The Future of Technology: What Cyber Threats are on the Horizon?

Arrington Goode

POLS 426

3/12/24 - 4/9/24

Introduction

Cyber crimes have grown exponentially throughout the last couple of years. With the rise of certain technologies, criminals have been able to expose and threaten institutions all over the world. Looking even further into the future can give some insight to how dangerous the cyber world could become. Many people do not often consider how important it is to be cautious of any new technologies that are being developed. Criminals are paying close attention as well. Moreover, the cyber crime world feeds off of new inventions. When someone creates a piece of technology that can make someone's life easier, a criminal sees an opportunity and a chance. In particular, there are three new technology advancements that could pose a huge threat to humanity in the near future. One is biometrics. Biometrics is the combination of the human body and technology. It is very dangerous due to the severity of the data within biometrics. Second, Artificial Intelligence cloning and replacement. We have already begun to see the rise of AI within every industry. This is only going to grow rapidly. AI is already used so frequently that it has the potential to take many jobs and careers away from the average citizen. On the security side, AI could be used in a variety of ways to steal information and commit cyber crimes. Lastly, ransomware is an emerging threat to many different nations across the world. Ransomware is a type of malware that can be disguised and sent as anything - most of the time it looks like a simple email. Criminals have worked hard at their ransomware so that nowadays, it is very hard to tell the difference between what is real and what is fake on the internet. These three pieces of the future pose a huge threat to security around the world. Each one comes with its own threats but also its own solutions. Developing a good plan for each one will give us a chance to combat any negatives that they may bring.

Biotechnology - Introduction

Biotechnology is the combination of biology and technology. This field of study is rapidly expanding. Technology mixing in with life is not a new concept, however it is becoming more and more dangerous. It is one of the newer technologies that we need to look out for. In a book by James Parrett, they explain how complex this area of study truly is. From the foods we eat to the blood in our systems, technology is being used to manipulate it. In the book, Parrett warns us of the potential dangers to national security. Different organizations can use biotech for nefarious purposes. They could potentially steal personal identifying information such as eye scans, blood work, and fingerprints. (Parrett, 2001) Not only could specific information be stolen but now the technology can be used against a certain group, company, or even a whole nation. This specific category of information is very sensitive. It can directly trace back to one person or one specific business. Having access to that type of data allows the criminals to directly target whoever they choose. It also means that many innocent civilians can get caught in the crossfire. Biotechnology, as the article explains, first started with DNA. Scientists wanted a way to map and manipulate genes and DNA within the human body - thus biotechnology was born. (Parrett, 2001) Moreover, biotechnology can be weaponized for today's use.

Biotechnology - Dangers

When discussing the subject of biotechnology, the potential dangers that it creates is at the forefront of the conversation. Continuing on throughout Parrett's article, we learn that biotech as a science is lethal because it has the potential to create new and lethal ailments to the human body. (Parrett, 2001) Technology, especially in the medical field, rapidly reduces research time. In this time, scientists have constructed potentially dangerous situations such as lab-born illnesses that the human body has a hard time fighting off. Since this type of science is heavily

intertwined with DNA and genomes, it is very easy to understand the types of threats biotech poses. Understanding the human body on a deeper level could also lead to weaponizing it. How does technology factor into all of this? Different technologies such as fingerprint scanners and medical equipment have been constantly improved to fit the changing times. Even now, face scanners and fingerprint scanners are prevalent within most smartphones. This technology is now in the hands of the everyday person. The technology is very easy to access and repurpose. All these dangers are very prevalent when the discussion of national security is brought up. Biotechnology has the potential to hurt a person on a small or large scale. Cyber warfare is growing and if an attacker were to target the everyday person, that person would have little to fight against this attack.

Artificial Intelligence - Introduction

The discussion around AI is mixed and nuanced. AI has opened a lot of doors when it comes to improving technology. However, AI also poses a great threat to our security. One example of this comes from an article titled, *The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms,* by Spyros Makridakis. In the article, the author mentions how impactful AI has become and how it has reached into every facet of human society. (Makridakis) When AI becomes a part of the conversation, many people have different reactions. Some find the technology to be a vital part of the future. Some other people, on the other hand, have weighed the benefits with the risks and come to a different conclusion. The ability to create intelligence and put it into a machine that is not human is a big risk. Now that technology can imitate human thought, it can transcend what we thought possible. Its “brain” can think of millions of scenarios in the time a regular person could do in the same amount of time.

Many professionals within the field have warned us about the types of dangers that are associated with AI.

Artificial Intelligence - Dangers

"Unemployment" and "wealth inequality" are some of the dangers that this technology poses. Unemployment has been a glaring issue even without the use of AI. However, AI can be used to complete tasks that would otherwise need a worker. Moreover, AI is becoming a lot more intelligent. The types of jobs that AI can do is ever expanding. (Makridakis) AI will not stop at "simple" jobs. It is starting to bleed into creative careers and higher level thinking. Many people believe that AI will be a true positive in our society. However, when we give technology human intelligence, the consequences are unknown. People will use this technology to cut corners in every department. When it comes to security, this technology can be used to quietly hack into nations and businesses across the globe. Since AI can do time consuming tasks, it can do things like password cracking and sending phishing emails. This technology does not tire nor need food or rest. In the book "Cyber Defence in the Age of AI," the authors talk about how nations around the world are increasing their cybersecurity measures. Criminals are also using these technological advancements to make their own attacks even more elaborate. AI can help aid these criminals and even come up with ways to infect their targets. AI can also think logically and find out ways around situations in half of the time a human could. Security on each and every level has to have a way to protect themselves against AI. Laws and policies also need to be established so that this technology is not misused. Cyber law is a vital tool when navigating a future that involves artificial intelligence. Current laws and policies do not fully cover AI due to the fact that we do not know the extent of AI ourselves. Everyday this technology becomes more and more refined. Each day it can do more and it can even do it better than most people. So much

so, that many people often have trouble discerning what is human-made and machine-made. If the line becomes blurred then what is to stop anyone from taking advantage of this.

Ransomware - Introduction

Ransomware is a dangerous technology that has only gotten worse over the years. In the past, when the internet was still new, ransomware was not as popular as it is now. In "The Ransomware Dilemma," the authors go over the history and future of ransomware and how it impacts us. In one passage, they discuss whether or not victims should ultimately give into ransomware and pay the demands. (Leo et al.) However, they are opening a dangerous door when they do this. Ransomware was invented to hold information for ransom in exchange for some kind of profit. Giving into the attackers demands ultimately shows them that they can continue this behavior and get away with it. Then, it could potentially snowball into a much larger scheme. When future technologies are discussed in terms of security, ransomware is often left out of the conversation. Criminals have reversed engineered ransomware so that it is much more effective now. Stealing information and then holding it until you get what you want is a practice that has evolved and has now become a future technology that we should be on guard against.

Ransomware - Dangers

When it comes to security and the future of cybersecurity in general, ransomware is a big aspect to consider. As previously mentioned, giving into ransomware could potentially lead to more in the future. If a cybersecurity team can not find the attackers, then they can take what they have learned from one attack and use it for future attacks. In "The Ransomware Dilemma," the authors speak on the underinvestment in cybersecurity teams across the board and how they directly feed into this issue. From a security perspective, ransomware could lead to many more

issues than what meets the eye. Ransomware takes one thing into account that other types of attacks do not - social engineering. Ransomware relies on people and how connected and desperate they can be. Social engineering is a very complex concept. The manipulation of people within cyberspace is a tool that is used often without anyone truly knowing. In "Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations" the author suggests a radical approach when it comes to researching and solving the social engineering problem. The article uses qualitative methods in the form of interviews to ask people how they feel about social engineering. (Steinmetz et al.) In the research, the interviewees said that they prefer a more human and educational approach when it comes to dealing with social engineering. Education is perhaps the best tool when fighting ransomware in general. Most cybersecurity teams have policies and procedures in place to combat these types of attacks. However, it is vital that more policies are put into place to ensure the decline of ransomware. In the United Kingdom, for example, they have set standards for dealing with ransomware - a step by step guide. This is the type of policy that should be worldwide. Each country should have a standard set for dealing with the attacks and mitigating them before they happen.

Conclusion

To conclude, each one of these types of attacks pose a huge threat to the future of security. Biotechnology is a threat to the sensitive and personal identifiable information relating to a person. Artificial Intelligence is a risk because it greatly impacts our daily lives - through the workplace or through inequality. Ransomware is a threat because it gives criminals a way to directly disrupt cybersecurity teams around the world. While there are many technologies that can be huge threats to us in the future, these three are ones that are actively being worked on. They are being created in real time. In order to properly coexist with them, cybersecurity teams

need to develop the proper procedures. Having a universal law surrounding biotechnology, artificial intelligence, and ransomware will only help to strengthen our future endeavors.

References

Jahankhani, Hamid, et al. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity [e-Book]*. 1st ed. 2020.., 2020.

Leo, Philipp, et al. "The Ransomware Dilemma." *MIT Sloan Management Review*, vol. 63, no. 4, 2022, pp. 13–15.

Makridakis, Spyros. "The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms." *Futures : the Journal of Policy, Planning and Futures Studies*, vol. 90, 2017, pp. 46–60, doi:10.1016/j.futures.2017.03.006.

Parrett, James W. "A Proactive Solution to the Inherent Dangers of Biotechnology: Using the Invention Secrecy Act to Restrict Disclosure of Threatening Biotechnology Patents." *William and Mary Environmental Law and Policy Review*, vol. 26, no. 1, 2001, pp. 145–145.

Steinmetz, Kevin F., and Thomas J. Holt. "Falling for Social Engineering: A Qualitative Analysis of Social Engineering Policy Recommendations." *Social Science Computer Review*, vol. 41, no. 2, 2023, pp. 592–607, doi:10.1177/08944393221117501.