Cybersecurity Education; Political Implications

Robert Timmons

School of Cybersecurity

CYSE 425w: Cybersecurity Strategy and Policy

Professor Bora Aslan

February 18th, 2025

Cybersecurity Education; Political Implications

Implementation of policy needs more than just pen and paper, requiring inquiry, research, debate, and support of the people. Policies usually have humble beginnings, starting out as basic ideas and loosely associated steps. As the internet and its technologies have exponentially grown, so has the need for political responses to protect and define the cyber landscape. Policy makers have enacted cyber policies and laws at all levels of government, from state to Federal. With the uptick in these cyber related policies, many industries, public and private, local and international have been affected. Cybersecurity education as a policy is very broad, covering vast domains and topics, so it too has been subjected to political wills and scrutiny. Politicians debate, lay out opinions, and produce actionable legislation based on policies like cybersecurity education. This paper aims to highlight state and Federal political actions based on the policy. The paper will also discuss how there's still a long way to go, and current political action may not be enough. Policy is more than just words on paper, requiring debate and deep understanding. With the information age and its new and advanced technologies, there's a need for policy makers to swiftly respond to new dynamic challenges.

Before looking at the larger national policy, it would be fitting to first delve into a local, state level political response. The state of Virginia has been at the forefront of cyber; being close to the United States capital of D.C and having the second largest data center in the Americas; Virginia has had the need for sound cyber policy. During Governor Terry McAuliffe's administration, Virginia began taking serious action to better solidify its cyber security posture. The Virginia Cyber Security Commission was one of these endeavors, established to "…identify high-risk cybersecurity issues facing the Commonwealth of Virginia, provide suggestions for more secure network plans and procedures, offer response strategies and best practices for the

State, promote cyber hygiene, help facilitate the presentation of cutting-edge science and technologies in the cybersecurity realm, implement state cyber assessments, and contribute to the over to the overall cyber-safety of Virginia as a whole." (Spidalieri, 2015) Part of their lengthy mission statement included stipulations for educational awareness. Dubbed the Cyber Security Partnership, or CSP, it has in recent years leveraged a multitude of public and private sector experts to further cyber security education. The CSP has provided support for colleges, Virginian-based corporations, and other state entities for their cybersecurity missions. They've accomplished this through info sharing arrangements and cyber-based professional development courses. CSP has provided platforms to send information pertaining to recent attacks or defense new defense policies and measures, allowing other entities to create training material based off this information. The professional development aspect helps foster and fund groups to cyber professionals and aspiring students to interact with one another. The CSP and VCSC are unique, being a "ground up" approach to cyber awareness and education that many states do not have. With a better understanding of a state level response to cybersecurity education, it's important to now dive into the Federal government's reactions.

The Federal government has spent decades playing catch up against hackers, with policy makers drafting legislation and frameworks to combat ever-growing cyber threats. As a reaction to cyber-attacks and lack of knowledge of threats, the National Institute of Standards and Technology has created sub-groups in its organizational structure to better facilitate educational opportunities. Policies makers like Dr. Laurie E. Locascio, head of NIST, have led the charge in the creation of programs like NICE, or the National Initiative for Cybersecurity Education. NICE aims to develop and foster cyber programs in both high school and colleges across the country. Reports reinforce this point, stating NIST "… has collaborated with high schools and colleges to

design courses and programs that will attract students and provide them the training that befits a cybersecurity specialist." (Conklin et al., 2014) Acting as a reference model, NICE defines competencies, skills, and positive traits sought after in the cyber workforce. More specifically, it lays out job roles, such as penetration testing, forensic analysis, or network administration, and maps skills that the role requires. NICE benefits not only individuals seeking work in these fields, illuminating what the job entails; but also, government and private organizations, enabling them to develop standardized training curriculum based around NICE's frameworks. Federal government action is not only breeding the next generation of cyber professionals but also raising awareness and public conscious of current cyber threats. Knowledge is power, and in the realm of cybersecurity every bit of information counts.

On top of the NICE program, the Federal government bureaus have been assisting in the cyber knowledge effort. The NSA and DHS have been tasked to jointly work together in the efforts of enhancing cyber education. This speaks to the increasingly priority set on educating the public on cyber threats, with politicians and policymakers increasing the number of organizations set on cyber education. This idea is reinforced through a paper documenting increases in government action in the cyber realm, "Furthermore, institutions hosting cybersecurity or related disciplines should establish a center for cybersecurity education to offer guidance and promote collaboration among academia." (AlDaajeh et al., 2022) Circling back to the NSA and DHS, they currently manage the Centers for Academic Excellence. This institute contains various academic tracks for cyber, working on technical responses to attacks to cyber education policy. These centers operate at undergraduate and graduate levels, with other programs outside of the university. Despite all these efforts to build a better understanding of cybersecurity threats, there is still tons of work to be done. Businesses don't feel the ever-present threat of cyber-attacks,

only fixing them after the fact. To put it bluntly, the consequences of the implemented policies won't be felt for at least the next two decades. There are still a myriad of old protocols and devices that are still standard practice in many businesses. Policymakers and politicians have built a sound foundation, but it will take time to truly see the fruit of their labors.

Cybersecurity education has made leaps and bounds the past two decades. This is in part due to state and federal governments alike drafting frameworks to assist the policy in growing. Programs like the Federal government's NICE or Virginia's VCSC are a solid start to educating the public and providing resources for businesses, educational institutions, and other government organs. As politicians raise alarm bells on the threats of cyber-attacks, we will see more and more government departments gearing towards cyber and the production of education materials, as seen with the NSA and DHS. As previously stated though, this continuing education will be a slow process, as businesses don't feel the sting of cyber threats until its too late. Politics is a slow, grueling process, with tons of chaos and uncertainty. Political responses to the increasingly complex issues faced in cyberspace will become necessary as we barrel through the information age.

References

Spidalieri, F. (2015, January 1). *State of the states on cybersecurity*. Academia.edu. https://www.academia.edu/34265508/State_of_the_States_on_Cybersecurity

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). *Re-engineering cybersecurity education in the US: An analysis of the critical factors | request PDF*. ieeexplore. https://www.researchgate.net/publication/262165260_Re-engineering_Cybersecurity_Education_in_the_US_An_Analysis_of_the_Critical_Factors

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022, May 18). *The role of National Cybersecurity Strategies on the improvement of Cybersecurity Education*. The role of national cybersecurity strategies on the improvement of cybersecurity education. https://www.sciencedirect.com/science/article/abs/pii/S0167404822001493