Cybersecurity Project Paper

Jonathan Roeseler

Old Dominion University

CYSE 426: Cyber War

Professor Korb

April 6, 2025

New and emerging technologies seem to be developing and are more apparent in today's world than at any other time in recent history. These technologies have the capability to fundamentally change not only approaches to cybersecurity as a whole, but the world as well. The technologies with the capability to change the cyber domain include: artificial intelligence [AI], quantum computing, and space infrastructure. All of these technologies will change and reshape security, and they will have civilian, government, and military applications.

Artificial Intelligence already has the most profound effect on today's society, with recent successes like ChatGPT, with hundreds of millions of global users. AI has tremendous impacts on current and future infrastructure, offering both offensive and defensive security capabilities, in addition to unmatched research capabilities. Mainstream AI tools, including ChatGPT and Microsoft's Copilot, allow low-knowledge users to plot and execute more advanced attacks with their extensive datasets. Patrick Chow's research paper demonstrates how easy it is to elicit harmful responses from these massive large language models [LLMs]. Attacking these tools to develop advanced tools is simple, as demonstrated by his paper and its associated documents. By simply altering the prompt submitted to an LLM, an attacker can practically obtain knowledge of anything the model has access to - and with the use of Retrieval Augmented Generation [RAG] AI like Microsoft Copilot, an attacker can easily obtain the resources needed to construct a complex attack that is effective now. Generative AI tools completely change the cyber landscape, allowing for easy construction of complex attacks, even with popular models. Generative AI also aids in advanced phishing attacks, being able to mimic people, websites, and organizations extremely well. Additionally, some models with image generation capabilities contribute to the development and use of advanced deepfakes, some of which are indistinguishable from being real, leading to another complex web of threats and ethical issues. Artificial intelligence is already being used both offensively and defensively by both red and blue teams today, and as AI systems develop, these capabilities are going to grow. Security Copilot, developed by Microsoft, is a great example of a good blue-team AI-driven security solution. It is an all-inclusive system that can be used as a generative solution to better automate and fact-find within your environment and understand CVEs, in addition to being a one-stop shop for all of Microsoft's security products (Defender, Sentinel, Purview). As it evolves, it stands to simplify security and free up administrators' time to better respond to more complex and sophisticated threats. AI excels in anomaly detection in SIEM/SOC environments, and defense teams stand to benefit from the tool to address other risks in their respective environments. Burp Suite is a red-team tool that tests web applications for vulnerabilities. Recently, they have released an AI-driven solution that analyzes the results of a scan for its users, revolutionizing web application testing and speeding up the results of a penetration test. From a security perspective, tools like Burp's AI scanner give users who do not necessarily know the underlying systems the ability to cause havoc at a small cost, emphasizing the need for internet-facing systems to be completely secure and do their best to hide their architecture from automated scans. Binhammad puts it best when he says that AI in threat detection is a game-changer. It detects and blocks threats that are not

noticeable to humans, all while being able to reduce false positives in alerts and reporting. AI can implement responses to these alerts as well with a click of a button (or even recommended mitigation strategies when it does not have access to do so). Microsoft's recently released Security Copilot throws all these features together, and it indicates a rapid change in how security will be handled in the future. AI's ability to handle and detect fraudulent actions is necessary for the security of future systems, which are being attacked by equally capable intelligence and individuals. Current and future weapon systems are increasingly being used autonomously with the development of more sophisticated artificial intelligence. Additionally, state surveillance systems leverage AI to achieve their goals, widely infringing on the rights of the ordinary person, as AI can draw conclusions that may be false, leading to inappropriate actions from a state. As a result of these dangerous applications, AI must be developed ethically and be transparent, so as not to cause unjustified damage or destruction. Lukas' article states many of the potential misuses of already available AI, such as its use for propaganda and deception through manipulation of media (deepfakes, highly realistic articles that are indistinguishable from the real thing). Another potential attack that is possible with AI is Social Media spear phishing - essentially, social engineering at its peak. AI uses its algorithms and knowledge of a user it gets from online sources to construct a series of actions that will eventually entice the user to make a mistake, clicking a false link or sharing sensitive information that can be used for further attacks. Valencia's paper describes AI as the new hacker, harnessing its capabilities to carry out complex attacks in a fraction of the time it takes for a proven hacker group to do the same. Once again, AI as the new hacker raises numerous questions regarding ethics and safety. Using tools available such as GPT4, Valencia was able to construct a hacking agent capable of taking on complex, hardened systems and generating sound reports based on results efficiently - and at a price tag of only forty dollars. The development of ultra-smart, no-interaction hacking tools at forty dollars proves the coming shift in cybersecurity - AI tools that operate on both sides of a network or penetration test. Although AI has been a super-trendy topic and new, improved models seem to arise every couple of days/weeks, it is still a technology in development. AI raises numerous complex ethical and societal questions that need to be addressed. In conjunction with quantum computing, AI will be "supercharged" and at that point it will be most effective and efficient; however, it will further the digital divide across the globe, as it will be a very complex and expensive technology for all parties. As artificial intelligence continues to evolve in all applications, society and governments must prioritize strengthening overall security to mitigate the risks posed by these highly advanced tools. Moreover, nation states leveraging artificial intelligence for offensive operations and surveillance underscores the urgency of developing ethical frameworks and transparent systems to ensure these world-changing technologies are used responsibly and do not infringe on individual freedoms.

Quantum computing will change the cyber landscape tremendously. Not only will quantum computing render current encryption protocols and standards obsolete, but it will also

allow for faster and more efficient AI, in addition to introducing new attack vectors for both quantum and pre-quantum devices (especially with new protocols needing to be introduced for quantum devices). Today, states with vast technological and cyber capabilities are collecting data on a mass scale, even data that is encrypted, in anticipation of being able to later break it and gather valuable insights; this attack is being dubbed 'harvest now, decrypt later'. Nation-states can leverage this data for several nefarious purposes, including but not limited to: spying on citizens and subsequently further abusing their rights, gathering highly sensitive classified information, and stealing highly protected trade secrets (Wallden). Cyber must grow to protect classic computing devices from being 'broken' by a quantum device with the development of post-quantum protocols and safe encryption methods - many of the widely used and standardized encryption protocols today (RSA, DSA) are effectively obsolete with these ever-evolving quantum computers (Wallden). Quantum computing will additionally introduce new protocols and architecture that will allow for them to be used to their best potential; these protocols are also susceptible to being vulnerable as they will have to accommodate some backward compatibility to participate in the Internet today. Quantum computer and networking protocols will be more secure, however, this is easier said than done, especially as quantum computing is a complex topic, and in some cases may require new kinds of coding specific to quantum devices. Similar to how specifications like HTTP, for example, HTTP1 versus HTTP2, (the specification not being insecure in of itself), quantum protocols will have to be coded securely to the best of the standard or specification, which is very hard to do, and it always will leave vulnerabilities open to be exploited, differing from its implementation on server/client side, as well as from vendor to vendor. A great example of an exploit that occurred on classic computing from differing vendor/architecture implementations is the infamous EternalBlue exploit. In this attack, at a high level, a server which was designed to interact with two different styles of communication (in this case: pre-NT and NT/post-NT) was attacked by sending these two different message structure values together, leading to a buffer overflow and thus a remote code execution. This attack, a result of backwards and universal compatibility, led to one of the most devastating cyber attacks in the world. Additionally, with differing styles of quantum computers (they are built differently, even though they still ultimately use a qubit), vendor-to-vendor vulnerabilities will be readily apparent and exploited, and receiving such unexpected messages may be even worse with quantum computing, as it is an even more diversified field than just Windows 10 versus 11. As quantum computing continues to emerge as a disruptive technology, it holds both incredible promise and significant risk, particularly in its cyber capabilities, where it may become a potent tool for nations to exploit vulnerabilities and gain unprecedented advantages at home and abroad.

Space infrastructure is another highly complicated and complex system; however, its potential for civilian, government, and military capabilities is unmatched. Most recently, space infrastructure can be highlighted with Starlink. Starlink is a collection of communication satellites developed by SpaceX, and it is used by first responders, everyday civilians, and on the

battlefield in the Ukraine-Russian war. Space offers numerous capabilities that all nations want: fast, efficient communication for all citizens with minimal maintenance needed, signals intelligence, and new horizons for resources and scientific discovery. From a security perspective, space is a mess and is bound for some major security failures. Space communications are all able to be intercepted from Earth; communication satellites' moves are predictable (they orbit fixed in most cases), making them susceptible to jamming, interception, and destruction. All these risks are going to amplify with the space industry projected to continue to grow at least double in market cap approximately every 5-8 years (Manulis). Furthermore, as global communication (smartphones specifically) seems to accept satellite services as a good, reliable alternative to costly cell towers, the attack surface is going to expand. According to Manluis' paper, nations are also looking to space for future war capabilities, with nearly 70% of munitions in the 2004 Iraq war being guided by satellite systems. Many of the systems we enjoy today, like GPS, weather satellites, are all vulnerable to basic attacks, as there was no security design built into these satellite systems (of any kind!). These 'ancient' systems relied on security through obscurity - a terrible practice from a system that can be eavesdropped and communicated with from anywhere on Earth; all that is needed is a dedicated and somewhat smart adversary to take it and run. Current systems are now more open-source in order to curb this threat; however, there are still many flaws needing addressed, especially with their coming spike in use with smartphones. Encryption, anti-jamming (DoS) technologies would need to be implemented to not overwhelm these critical networks with malicious requests and signals. Nations leverage the capabilities of satellites to spy on both citizens and adversaries through the use of strong, advanced antennas that pick up chatter on Earth. These systems are critical to intelligence-gathering operations, and it was paramount to US security in the Cold War (Manulis). Despite not being publicized like other popular and major breaches, satellite networks have been heavily targeted just as much as any other network system in the world. Additionally, breaches have been common, new and old, government and private systems, with a wide range of motivations for the various hacks (Manulis). Interestingly, many of the sophisticated attacks did not occur directly with the satellite, but in another part of its communication architecture. Space systems are reliant on ground/base systems to ultimately then deliver the data to a proepr requesting entity (think DirectTV dish). Space-based systems have a large attack surface, meaning all parts of its process should follow strict measures to ensure security, such as the adoption of a zero-trust architecture. States may also exploit or hijack signals of a broadcast of an adversary nation to carry out objectives such as: political messages through the hijacking of a communication system (satellite TV), or propaganda campaigns. Studies have shown that as space systems continue to expand, incidents have exponentially risen, emphasizing the need for stronger security measures in all parts of the process, including, but not limited to: satellite to ground (encryption, DoS/anti-jam capabilities), ground system (common IT security practices MUST be in place - least privilege, secure physical perimeter and network). The security of space systems is very much necessary to ensure global security in the space domain and prevent catastrophic breaches and the disruption of everyday activities, like GPS or phones relying on

satellite capabilities. In conclusion, space infrastructure offers unrivaled potential across civilian, governmental, and military applications, but its vulnerabilities present significant security hurdles. The predictable nature of satellite movements and reliance on ground systems and networks create exploitable and weak attack points, increasing risks such as interception, jamming, and breaches. As the space industry grows exponentially - both in the public and private sectors - and continues to expand and develop further into critical services like global communications and navigation, it will require robust encryption, anti-jamming (in addition to ordinary Denial of Service) technologies, and zero-trust architectures to safeguard its systems and communications. Nations will continue to utilize space for intelligence gathering and strategic/military operations, further highlighting the necessity for strong security measures to counter exploitation and malicious attacks by a diverse set of actors. From a security perspective, strengthening the security of space infrastructure is required to ensure its availability and prevent widespread disruptions in our increasingly space-reliant, tech-driven world.

The rapid evolution and improvement of emerging technologies such as artificial intelligence, quantum computing, and space infrastructure suggest that there is a new era in cybersecurity and overall global development and infrastructure. These disruptive innovations possess astronomical power, reshaping civilian, government, and military applications across the globe. While they all promise significant advancements and improved capabilities and functionality in their respective ways, they also introduce complex challenges and risks, especially in terms of potential exploitation(s), and societal, as well as ethical dilemmas. The continued development and adoption of these technologies will require diligent strategies to harness their extraordinary potential(s) while mitigating their respective threats, ensuring that their impact fosters global and societal progress and security rather than being exploited for potential misuse by malicious entities - government or group.

References

Binhammad, Mohammad, et al. "The Role of AI in Cyber Security: Safeguarding Digital Identity." *Journal of Information Security* 15.02. https://doi.org/10.4236/jis.2024.152015 (2024): 245-278.

Chao, Patrick, et al. "Jailbreaking black box large language models in twenty queries." *arXiv preprint arXiv:2310.08419* (2023).

Manulis, Mark, et al. "Cyber security in new space: analysis of threats, key enabling technologies and challenges." *International Journal of Information Security* 20 (2021): 287-311. https://link.springer.com/article/10.1007/s10207-020-00503-w.

Pöhler, Lukas, et al. "A Technological Perspective on Misuse of Available AI." *https://doi.org/10.48550/arXiv.2403.15325* (2024).

Valencia, Leroy Jacob. "Artificial Intelligence as the New Hacker: Developing Agents for Offensive Security." https://doi.org/10.48550/arXiv.2406.07561.

Wallden, Petros, and Elham Kashefi. "Cyber security in the quantum era." *Communications of the ACM* 62.4 (2019): 120-120. https://doi.org/10.1145/3241037.