersecurity of the nation. From the evidence gathered, internet access was made available in the 1990s and cyber technologies in general were not used often in the past. Over time, as "government agencies, private sector corporations, the military, and even retail shoppers shift their activities and functions to the Internet, cybersecurity becomes a pressing concern" (Harknett & Stever 2011). In relation to SCOT, cybersecurity is still developing rapidly, but most of it is still not fully understood. There seemed to be at least one attempt to better the nation's cybersecurity in each presidential era. However all of these attempts were not effective as the issue of securing the nation's cybersecurity is still prominent today. This reveals that the government is trying to play a large role in the construction of cyber security, but it has not been successful.

Early notices of the US government response to cybersecurity occurred in 2002 and 2003 with President Bush's administration. President Bush created the Department of Homeland Security in 2002 in response to the attacks on September 11th, 2001 (Bush, 2002). Bush started the National Strategy for Securing Cyberspace (NSSC) as a way to identify "the existence of cyberthreats and [call] for a coordinated national effort to close vulnerabilities" (Harknett & Stever 2011) during the Cold War. In 2008, Bush also created the Comprehensive National Cybersecurity Initiative (CNCI), which initiated the fact that the government "must exercise a

leadership role in developing cybersecurity technologies", and it listed several initiatives that the government should take to secure the nation (Harknett & Stever 2011). However, these documents were never enforced and were very weak. The NSSC were only suggestions to what can be done, so these suggestions were never enforced. The CNCI was incomplete when the Bush presidency ended, and had to be continued under President Obama. Cybersecurity was still very unsettled after the era of President Bush.

President Obama then took a more top-down approach from 2009 to 2017. He implemented a review team of experts to assess the cybersecurity situation in the government within the Department of Homeland Security and Governmental Affairs through congressional reports. This was a good implementation as it allowed for a constant checkup of the government's cyberdefense, however similar to the policies Bush created, the congressional reports were neve enforced or followed. He also attempted to continue the CNCI from Bush, but it failed as it did not meet his objectives. Analysis was done on CNCI and it reported that "CNCI is neither comprehensive in scope, national in perspective, nor propelled with an initiative that meets the urgency required to correct the nation's vulnerability to cyberattack" (Harknett & Stever 2011). The fact that the CNCI was also very secretive to the public made it difficult for the social group of the government agencies and the public to interact and prevented the growth of cybersecurity in general. President Obama's policies had similar issues to President Bush's policies, as they were never forced, but the beginning of initiatives were created.

From 2017 to 2021, President Trump's administration had some positives, but many negatives involving policies and actions relating to cybersecurity. Trump signed into law the Cybersecurity and Infrastructure Security Agency (CISA) in 2018. The CISA was a branch of the Department of Homeland Security and their goal was to advance national security by

eliminating threats to the United States. It is still active today in warning the nation about potential threats, but "it still lacks a Division of Enforcement, similar to the Divisions of Enforcement of the SEC, CFTC, or FTC to serve as an investigatory/enforcement/ international-information-sharing arm", meaning it again has similar issues to previous policies made by Bush and Obama (Atkinson, 2020). Since the Obama era, congressional reports were created and used to voice concern about potential deficiencies in their cybersecurity and to prompt further action to fix those issues. Even though they were not enforced, they do give an idea of what the situation is like within the government. In a 2019 Congressional report on the US Federal Government, the Committee on Homeland Security and Governmental Affairs investigated eight agencies within the government and found a long list of vulnerabilities. In many cases, the agencies even lacked government certification that their systems were in proper working order (Senate, 2019). It was recommended that these agencies check their systems and fix the listed vulnerabilities. However, two years later, the Committee on Homeland Security and Government Affairs investigated the same eight agencies and they identified many of the same issues they found (Senate, 2021). In addition, under the Trump administration, cybercrime still continued to grow, leading to record numbers of "complaints and economic losses in 2019" (Fidler, 2020). This shows that the policies and actions by the government in the past eras of presidency were not effective enough to stop damages to the nation.

President Joe Biden has also tried to make some impact in regards to cybersecurity. Mentioned previously, on May 12, 2021, President Joe Biden issued an executive order to improve the nation's cybersecurity. The executive order aimed at modernizing cybersecurity defenses in the country by having open channels for sharing information on cybersecurity and enforcing cybersecurity requirements on organizations to prevent further damages. Federal

agencies are also expected to modernize their technology environment and security practices (The United States Government, 2021). The executive order also called for updating authentication and encryption frequently and executing planned timelines for implementing and monitoring each federal agency and its technology environment (The United States Government, 2021). Because this executive order was so recent, it is hard to tell if it even had any substantial impact because the JBS Foods attack took place 18 days after. Even so, these methods were very indirect in solving the situation of cyberattacks and it seems that the US government hasn't fully been able to deal with cybersecurity as it is still a developing technology.

Discussion

The evidence gathered revealed that the US government has attempted to play a major role in the social construction of cybersecurity and cyber technologies but they were not able to enforce their suggested changes or had any positive effects. In a recent journal article by Karen Guttieri that also assesses the US government's role in cybersecurity, they called for the government to accelerate change or they will lose the information war. Information war is a term for cyberwarfare and the author states that "if [the US government] fail to adapt -- we risk losing the certainty with which we have defended our national interests for decades" (Guttieri, 2022). Her ideas were similar to what this research paper found in that the government has not done enough to deal with the growing issue of cybersecurity.

This research paper had limitations in its research design. More government sources could have been used to find more direct information on how the government deals with cybersecurity. This paper could have gone over more policies from each presidential era, and it relied on the policies being chosen subjectively instead of an objective reason.

If this paper were to be done differently, it would include more government sources and more sources in general, especially more about the past. Other than articles and government sources, surveys could be created to see the public's opinions on how the government responds to cybersecurity and then that information could be used to further determine the government's role. Lastly, this paper could have included interviews with the public to find out more about the public opinion of the government and cybersecurity to learn more about the different social groups that develop cybersecurity.

Conclusion

By analyzing the evidence, we can see how the US government has yet to pass any effective policies in the social construction of cyber technologies. Their attempts in the past to address this issue have all failed. Cyberattacks are still prevalent as ever to this day and will continue in the future unless the government takes effective action involving carrying out their initiatives and suggestions. The government needs to be able to adapt to the growing usage of technology and begin to make and enforce legislation involving cyber technologies and cybersecurity.

It is exciting to see the government continuing to take action from President Biden's recent executive order, but similar actions have been done in the past to no avail. Hopefully the government will be able realize that they have the power to strengthen the nation's cybersecurity and be able to complete the stabilization in this social construct of technology. They have to stop only giving suggestions on what can be done, but actually try to enforce those suggestions if they want to secure the nation's cyberspace.

References

Atkinson, W. H. (2020, October 23). *A review of the Trump administration's National Cyber Strategy: Need for renewal and rethinking of the public-private partnership in U.S. National Security policy*. The Institute of World Politics. Retrieved April 17, 2022, from https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/

Bush, G. W., The Department of Homeland Security (2002). Retrieved April 17, 2022, from https://www.dhs.gov/publication/proposal-create-department-homeland-security.

Cavelty, M. D. (2018). *Cybersecurity Research Meets Science and Technology Studies* (thesis). Cogitatio, Lisbon.

Digital McKinsey and Global Risk Practice. (2019). *Perspectives on transforming cybersecurity*. *McKinsey & Company*. Retrieved October 17, 2021, from https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.

Fidler, D. P. (2020, December 2). *President Trump's legacy on cyberspace policy*. Council on Foreign Relations. Retrieved April 17, 2022, from https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy

Gregory, J. (2021, September 1). What has changed since the 2017 WannaCry ransomware attack? Security Intelligence. Retrieved October 4, 2021, from https://securityintelligence.com/articles/what-haschanged-since-wannacry-ransomware-attack/.

Guttieri, K. (2022). Accelerate change: Or lose the Information War. Retrieved from http://www.jstor.org/stable/10.2307/48651811?refreqid=search-gateway.

Harknett, R. J., & Stever, J. A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, *71*(3), 455–460. https://doi.org/10.1111/j.1540-6210.2011.02366.x

Klein, H. K., & Kleinman, D. L. (2002). The social construction of Technology: Structural Considerations. *Science, Technology, & Human Values*, *27*(1), 28–52. https://doi.org/10.1177/016224390202700102

Nair, A., & Reese, C. (2021, June 10). *Meatpacker JBS says it paid equivalent of $11 mln in Ransomware attack*. Reuters. Retrieved October 17, 2021, from https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/.

The United States Government. (2021, May 12). *Executive order on improving the nation's cybersecurity*. The White House. Retrieved October 17, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg. Retrieved October 4, 2021, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-usingcompromised-password.

Yekta, S. (2019). *The social construction of online fraud* (thesis).