The Missing Piece of Cybersecurity Education, from an STS Perspective

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

Jason Lee

Spring 2024

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

Pedro A. P. Francisco, Department of Engineering and Society

Introduction

Recently, on January 31st, 2024, a congressional hearing was held with several CEOs of massive tech companies (Discord, Snapchat, Facebook, TikTok…) regarding monopolistic practices and protecting children online (Kern et. al, 2024). Congressional legislation, ranging from the second half of the 1990s to 2018 and beyond, has attempted to do this before with legislation such as the Communications Decency Act (CDA), the Stop Online Piracy Act (SOPA) and the Allow States and Victims to Fight Online Trafficking Act (FOSTA) (Kozak, 2018). However, several soundbites from hearings such as the Facebook/Cambridge Analytica hearing ("Senator, we run ads"), and the off topic remarks of the most recent hearing (such as the relentless questioning of TikTok CEO Shou Zi Chew's political ties (Leal, 2024)) have demonstrated one key fact: congressional members have very little knowledge on how the internet is run and operated.

Lawmakers are not opposed to big statements, especially those that are as highly televised and politicized as a congressional hearing. In the most recent hearing, there was a moment of bipartisan unification where Republican and Democratic senators both condemned the tech companies equally on their failure to protect children from harm (Rosenblatt et. al, 2024). However, congress itself is very slow to pass or repeal any legislation regarding tech, and to a lesser extent cybersecurity.

Along with this, some congressional members fundamentally lack the knowledge required to properly investigate and interrogate defendants on their misuse of technology. A somewhat dated example is an argument against net neutrality by Ted Stevens, who described the internet as a "series of tubes" (Seitz, 2022). While it's true that broadband connections and data can be thought of as a series of tubes of differing sizes, his depiction of the information (and also

his mistaking of email and internet) was a very rudimentary description. Ted Steven's analogy would be more accurate to how networks operated, yet his argument on how Netflix and emails would interact is highly exaggerated. However, other congressional lawmakers are much less aware about popular internet applications and how they function. For example, at the Facebook/Cambridge Analytica congressional hearing, Sen. Orrin Hatch asked how Facebook makes its money, when it offers its services for free (Watson, 2018). Facebook CEO Mark Zuckerberg replied, "Senator, we run ads" after a bewildered pause. Many internet users (especially on social media platforms such as *X* (formally Twitter)) were quick to point out the congressman's age and mock him for being behind the times (Burch, 2018).

This last point demonstrates a fundamental fact: People who have lived with (and on) the internet have intrinsic knowledge, or common sense of how the internet is run. They have tacit knowledge on how everything works. There exists a generational cultural lag where older generations are less adaptive to newer technology compared to the rapid speed and growth of said technologies. Older generations are slower to adapt technologies, yet they are less likely to be the victim of cybersecurity threats (Brett, 2021). Whether it is due to a lack of life experience or overconfidence in their tech savvy-ness, there's a gap in knowledge that leaves them vulnerable to these attacks. In order to better our Internet and cybersecurity education, work must be done in bridging the gap between those exposed to the technology and those far away from it. To facilitate the diffusion of innovation, we should approach education by tackling tacit knowledge first, before exposure to any complicated and complex concepts.

Background

Lawmakers, government officials (specifically the NSA), and technology companies have been in contention with each other for quite some time. Lawmakers, lobbied by media companies, attempt to prevent internet privacy by implementing strict copyright, while the NSA/FBI attempt to undermine information security in order to maintain national security (whether it be through surveillance or other methods). While the NSA/FBI are quite aware of the cybersecurity risks and don't care much for them, lawmakers (most often) are unaware of problems that their legislation may cause.

SOPA and PIPA are two legislative acts that caused several technology companies to go completely dark in protest (Belleville, 2012). SOPA and PIPA would give media companies the power to take down any internet website for any copyrighted content, including those that are user-generated. One of the most dangerous parts of this bill is the power to edit DNS (Domain Name Systems) servers of popular websites if they violate copyright guidelines. By wiping the DNS of a popular website which hosts user-generated content, this leaves a hole that can be used by malicious users to masquerade as the website themselves by snatching up the DNS number of the now-defunct website. The massive privacy risk and identity theft available from these types of attacks would have fundamentally crippled and led to the death of the internet as a whole.

Along with this, government agencies are often hypocritical about how to handle cybersecurity. The NSA wants to strengthen encryption from attacks outside of the United States, but wants the power to track individual peoples via surveillance and security weaknesses in technology. One recent example is Foreign Intelligence Surveillance Act Section 702, intended to collect intelligence on terrorist cells and foreign nationals while also protecting the rights of US citizens to privacy (Gemar 2020). However, this act was used by the FBI and other government agencies and personnel to unlawfully obtain information on US nationals whose

information was collected in the past. A more public example is Apple vs. the FBI in the wake of the San Bernardino mass shooting, where Apple refused to assist the FBI in unlocking the work phones of one of the shooters (Nakashima, 2016). Apple's refusal stemmed from a court order that Apple claimed would "create and install a backdoor" that would compromise most or all of Apple's products. The court order specifically used a more than 200 year old piece of legislation (All Writs Act of 1789) to justify the creation of a version of the iOS operating system that would bypass some security functions, such as unlimited password attempts, and electronic input of passwords (Chesney, 2016). Cybersecurity experts and Apple CEO Tim Cook, have pointed out the problem with this new, theoretical OS system: If created, it can be used again by someone else (Burgess, 2016). While the FBI have noted that they would delete the OS as soon as they obtained the information from the phone, the mere creation would spur attempts to recreate the exploit, which would have Apple security and privacy personnel scrambling to patch it before it has a chance to propagate through to other iPhone users.

Shifting gears, we now discuss the state of cybersecurity education. As the internet and cybersecurity is a constantly growing field, cybersecurity and internet education from 20 - 30 years ago cannot be used effectively in today's modern classrooms. Along with this, aside from learning how to use word processing and presentation systems such as Google Drive or Microsoft Word, most schools don't teach children how to explore the world in a safe manner. Some schools teach typing classes, others have full computer science courses, others relegate coding to club activities, and the rest do not have access to school-funded computers or educators. According to Yadav et. al (2016), one of the major limiting factors is the lack of computer science educators around the world, meaning schools who want to offer these courses are unable to create, much less update their computer science curriculums. There are 2

consequences to this. Children with access to technology learn tacit knowledge and rules about the internet, sometimes without adult supervision. While learning by experience is effective, this could lead to children being exposed to harmful situations, as discussed in the January congressional hearing. However, children without access to technology (such as those of lower SES (socio-economic status)) lose the tacit knowledge on how to navigate the internet safely. With our society rapidly orienting itself to own at least 1 personal computing device per person, this would mean that these children would be at a disadvantage as they grow up and join the workforce. These future workers can also be a source of security risk, as they are less experienced with experiences such as phishing and/or social engineering attacks. This means that there's an inherent disadvantage when a child manages to get into higher education from a lower SES, due to their inexperience with the internet. We must bridge this cultural lag (both in age and SES) and provide tacit knowledge to those who never experienced this type of technology for themselves in order to create a more equal society.

Methodology

My methodology combines several different sources of information and attempts to synthesize them using the analytical framework of the diffusion of information.

First, analysis of surveys of tech literacy is a good stepping point to discover where the cultural lag may be. While older generations and lower SES are primary candidates, we may be able to discover that there are several other areas that experience this cultural lag as well.

Second, a literature review involving recent and outdated laws involving digital technology, along with educational curriculums in both K-12 and university settings will shed light in two separate areas. Review of the laws can assess the speed and effectiveness at which

cybersecurity legislation is being passed, while a review of the educational curriculums can show what areas of technology younger generations are being taught, while highlighting which significant areas are missed. To format this into my research question, I will use diffusion of information to discover which variables most affect technological literacy, which I will use as a guideline of how fast an area adopts the internet and its applications. The variables I've identified before the research was conducted was tacit knowledge and cybersecurity/tech literacy education To further my analytical framework of the diffusion of information, I will apply this to a case study, specifically of SOPA and PIPA's main contributors and opponents.

Literature Review:

Grant (2010) dissects the issue of cybersecurity legislation and discusses at length about the issues behind a distinct lack of congressional and legislative action regarding cybersecurity. He discusses several issues, such as the lack of clear and standardized cybersecurity arrangements when it comes to agencies of the executive branch. He notes in reviews of FISMA (the Federal Information Security Management Act), there are little actions being done to improve security, including a lack of testing of vulnerabilities, failures of defining responsibilities, and recognition of new technologies, threats, and network architectures. The lack of standardization (in terms of both testing and implementation of systems), especially when the industry itself has created its own standardization for keeping systems secure, is a serious risk. Generally speaking, a broad approach to a complicated topic can be useful, such as the IETF's "rough consensus and running code" approach when handling internet architecture (Ohta, 1998). However, a lack of regulation, guidance, and maintenance of these practices will not create a secure system.

Grant (2010) also cites an issue with congressional action, stating that congressional action is quicker with an outside motivator (such as the 9/11 attacks). Along with this, he states that cybersecurity issues, such as data breaches, denial-of-service attacks, and other possibly crippling cyberattacks, are not significant enough in perceived stature or prolonged disruption to become a motivating factor, even though the perpetrators could be large nation-states attempting to bring down critical infrastructure. This lack of wariness for potentially devastating attacks can be due to multiple issues, such as the constant nature of these attacks (desensitization) or just a general lack of knowledge about what is possible for attackers to do. Providing enough training to build intrinsic knowledge could bring cybersecurity issues to the forefront of legislative action, or even bolster spending on cybersecurity education in the future.

Finally, There were two solution proposed in this article: create an agency large and adept enough to handle all cybersecurity issues (like the creation of the Department of Homeland Security after 9/11), or create a management system that standardizes the policies and procedures of all the departments that deal with cybersecurity issues (Grant, 2010). Lastly, he states that the industry has more expertise and resources to create these standards to keep the machines safe, which may be more effective than congressional action. Expertise comes with intrinsic knowledge that is not available to those unfamiliar with the technology, creating a gap that is unaddressable without the proper training and education. Reducing the need for training and education (by spreading this intrinsic knowledge) helps in our diffusion of innovation.

Next, let's address the intricacies of teaching cybersecurity education. A recent trend in cybersecurity training for youth is gamification, where several video games are created in order to engage younger generations and inspire a larger number to pursue a career in cybersecurity. A prime example is Jin et. al's (2018, February) 1-week summer camp and Purdue University

Northwest, where a large number of high school students attended sessions of educational gaming. They presented the project as a success, with a large number of participants saying that they would be interested in the field of cybersecurity in their exit surveys. However, there are several limitations. A majority of the male demographic enjoyed the gamification, while the female demographic were less enthusiastic about it.This gender difference in video game enjoyment could be caused by a simple issue: tacit knowledge. A study done in 2012 by Ghuman & Griffiths showed that a majority of gamers in most genres tended to be male. If this is the case, then the reason there may be less enjoyment could be due to a lack of tacit knowledge, something that can only be gained by experience playing the games genres mentioned in the paper (which was primarily tower defense) (Jin et. al, 2018, February). Along with this, while this particular camp highlighted the 51% makeup of underrepresented groups (African Americans and Hispanics), this diversity doesn't fully translate to every area, with under-funded and lower SES areas being areas that may struggle to implement this tactic. While this is great at recruiting a larger number of people into cybersecurity, the problem lies in diversity, and the lack of a diffusion of innovation due to SES. This problem also exists in cybersecurity competitions, as noted by Mouheb, Abbas, & Merabti (2019), as the competitions are great for companies to identify strong candidates for higher, yet lack in recruiting candidates that may be interested in the field. They also recommend that cybersecurity education be split into separate fields based on what the end goal of the student is, whether it be academia, industry, or government. The industry "demands for trained graduates rather than educated ones" (Mouheb, Abbas, & Merabti, 2019). While graduates have the knowledge behind the theories of attack and defense, they do not have the tacit knowledge nor training experience to implement and address threats as they occur.

Discussion

So, why is it so difficult to educate the general public/non-experts about cybersecurity? The difficulty behind cybersecurity can be explained by several factors. Cybersecurity is a constantly changing topic, and unless you have previous knowledge of what's happening, it is jarring and difficult to dive head first into the field. Cybersecurity requires several skills that don't just fall under the realm of computer science. While knowing how to code and knowing the principles behind how machines work can be helpful in understanding where these attacks come from, the knowledge to prevent phishing and social engineering attacks doesn't come from school lectures. Knowing the parts of the internet protocol do not teach you how to prevent someone from tunneling through the firewall and accessing sensitive data. Cybersecurity requires you to be adept with computers, the internet, and (most importantly) how the internet functions. This is how most people avoid clicking on fishy download links, blocking obvious scam emails, and avoid malicious malware. The knowledge of how to buffer overflow a program does not translate to the knowledge of figuring out whether THIS_IS_NOT_A_VIRUS.exe is a virus or not.

We are currently seeing a slow but steady diffusion of innovation from upper to lower SES, and groups that are underrepresented groups are getting more access to computers and technology. A large proportion of young people own a smartphone, and a majority of homes own a computer. However, those in poorer/rural neighborhoods have less access to these devices, leaving them with less experience and ultimately, less tacit knowledge. There may not be enough funding in these communities to create a robust or even miniscule computer science program, potentially diverting them away from a cybersecurity career (and therefore cybersecurity

education). If they did attempt to pursue computer science, they would be stricken with serious cultural lag: the social norms and values of the internet are not the same as those in real life conversations.

The same cultural lag applies when looking at the differences between younger and older generations. Older generations did not grow up with the same internet that younger generations had, and some didn't grow up with the internet at all. Some apps look and feel completely different from what they were before, such as YouTube and Facebook, and demographics that use these platforms are vastly different from one another. The internet has a diversity of communities of a vast number of age ranges, and each niche community has certain social norms that other communities dislike. One prominent example may be the use of emojis on certain platforms, where some platforms strongly dislike the use of common emojis while encouraging the use of other, more satirical ones such as the Moai emoji. This knowledge is tacit to me and many others who frequently use websites like Reddit.com, but aren't available to those who use other platforms such as YouTube or Instagram. In order to understand the social norms of the internet, you must use it and you must use it frequently. Ones who grew up on the current internet, fast-paced and ever-changing, are more adept and malleable to these changes. Those who grew up without or on a slower, more meticulous form of the internet are not used to these speeds, and therefore become out of touch and alienated. This results in cultural lag. While this example is purely based within social media, innovation regarding cybersecurity changes just as rapidly. Those who are not in the loop and in the know about new exploits and vulnerabilities will not be able to defend themselves. The younger generation are more prepared for a cyberwar due to their adaptive behavior, while the older generation falls behind if not trained or educated in the field.

Conclusion:

Education non-experts on a topic as complicated and interdisciplinary as cybersecurity is a difficult task. In order to even begin accomplishing this, everyone who wants to learn must have a baseline understanding of how computers work, how the internet works, and how to avoid malicious threats. To facilitate the diffusion of innovation in the realm of cybersecurity, work needs to be done in bridging the cultural gap between generations and between higher/lower SES, brought about by a lack of tacit knowledge about how quickly the internet can change and adapt.

Exactly how can this be accomplished? The first and most important step is to expose as many people to the internet as possible, which is currently being done in the United States with programs designed to give underprivileged communities access to the internet and other modern commodities. The second step in promoting education is motivating the public to pursue computer science and cybersecurity. This could be done in several ways. My personal recommendation is to improve gamification of cybersecurity topics (as discussed earlier by Jin et. al (2018, February)), as this will entice younger generations to further explore the topic. However, this will not work for older generations who have little motivation to participate in internet activities. For these older generations, there needs to be an effective course or system in place to give them hands-on experience in being more aware of threats on the internet. For this, a possible approach could be to use a virtual environment to guide older generations on how to spot malicious or fake website links, how to navigate the internet in general, etc. Another possible exercise that can be done in a virtual environment is showing the possible effects of computer viruses and malware on a device, where it may hide itself, and other general safety tips

demonstrated through a "what *NOT* to do" approach. This would not only inform the student of how malware can work and operate, but also teach them tips on how to avoid getting in the situation in the first place.

All of the above recommendations attempt to allow for a smoother, more even diffusion of innovation throughout our society. Their main goals are to provide tacit knowledge for individuals unfamiliar with the internet environment, and to bridge the cultural gap between generations. In order for any of this to happen, however, there must be nationwide implementation of these practices in schools and homes, which requires further action by congressional representatives and the Department of Education. Strengthening the weakest link (the user) is key to creating more secure systems and critical infrastructures, while also bolstering cybersecurity defenses.

References:

Al Daajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Belleville, M. (2012). IP wars: SOPA, PIPA, and the fight over online piracy. *Temp. Int'l & Comp. LJ, 26*, 303.

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training. *2016 IEEE 39th Annual Computer Software and Applications Conference (COMPSAC)*, 1-6. https://doi.org/10.1109/COMPSAC.2016.257

Brett, A. (2021, October 4). Study: Millennials and gen Z say they are bigger victims of Cybercrime. *GlobeNewswire News Room*. https://www.globenewswire.com/news-release/2021/10/04/2307751/0/en/STUDY-Millennials-and-Gen-Z-Say-They-are-Bigger-Victims-of-Cybercrime.html

Burch, S. (2018, April 11). Senator Orrin Hatch shocked to learn Facebook makes money off ads. *TheWrap*. https://www.thewrap.com/senator-orrin-hatch-facebook-biz-model-zuckerberg/

Burgess, M. (2016, February 17). Why Apple is right to refuse an FBI demand to crack a killer's iPhone. *Wired UK*. https://www.wired.co.uk/article/why-apple-refuse-help-fbi-iphone

Chesney, R. (2016, February 22). Apple vs. FBI: ‘Going Dark’ dispute moves from Congress to the courtroom. *Lawfare*. https://www.lawfaremedia.org/article/apple-vs-fbi-going-dark-dispute-moves-congress-courtroom

Conklin, W. A., Cline, R. E., & Roosa, T. (2014, January). Re-engineering cybersecurity education in the US: an analysis of the critical factors. *2014 47th Hawaii International Conference on System Sciences*. IEEE. https://doi.org/10.1109/HICSS.2014.256

Gemar, S. (2020). A Crucial Aspect of National Security in Need of Reform: Section 702 of the FISA Amendments Act. *SDL Rev.*, *65*, 489.

Ghuman, D., & Griffiths, M. (2012). A cross-genre study of online gaming: Player demographics, motivation for play, and social interactions among players. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 2*(1), 13-29. https://doi.org/10.4018/ijcbpl.2012010102

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn), 12*(1), 150-158. https://doi.org/10.11591/edulearn.v12i1.9203

Kern, R., Reader, R., Chatterjee, M., & Mui, C. (2024, January 31). Senator to Big Tech: 'Collectively, your platforms really suck at policing themselves'. *Politico*. https://www.politico.com/news/2024/01/31/senate-grills-zuckerberg-other-tech-ceos-on-kids-safety-failures-00138718

Kozak, Nadine Irène. "Fighting for the internet: online blackout protests and internet legislation in the United States, 1996-2018." *M/C Journal* 21.3 (2018).

Leal, Isabela Espadas Barros (2024, February, 1). Sen. Tom Cotton faces backlash for repeatedly asking TikTok's CEO about his citizenship, *NBC News*, https://www.nbcnews.com/news/asian-america/tom-cotton-backlash-tiktok-ceo-shou-chew-rcna136673

McClure, R. F., & Mears, F. G. (1984). Video game players: Personality characteristics and demographic variables. *Psychological Reports, 55*(1), 271-276. https://doi.org/10.2466/pr0.1984.55.1.271

Nakashima, E. (2016, February 17). Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. *The Washington Post.* https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

Office of Educational Technology. (n.d.). Infrastructure. *Office of Educational Technology*. https://tech.ed.gov/infrastructure/

Ohta, M. (1998). IETF and Internet standards. *IEEE Communications Magazine*, *36*(9), 126-129.

Redman, S. M., Yaxley, K. J., & Joiner, K. F. (2020). Improving general undergraduate cyber security education: A responsibility for all universities? *Creative Education, 11*(12), 2541-2552. https://doi.org/10.4236/ce.2020.1112189

Rosenblatt et. al (2024, January 31). Senate hearing highlights: Lawmakers grill CEOs from TikTok, X and Meta about online child safety. *NBC News*. https://www.nbcnews.com/tech/live-blog/senate-hearing-online-child-safety-big-tech-live-updates-rcna136235

Seitz, N. (2022, January 14). A remembrance and defense of Ted Stevens' "series of tubes." *PCMag*. https://www.pcmag.com/news/a-remembrance-and-defense-of-ted-stevens-series-of-tubes

U.S. Department of Education. (2022, October 5). Department of Education announces K-12 cybersecurity resilience efforts. *U.S. Department of Education*. https://www.ed.gov/news/press-releases/department-of-education-announces-k-12-cybersecurity-resilience-efforts

Watson, C. (2018, April 11). Mark Zuckerberg's testimony to Congress: the key moments. *The Guardian*. https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Yadav, A., Gretter, S., Hambrusch, S., & Sands, P. (2016). Expanding computer science education in schools: understanding teacher experiences and challenges. *Computer Science Education*, *26*(4), 235–254. https://doi.org/10.1080/08993408.2016.1257418