Cyber, The United States, and Trump: A Path to Security

Diana Hajali

Cyber-attacks have evolved over the past three decades from the spread of viruses to the hacking of credit card information to large breaches directed against entire companies. Today, cyberattacks are a serious and eminent threat not only to individuals and corporations, but also to the national security of countries around the world, the United States being a prominent target. In order to protect against cyberattacks and prevent a future cyberwar, corporations such as Windows began creating software security systems and anti-hacking software. In the federal realm, a cybersecurity strategy was developed in 2003 by George W. Bush and in 2008, Bush proposed a 10% increase in cybersecurity funding in order to combat attacks against federal information systems and databases by China, Russia, and others.[1] In 2011 under Barack Obama, a Cyber Security Division was created under the Department of Homeland Security (DHS) which enhances "the nation's critical information infrastructure and the internet" through "new technologies, tools and techniques [that] enable DHS and the U.S. to defend" against cyberattacks.[2]

Seven years later, President Trump signed a bill which created a new department under DHS known as the Cybersecurity and Infrastructure Security Agency (CISA). The department aims to strengthen the U.S.'s protection of infrastructure from cyberthreats and to pre-plan responses for any major cyberattacks, as well as present more of an offensive cybersecurity strategy rather than solely defensive.[3] While President Trump has been an active proponent of U.S. cybersecurity, more should be done in order to guard the nation against rising threats from Russia, China, and other adversaries. This paper makes the following recommendations to the

---

[1] Wolf, Richard. "Bush Calls for Tighter Cybersecurity." *ABC News*, 15 March 2008, https://abcnews.go.com/Technology/story?id=4457451&page=1.

[2] "Cybersecurity Programs." *Department of Homeland Security*, 10 Oct. 2018, www.dhs.gov/science-and-technology/cyber-security-division.

[3] "Trump Creates CISA, Official Federal Cybersecurity Agency (Multi-Video)." *American Security Today*, 23 Nov. 2018, americansecuritytoday.com/trump-creates-cisa-official-federal-cybersecurity-agency-multi-video/.

president and his administration: first, the cybersecurity branch within the Department of Homeland Security should receive more funding for its initiatives; second, cybersecurity and computer science programs should be integrated into the nation's education requirements; and third, the federal government must increase its collaboration with private security and information technology (IT) companies. Although these proposals might seem logical, or common sensical, not enough is being done due to difficulties in appropriating funding, party bipartisanship in regards to military spending and the education sector, and a lack of presidential effort.

As stated, it is recommended that President Trump continue pushing for an increase in the budget for the cybersecurity section of the Department of Homeland Security. In 2019, the budget requested for DHS was $47.5 billion, a 7.8% increase from the 2018 President's Budget. While the 2020 fiscal year budget request is set at $51.7 billion, hinting at a rising dedication to supporting DHS's various missions, only $1.3 billion of it would be set aside for cybersecurity and infrastructure security.[4] In 2019, $1.1 billion was dedicated to DHS's cybersecurity budget, so while the total DHS budget is set to increase by $4.2 billion, the cybersecurity budget will only see a $200 million increase. In addition, in 2020, 20% of the U.S.'s entire budget is projected to go towards the Department of Defense (DoD) while 1.4% would be given to DHS and even less than 0.3% would go towards cybersecurity in both DoD and DHS combined.[5] This is not nearly enough to protect the United States from foreign cyberattacks emanating from China and Russia. If the budget is not increased significantly, the U.S. will remain one of the most targeted nations in the world, as foreign actors will have little standing in their way.

---

[4] "President's Fiscal Year 2020 Budget." *Department of Homeland Security*, 19 Mar. 2019, www.dhs.gov/news/2019/03/18/president-s-fiscal-year-2020-budget.

[5] Johnson, Derek B. "House Homeland Committee Wants More Cyber Funding for DHS." *FCW*, 15 Apr. 2019, fcw.com/articles/2019/04/15/dhs-cisa-funding-letter-johnson.aspx.

Therefore, while cyberspace is on President Trump's agenda as an emerging field that needs U.S. attention, it is not receiving nearly enough money as other programs or departments and will not be able to reach its full potential of keeping the U.S. safe without a larger budget. Increasing the budget for cybersecurity through DHS will help offset the massive losses that the U.S. has already suffered due to cybercrimes and information theft. For instance, cybersecurity costs reach up to $4.13 million per company in the U.S. due to data breaches, malware attacks, and stolen information.[6] Not only would increasing the budget for cybersecurity diminish these losses through bolstering U.S. cyber defenses, but it would also create opportunities for a domestic industry that could benefit the economy rather than hurt it. This would also be a major initiative for President Trump that would be looked upon favorably by those in government who see cyberthreats as equally important or even moreso than military threats, as well as by tech companies in the U.S.

Perhaps in synergy with an increased budget, it is recommended that President Trump push Congress to propose new legislation that introduces cybersecurity and computer science programs as educational requirements for K-12 grades. As of 2015, 94% of children aged three to eighteen had access to computers, with 61% having online access as well. Many of those born into Generation Z are still in school and have grown up practically surrounded by technological advances. Generation Alpha, following Z, is composed of children who are born almost literally immersed into technology. Both generations are and will be incredibly influential and their skills and potential in the tech sphere is something to be embraced and built upon. Therefore, in schools, educating students on issues such as privacy, drone laws, and secure information will come hand-in-hand with what these children are already adept at using – technology. For more

[6] Sobers, Rob. "60 Must-Know Cybersecurity Statistics for 2019." *Inside Out Security*, 17 Apr. 2019, www.varonis.com/blog/cybersecurity-statistics/.

conventional learning, cybersecurity exercises can easily be paired with other lessons learned, such as comparing malware to getting sick due to not washing hands.[7] Providing training to educators across the U.S. and having a federally organized cybersecurity learning program included in the required curriculum of all schools in the nation will undoubtedly prepare current and future generations to tackle the issue of cyberattacks and strengthen U.S. national security in the long-run. Learning safe cybersecurity habits early on will first provide children with greater online security in an age where information is too easily accessible and manipulated, and second, will inspire younger students to pursue a cyber-related career in their future.[8]

While cybersecurity education training programs already exist, it is difficult for a majority of U.S. schools to both provide professional training for educators as well as afford the necessary equipment for students to interactively learn about cybersecurity and other STEM related topics. With the president's backing of a congressional mandate that requires these concepts to be taught in schools from kindergarten to high school, more funding will be provided to schools across the nation for training and equipment that will contribute positively to the nation's economy and security in the long-term as more students will enter one of the fastest growing fields in today's world. Indeed, many experts believe that "the early stages of future wars will be conducted online as hackers take out key national infrastructure like power grids, banks and core government systems" but that "governments around the world have [a severe skills shortage] when trying to deal with cyber warfare."[9] In order to combat this shortage and

---

[7] Barack, Lauren. "Cybersecurity a Must in Curriculum in Increasingly Digital Classrooms." *Education Dive*, 9 Jan. 2019, www.educationdive.com/news/cybersecurity-a-must-in-curriculum-in-increasingly-digital-classrooms/545336/.

[8] Dawson, Howard. "Why it is Vital that we Teach Cybersecurity in our Schools." *Emerging Education Technologies*, 5 Feb. 2019, www.emergingedtech.com/2019/02/why-it-is-vital-that-we-teach-cybersecurity-in-our-schools/.

[9] "The Importance of Teaching Cyber Security in Schools - Panda Security." *Panda Security Mediacenter*, 26 June 2017, www.pandasecurity.com/mediacenter/news/cyber-security-school/.

exponentially grow the number of security and IT experts trained to defend our nation's defenses, cybersecurity must be a required part of the national education system.

In addition to making cybersecurity education mandatory, President Trump must make extra efforts to increase cybersecurity collaboration between the federal government and private security companies. According to the Council on Foreign Relations, a "private sector-centric" approach, or the "Home Depot" model, could serve as a successful method for the government and the private sector to work together on cyber issues while still maintaining a balance in responsibilities and preventing governmental overreach. For instance, with this approach, private companies would be able to build and spend on their own network defenses while relying on the government to help in areas in which private companies have less power, such as "investigat[ing] and prosecut[ing] cybercrime, apply[ing] diplomatic pressure on other countries to stop engaging in economic espionage, us[ing] economic sanctions, […] collec[ting] intelligence, and defend[ing] United States [national security from major] events."[10]

If President Trump were to play a larger role in federal and private cybersecurity relations, not only would the government be able to assist private companies in areas that are less accessible to them, but increased information sharing and cooperation would benefit the cybersecurity market, allowing private companies to focus more on creating new products and technologies.[11] President Trump has the power to issue an executive order that allows for increased information sharing, but even without using his executive power, the president can

---

[10] "Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model." *Council on Foreign Relations*, Council on Foreign Relations, 31 Mar. 2015, www.cfr.org/blog/private-sector-and-government-collaboration-cybersecurity-home-depot-model.

[11] "Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model." *Council on Foreign Relations*, Council on Foreign Relations, 31 Mar. 2015, www.cfr.org/blog/private-sector-and-government-collaboration-cybersecurity-home-depot-model.

encourage and foster a relationship between private companies and the federal government by providing aid when needed, discussing strategies and cyber developments with cybersecurity experts in the field, and indirectly protect private networks through the use of diplomacy and power-projection abroad. President Trump's initiative to strengthen the cooperation between the government and the private sector will also pave the way for future presidents to be able to turn to private companies for cybersecurity information, as well as for private companies to have confidence in the government in times of high threats and attacks by foreign countries.

To conclude, due to the rise of cyberattacks against critical U.S. infrastructure and information systems, it is imperative that President Trump approach cybersecurity with greater attention and enthusiasm. Many departments, organizations, and private start-ups have been created over the years by various presidents, leaders, and CEOs, but due to the recent increase in foreign cyberattacks, specifically by China, cybersecurity deserves new and improved vigor. The safety of the U.S. and its citizens will be at stake if cybersecurity is not considered one of the most major security threats facing the nation today. Therefore, it is recommended that President Trump increase the funding for cybersecurity through the Department of Homeland Security, push for legislation mandating that cybersecurity and computer science programs be required in schools, and finally, stimulate more collaboration between the federal government and private security companies in the field of cybersecurity.

Bibliography

Barack, Lauren. “Cybersecurity a Must in Curriculum in Increasingly Digital Classrooms.” *Education Dive*, 9 Jan. 2019, www.educationdive.com/news/cybersecurity-a-must-in-curriculum-in-increasingly-digital-classrooms/545336/.

“Cybersecurity Programs.” *Department of Homeland Security*, 10 Oct. 2018, www.dhs.gov/science-and-technology/cyber-security-division.

Dawson, Howard. “Why it is Vital that we Teach Cybersecurity in our Schools.” *Emerging Education Technologies*, 5 Feb. 2019, www.emergingedtech.com/2019/02/why-it-is-vital-that-we-teach-cybersecurity-in-our-schools/.

Johnson, Derek B. “House Homeland Committee Wants More Cyber Funding for DHS.” *FCW*, 15 Apr. 2019, fcw.com/articles/2019/04/15/dhs-cisa-funding-letter-johnson.aspx.

“President's Fiscal Year 2020 Budget.” *Department of Homeland Security*, 19 Mar. 2019, www.dhs.gov/news/2019/03/18/president-s-fiscal-year-2020-budget.

“Private Sector and Government Collaboration on Cybersecurity: The Home Depot Model.” *Council on Foreign Relations*, Council on Foreign Relations, 31 Mar. 2015, www.cfr.org/blog/private-sector-and-government-collaboration-cybersecurity-home-depot-model.

Sobers, Rob. “60 Must-Know Cybersecurity Statistics for 2019.” *Inside Out Security*, 17 Apr. 2019, www.varonis.com/blog/cybersecurity-statistics/.

"The Importance of Teaching Cyber Security in Schools - Panda Security." *Panda Security Mediacenter,* 26 June 2017, www.pandasecurity.com/mediacenter/news/cyber-security-school/.

"Trump Creates CISA, Official Federal Cybersecurity Agency (Multi-Video)." *American Security Today,* 23 Nov. 2018, americansecuritytoday.com/trump-creates-cisa-official-federal-cybersecurity-agency-multi-video/.

Wolf, Richard. "Bush Calls for Tighter Cybersecurity." *ABC News*, 15 March 2008, https://abcnews.go.com/Technology/story?id=4457451&page=1.