Joshua Morton

Dr. Karahan

POLS 426

4/12/2024

Securing Tomorrow: Navigating the Security Challenges of Emerging and Future Technologies

The past ten years have been an eye-opening experience to the fact that technological advancement is reshaping the lives of societies and governments around the world. From the Internet of Things to artificial intelligence and autonomous vehicles, society has become more reliant on and comfortable with emerging technologies in everyday life. With the growing reliance on new technologies, many in the security and law enforcement sector have begun to ask: how will this affect already growing security concerns and challenges posed by the new and emerging technologies that are beginning to become commonplace? As threats begin to increase, the global discussion and response about countermeasures and the effect on society have exploded in the last couple of years, which is what will be discussed throughout this essay. It can be found that delving deep into the multifaceted risks posed by these new and emerging technologies can create a further sense of understanding of how they will affect our societies and systems if compromised, can create enough discussion to warrant more intricate security measures and regulations that can help to reduce or totally eliminate the risk posed by the frequent use of these technologies. Today, many new technologies have made themselves available and commonplace, but the most influential, and potentially most damaging, new technologies include the convergence of AI in the processes and organizational operations of government and commercial entities, the integration of blockchain technology and

cryptocurrency into our global economy, emerging methods of biometric authentication and their possible concerns with user privacy, and finally, the rapid proliferation of autonomous vehicles and home systems used in everyday life that can be compromised by hackers.

Firsty, when speaking about an emerging technology that is exploding in use you cannot fail to mention the impact of Artificial Intelligence on not only the commercial and governmental aspects of operations but also the citizen impact as it is being used more and more by ordinary people. Artificial Intelligence has proven to actually be very fruitful in cybersecurity in its ability to make the process of system surveillance to be a more efficient process in understanding assets within a system to protect but this efficiency also leads to concern in the event that AI is put forth in its ability to be compromised and used nefariously by a foreign entity (Rubinoff, 2020). AI is known for the ability to think and run processes automatically, this is extremely important when speaking on cyber attacks in that attackers may be able to run more complex and automated attacks by using an AI to automatically find exploits in a certain system, give advice to running a payload through the exploit, execute an attack, and collect data if need be. This process is important because of the fact it is plausible to utilize multiple AI capable of this process leading to an attack that can be, with the right resources and utility, untraceable and neverending as thousands of AI could be used to start an attack (Ventre, 2020). AI also has a huge factor that is affecting the operation of war and defense of countries; that being information. A recent example of the use of AI in the military field is the 2022 Russian invasion of Ukraine in which Russia has used AI in a information warfare operation since the very beginnings of fighting in Ukraine (Kostenko et al., 2022) , Russian use of AI voice replication, editing, script writing, and art creation has been influential in creating false propaganda to create a certain view of the war to people within and outside of Russian borders (Kostenko et al., 2022) . This use of AI for

information warfare has revolutionized how war is fought because the basis of war stands on information and with AI is able to be warped and manipulated to give a false sense of information reliance that could lead to mass hysteria or violence when the information is passed in oppositional countries which might serve the objective of the country responsible.

Secondly, the biggest and rising most popular innovation of the last century would be the integration of blockchain technology and cryptocurrency into our global economy. The use of anonymous use of cryptocurrency and its use in the investment in blockchain technology has already been proven to both be beneficial for and used by criminal entities to instigate theft and economic instability (Riesco et al., 2019). A problem presented by the exploitation of blockchain technologies by criminals is the fact that the theft of these technologies and currencies has been caused by simple attacks to users with private keys such as phishing and insecure storage techniques which lead to the eventual theft of blockchain technology such as NFTs which can cause economic damage due to their corresponding relationship with cryptocurrency. In regards to the collection and transaction of cryptocurrency on the blockchain hackers have the opportunity of compromising cryptocurrency wallets through the use of multiple attacks such as Distributed Denial of Service attacks, in which compromised computer systems known as bots will spread to multiple users and bruteforce authentication tools to gain unauthorized access to crypto wallets, and ransomware attacks, in which a myriad of malware tools are utilized to specifically target exploits related to private key authentication to gain access to crypto wallets (Gupta, 2018). The effect of the use of cryptocurrency in cyber attacks is important as it helps to highlight the weaponization of its anonymous nature to benefit criminals and foreign actors. For example, when the 2017 WannaCry attack was initiated it prompted affected computers to send payments of bitcoin to gain their computers back. Due to the anonymous nature of bitcoin global

law enforcement agencies had a much harder time distinguishing the attackers and had to move through alternative methods to find their identity which is an important threat to realize when criminals and foreign entities wish to anonymously acquire funds through crypto they may be untraceable.

Thirdly, as cyber attacks only seem to become more apparent many companies have had problems with insider attack and theft and have begun to implement a new system of authentication, that being biometric authentication. Biometric authentication has been discussed immensely due to its intensely secure nature and collection of specific anatomical traits to authenticate users and give them specific privileges. The problem with biometric authentication arises in its ability to store user data and anatomical information without being stolen and exploited by foreign entities and criminals through means of identity theft, exploitation, or espionage. If hackers were able to gain access to a unsecure system with the information of all of its employees and their biometric data the hacker could essentially leak data to individuals who could masquerade as actual employees by matching their own features to that of the authorized individual and gain unauthorized access to private information (Jain & Nandakumar, 2012). Biometric Authentication software can also be exploited purely based on the fact it is not perfect and can make mistakes, for example an authentication error, known as a false nonmatch, can occur in which an unauthorized individual can gain access to data by passing the biometric authentication software just by having similar authentication data (Jain & Nandakumar, 2012). Biometric Authentication in its current form relies on a similarity system, in contrast to a complete match system, and as such if a person willing to compromise an organization or company's systems and data was to have a fingerprint similar to another person with authorized access the biometric authentication software would have an error and pass the unauthorized user

as the authorized employee allowing them access to the systems (Jain & Nandakumar, 2012). Another such noteworthy attack that compromises biometric authentication is that of an adversary attack which may occur when the system is manipulated by foreign actors to exploit users with authentication to give access to hackers through social engineering methods to circumvent the attack and allow the hackers into areas with data without having to get access to systems holding the data (Jain & Nandakumar, 2012). The threat posed by exploitation and manipulation of biometric authentication is clear and is proof that even the newest technologies, even though it is advertised as so, are not impenetrable to attack and the consequence of relying solely on the system to dish keys and authentication out must be avoided. If a government organization or company with extremely sensitive data that affects national security are to implement a system such as biometric authentication it must be understood that it can be exploited and that it must be supported with other security systems as a way to prevent a national emergency.

Lastly, the automated home and automation industry has exploded in recent years with people all around the world implementing systems like home automation and security systems as well as self automated cars such as those put forward by the company Tesla, but the move towards automation has been cited as a large security issue amongst Americans due to its ability to be exploited. Automated software has been discussed recently purely based on its ability to keep users safe and with the threat of potential accidents caused by negligence based on the fact that a system is automated could lead to a societal discussion on the future of reliance on automated systems running a house or even a car. A glaring safety issue with automation systems in terms of automobiles is the phenomenon at which users feel a false sense of security which leads to negligence in their activities while driving a car leading to the increased number of

accidents (Taeihagh & Lim, 2019). Another such threat posed by automated systems in terms of automated housing systems is that of cyber security attacks in that those with automated security systems may also fall into the phenomenon of negligence due to an over reliance and false sense of security with their automated systems that could lead to things such as home invasion and theft. As said in the article, Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, "Various studies have analysed the possible cybersecurity threats to [Automated Vehicles], as computers possess greater control over the movements of an [Automated Vehicles], [Automated Vehicles]s are more vulnerable to hacking TRANSPORT REVIEWS 115 than conventional vehicles, and the driver is less able to intervene during an attack. Without sufficient security, V2V and V2I communication channels can be hacked, which can lead to serious accidents." automated systems controlling vehicles and home security systems are capable of being hacked and that poses a serious risk to national security based on the fact that with a capable and extensive team of hackers systems all throughout the world that are connected to a single company or organization may be compromised in the event of an attack (Taeihagh & Lim, 2019). Another threat posed by over reliance on automated systems is that many systems collect valuable data and information on their users to provide a better experience but this could also lead to a glaring security issue in that data breaches and leaks are absolutely possible and if hackers were to exploit a single governing system from the company hosting the security system it could be a potential leak of data from individuals in a country and pose a national security risk if the hackers involved were performing the operation as a reconnaissance method for other attacks (Taeihagh & Lim, 2019).

To conclude, it is now apparent the profound impact technological advancements have on the security of societies and nations throughout the world. Understanding these innovations and

their potential threat to the security of not only Americans but of citizens throughout the world is important because it puts us down the path of creating new systems, improving older systems to remedy these risks, and finding ways to mitigate threats. In light of challenges posed by newer and emerging technologies it is imperative for government agencies and security professionals around the world to engage in ongoing research and discussion about these technologies and advocate for comprehensive regulation to reduce these threats. The transformative impact of today's new technologies cannot be overstated. Among the most influential and potentially disruptive innovations are the integration of AI into governmental and commercial operations, the widespread adoption of blockchain technology and cryptocurrency in the global economy, the emergence of biometric authentication methods with privacy implications, and the rapid proliferation of autonomous vehicles and smart home systems vulnerable to cyber threats.

References

Gupta, R. (2018). *Hands-On Cybersecurity with Blockchain: Implement DDoS Protection, PKI-Based Identity, 2FA, and DNS Security Using Blockchain*. Packt Publishing.

Jain, A. K., & Nandakumar, K. (2012, November). Biometric Authentication: System Security and User Privacy. *Computer*, *45*(11), 87-92. DOI: 10.1109/MC.2012.364

Kostenko, O., Jaynes, T., Zhuravlov, D., & Usenko, Y. (2022). PROBLEMS OF USING AUTONOMOUS MILITARY AI AGAINSTTHE BACKGROUND OF RUSSIA'S MILITARY AGGRESSION AGAINST UKRAINE. *Baltic Journal of Legal and Social Sciences*, *4*.

Riesco, R., Larriva-Novo, X., & Villagra, V. A. (2019, September 20). Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommunication Systems*, *73*, 259-288. https://doi.org/10.1007/s11235-019-00613-4

Rubinoff, S. (2020). *Cyber Minds: Insights on Cybersecurity Across the Cloud, Data, Artificial Intelligence, Blockchain, and IoT to Keep You Cyber Safe*. Packt Publishing, Limited

Taeihagh, & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, *39*(1), 103–128. https://doi.org/10.1080/01441647.2018.1494640.

Ventre, D. (2020). *Artificial Intelligence, Cybersecurity and Cyber Defence*. Wiley.