Kris Vargas

POLS 426

# Cyber War Project Paper

How can we build a safer cyber world?

The impact that technology has had on the world cannot be understated in any way. This can be seen in everyday tasks and activities, such as being able to facetime your friend that lives across the globe, having access to millions of movies on a handheld phone, and unlocking your digital devices with so much as looking at your screen (face ID). The convenience and joy that technology has brought to the leisure and entertainment sectors of our lives has been exponential, and tech as a whole has become very much ingrained in our daily existence. But with this rise in overall prominence, technology has also become the popular mode of choice for more nefarious activities as well. This includes things such as cyber crime and cyberwarfare, both of which have contributed to the cyber world, which was at one time regarded as a relatively safe place, transforming into a dangerous and tricky landscape for users to navigate. This is an unfortunate reality of human nature, as the modern convenience and accessibility of the Internet and technology can also be applied to engaging in criminal activity on a digital scale. Just as it is possible to video call a loved one from across the globe, it is just as possible to be a victim of fraud or identity theft by a criminal thousands of miles away.  What makes this even more complex of an issue is that added difficulty in tracing some of these crimes, as the lack of a physical act means that finding and persecuting those who are responsible now requires digital investigations. With all of these factors considered, it might seem to some that the cyber world as a whole is better off to just be completely avoided. But all hope is not lost for a safer digital realm for all in the world to enjoy equally. There are various steps and processes that can be completed in order to achieve this new and improved cyber world.

One of the largest contributing factors to the cyber world being viewed as "dangerous" is simply the lack of proper education for the masses on browsing and using the Internet. With the continued growth and involvement of the digital realm in our everyday lives, it is paramount that more time be spent teaching people on how to be safe and protect themselves when online. The majority of people currently serve as the perfect victims for conspiring cyber criminals, as they are unaware of some of the warning signs of potential scams and the digital etiquette to practice when using the Internet. A simple and very plausible solution for this issue would be to integrate cyber-safety related topics into school curriculums from a relatively early age. Kids nowadays are digitally connected and active from extremely young ages, for better or for worse. Though some parents may choose to go the route of "no devices" to try and protect their children, it is not the most forward-thinking line of action to deal with this issue. The more beneficial and productive solution is to have their children properly educated on the dangers of the Internet, the types of crimes that can be committed digital and warning signs of each one, and how to protect oneself when using the Internet. Having this taught from a young age will gradually lead to a general population that is much more aware and informed regarding the threats of the cyber world, which directly correlates to a safer cyber world for all. As discussed in an article covering a social experiment that was seeking to confirm the trend of more young kids being exposed to high levels of internet access in the British Journal of Educational Technologies, a high percentage of children around the globe are now experiencing increased levels of Internet access. As such, the article goes on to support the line of thought that there is a pressing need for more cyber-safety education geared towards pre-school aged children.

As the growth of technology and digital means continue on their inevitable path of advancement, it will become increasingly difficult to provide means of safety and regulations on a large scale. This is where the industry of cybersecurity must be properly supported in order to keep up with these increasing demands of the cyber world. Cybersecurity itself seems to be an already rapidly growing field with more and more incentives for people to seek to join, such as high-paying positions and flexibility in terms of work-life balance, but there seems to be even more room for growth as a whole. In reality, cybersecurity below the federal level is mostly lacking when in comparison to the strides being made in the technological world. Stated in "Countering the Cyber Threat" by Henry and Brantly, "Below the federal level, most states and larger cities are only now just beginning to develop internal cybersecurity capabilities, while most counties and local municipalities have long been woefully ill-equipped to deal with a cyber domain that is quickly facilitating constituent services delivery". More and more financial resources must be set aside to be directly allocated towards the cybersecurity sector. It is unacceptable for a country such as the United States to be lagging this far behind in terms of Cybersecurity given their resources as a superpower. Consequentially, it is unreasonable to expect for a safer cyber world to develop within addressing this lack of cybersecurity infrastructure. However, the issue with the Cybersecurity industry is not just resolved through increasing funding. There is a glaring issue of fragmentation that is pertinent in the world of Cybersecurity. As also stated in "Countering the Cyber Threat" by Henry and Brantly, "…to advance Cybersecurity, there needs to be a consensus across the public and private sector." There is a recurring theme of a lack of planning and coordination between the different levels of government and sectors within the country. Without proper communication between all of these separate entities, it can be assumed that the Cybersecurity industry as a whole will fail to reach its full potential within the borders of the United States. But if these issues are properly addressed, the growth of the industry will be exponential, therefore contributing to a safer Cyber World.

To go hand in hand with the bolstering of Cybersecurity, harsher penalties may also be in order for those who choose to engage in illegal activities on the Internet if a safer Cyber World is the end goal. This applies to traditional forms of cybercrime, such as identity theft or fraud, but also applies to other more severe forms of cyber terrorism as well. There are already what some would consider "harsh" penalties for engaging in cybercrime, ranging from minimal fines all the way up to $100,000 and jail/prison time (Greenspun Shapiro). The severity of the current penalties are dependent upon the exact scope of the crimes committed and their impact, but I would suggest that these punishments may need to be increased even more. As the Internet and technology has grown, so too has the impact that so of these digitally based crimes can have on innocent people. Entire lives can be ruined through a couple clicks of a computer, so the mode of the criminal activity should not lessen the punishment for the convicted criminals. These punishments and penalties should reflect and be on par with the ones that are placed upon "real-life" crimes such as robbery and assault to properly address just how large the consequences of these cybercrimes can get. By making these changes to the penalties and punishment for cybercrimes, this would dissuade more criminals from committing their heinous acts in the Cyber World, therefore helping to make the Cyber World a safer place.

As the Cyber World is to be thought of as a global entity, securing it will require international levels of cooperation. Though there is still work to be done within the confines of the United States as I alluded to in one of the previous paragraphs, a truly safe Cyber World will only be a result of all nations across the globe working together. As stated in "Cyber-Crime and

Cyber-Terrorism” by the International Institute for Counter-Terrorism (ICT), “One of the basic principles for dealing effectively with cyber threats and terrorist operatives is cooperation”. Though this is semi-present already in the workings of NATO nations, there is still a lot of room for growth when it comes to global union in terms of Cyber World policing. Two of the glaring obstacles in complete union in terms of global cyber policing are some nations being hostile towards one another and refusing to cooperate and the imbalance in global resources that have led to smaller and poorer nations being unable to participate. For the global resources issue, more powerful nations need to set aside their egos and make the effort to try and contribute what they can to these smaller nations in order to bring them up to speed. This is a beneficial interaction for all parties involved, as the smaller nation will receive the necessary help that they need to begin building a strong cybersecurity infrastructure and can in turn do their part when it comes to combating global cyberterrorism, which only serves to help all inhabitants of the Cyber World, which is the global population. For the issue of hostility between nations, this is mostly wishful thinking at the moment, as some hostility is long-standing and does not look to be easing up anytime in the future. But from an optimist’s perspective, one can only dream of these issues being put aside for the greater good of humanity in a Cyber context. And in hoping for a safer Cyber World, an optimistic point of view must be adopted anyway, so this is a logical dream to have.

In conclusion, building a safer and more welcoming Cyber World is no small task and will require immense time, resources, and planning. But in the end, it is a very necessary burden to undertake due to the current circumstances of the world and the projective future circumstances. So much of our everyday lives are already closely aligned with technology and the World Wide Web, and this close relationship will only continue to intensify as our civilization progresses over time. Though the process will not be simple, there are a couple concrete ways that we can begin to start building towards the end goal. As I stated in the previous paragraphs, one of these ways is get people to be better prepared to enter and become involved in the Cyber World. Education regarding cyber-related topics and safety should be more plentiful and should start earlier for all people. Children in particular are beginning to become active and acquainted with the Internet from a very young age, so it is important for them to begin to learn about the dangers and pitfalls that they may encounter.  This will in turn lead to a majority of the adult population being more cautious and informed about cyber threats when browsing the Cyber World, as they developed strong foundations as children. My second course of action for creating a safer Cyber World was to begin an overhaul of the entire Cybersecurity structure, particularly within the United States. It is an unfortunate reality that Cybersecurity in the United States is nowhere near where it should be in relation to where technology is right now. Not only does funding and resource allocation towards the industry need to be increased, but also the different individual entities involved in Cybersecurity need to be working together and in lock-step. The current fragmentation that is plaguing the Cybersecurity infrastructure between the private and public sector, as well as the federal, state, and municipal level governments is weakening the industry and holding it back from developing properly. Having all of these bodies communicating and moving forward in harmony will exponentially increase the growth of Cybersecurity in all aspects, which will in turn contribute to a safer Cyber World. My third concept to address for a safer Cyber World was to look into implementing harsher penalties for cybercrimes. Doing this will help to dissuade more petty cybercriminals from committing smaller acts and will serve to keep the more major criminals locked up and away from the Cyber World for longer periods of time. My fourth and final way to start building a safer Cyber World was continuing to increase the amount of international coordination between nations in countering cyberterrorism. Though it might be a long time from now, having mutual agreements towards combating cyberterrorism and cybercrime in general with current hostile nations such as Russia and China will do leaps and bounds towards solidifying policing power in the Cyber World. With all hands-on deck on a global scale towards combating cyberterrorism, this would be perhaps the largest and most impactful step towards building a safer Cyber World in the future for our children and their future children to experience to the fullest.

**Sources Cited**

Edwards, Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the internet : A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, *49*(1), 45–55. https://doi.org/10.1111/bjet.12529

Kramer, F. D., & Butler, R. J. (2019). A ROADMAP TO BETTER CYBERSECURITY. In *CYBERSECURITY: CHANGING THE MODEL* (pp. 5–20). Atlantic Council. http://www.jstor.org/stable/resrep20932.5

HONG, J. (2016). A PATH FORWARD TO A SECURE INTERNET OF THINGS. In *TOWARD A SAFE AND SECURE INTERNET OF THINGS* (pp. 8–11). New America. http://www.jstor.org/stable/resrep10509.6

Clarke, R. A. (2016). The Risk of Cyber War And Cyber Terrorism. *Journal of International Affairs*, *70*(1), 179–181. https://www.jstor.org/stable/90012602

Cerf, V. G. (2011). Safety in Cyberspace. *Daedalus*, *140*(4), 59–69. http://www.jstor.org/stable/23046914

International Institute for Counter-Terrorism (ICT). (2018). Cyber-Crime and Cyber-Terrorism. In *Cyber Report 24 September-November 2017* (pp. 23–27). International Institute for Counter-Terrorism (ICT). http://www.jstor.org/stable/resrep17687.7

*You could face stiff penalties under Virginia and federal laws if charged with an internet crime*. Greenspun Shapiro PC. (n.d.). https://www.greenspunlaw.com/library/federal-and-virginia-cyber-crime-charges-you-could-face.cfm#:~:text=Fines%20ranging%20from%20a%20minimal,addition%20to%20jail%20or%20fines.