How Emerging Technologies Threaten Our Cybersecurity

Nickson Quak

Cybersecurity Analyst Intern
Cyber Threat Alliance White Paper

AUGUST 2023

CYBER THREAT ALLIANCE

Nickson Quak
Cybersecurity Analyst Intern
CTA White Paper
August 28, 2023

How Emerging Technologies Threaten Our Cybersecurity

"*Now I am become Death, the destroyer of worlds.*" Unless one has been living under a rock in July 2023, one immediately recognizes this quote to be from *Oppenheimer (2023)*, a blockbuster film based largely on the bibliography of atomic bomb pioneer, J. Robert Oppenheimer. The iconic quote, as Oppenheimer himself later confessed, had come to his mind upon the successful detonation of the first ever nuclear device built in history, as he watched the giant fireball engulfed the earth and sky in the fiercest of flames.[1] Indeed, as the Director of Los Alamos National Laboratory, Oppenheimer had played an instrumental role in destroying the pre-nuclear world, ushering in a precarious era of collective existentialism that continues through today.[2]

But Christopher Nolan's *Oppenheimer* was not the only thing to have made an explosive entry over the past year. In November 2022, OpenAI's ChatGPT, a Large Language Model (LLM) trained on 570GB of text-based data, sent shockwaves around the world when OpenAI demonstrated its astounding ability to produce human-like text and to hold complex conversations on a broad range of topics.[3] Garnering over 100 million users in just two months, OpenAI's ChatGPT broke into

[1] Atomic Archive, J. Robert Oppenheimer "Now I am become death...," n.d., https://www.atomicarchive.com/media/videos/oppenheimer.html.
[2] Darius von Guttner Sporzynski, "'Now I Am Become Death, the Destroyer of Worlds': Who Was Atom Bomb Pioneer Robert Oppenheimer?," The Conversation, August 3, 2023, https://theconversation.com/now-i-am-become-death-the-destroyer-of-worlds-who-was-atom-bomb-pioneer-robert-oppenheimer-209398.
[3] Bernard Marr, "A Short History of Chatgpt: How We Got to Where We Are Today," Forbes Magazine, May 22, 2023, https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/.

the mainstream in record time.[4] What followed after was an overwhelming flood of ChatGPT use cases and applications, and we suddenly found ourselves thrust into an AI-integral world.

Every Rose Has its Thorn

For every techno-optimist who puts ChatGPT on a pedestal, however, there exists another techno-pessimist who warns of its dangers. True enough, in just less than a month since ChatGPT was publicly released, cybercriminals were already leveraging it to create dangerous tools for malicious purposes. As early as in December 2022, Check Point Research's team had uncovered a thread titled, "ChatGPT – Benefits of Malware" on a popular dark web hacking forum, in which users were already actively sharing and discussing methods to make malware strains and techniques using ChatGPT.[5] The thread publisher, for example, was able to successfully create a Python-based Infostealer capable of searching for the 12 most common file types, copying these files to a temporary directory, and sending them over the internet—all that from mere ChatGPT natural language prompts.[6]

Phishing: Unprecedented Scale, Unthinkable Speed

Yet that is far from being the only malicious output to have been generated from a ChatGPT prompt so far. With ChatGPT's ability to generate coherent and conversational phishing emails with near perfect grammar in mere seconds, social engineering attacks have never been easier.[7] Not only can malicious threat actors now mass-generate generic phishing emails at an unprecedented scale, but they can

---

[4] Krystal Hu, CHATGPT sets record for fastest-growing user base - analyst note, February 2, 2023, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

[5] TECHx Media, "Cybercriminals Turn to Chatgpt for Help in Their Nefarious Activities - Techx Media," Online media and publishing platform for the technology community, covering top news and trends from MEA region's tech and business world., January 26, 2023, https://techxmedia.com/cybercriminals-turn-to-chatgpt-for-help-in-their-nefarious-activities/.

[6] Ibid.

[7] Matt Caulfield, "Chatgpt Is Changing the Phishing Game," Security Info Watch, April 18, 2023, https://www.securityinfowatch.com/cybersecurity/information-security/breach-detection/article/53057705/chatgpt-is-changing-the-phishing-game.

also mass-produce personalized spear-phishing emails with personal information scraped from the dark web at a speed that was previously unthinkable.[8] The first threat that emerging technologies like ChatGPT—when abused by malicious threat actors—poses, therefore, is the unprecedented scale and speed at which personalized and sophisticated spear-phishing attacks can be created to target even the most savvy individuals.

Arming Malicious Novices

Nevertheless, phishing remains the most "vanilla" case of ChatGPT exploitation. One can be a complete novice in malicious exploitation and still be able to generate a convincing phishing email without "jailbreaking" the chatbot. More experienced users, however, can "jailbreak" ChatGPT by circumventing its guardrails to prompt it to generate source code for phishing websites under the ironic false pretense of "defending against phishing attackers". Paired with the convincing ChatGPT-generated phishing emails, a whole slew of phishing attacks ranging from clickjacking to polymorphic URL attacks are now suddenly accessible to malicious threat actors who would otherwise have to rely on conventionally expensive "phishing/malware-as-a-service" offerings. ChatGPT (and its other LLM peers), therefore, have significantly reduced the barriers to entry for malicious novices to mount phishing attacks on their potential victims.[9]

But if ChatGPT can generate source code output for phishing websites, then could it also help malicious novices generate source code output for other types of malware? Absolutely, at least according to Ronen Ahdut, Cyber Threat Intelligence Lead at Cynet, who observed a threat actor requesting ChatGPT to "write a minimized JavaScript able to detect credit card numbers, their expiration dates, CVV numbers,

[8] Eyal Benishti, "Council Post: Prepare for the AI Phishing Onslaught," Forbes Magazine, March 6, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/03/03/prepare-for-the-ai-phishing-onslaught/.
[9] Sayak Saha Roy, Krishna Vamsi Naragam, and Shirin Nilizadeh, "Generating Phishing Attacks Using Chatgpt," arXiv.org, May 9, 2023, https://arxiv.org/abs/2305.05133.

billing addresses and other payment information with instructions to send all the stolen information to the threat actor's URL".[10] Asher Langton, Threat Researcher at Juniper Threat Labs, likewise argued that "ChatGPT has lowered the barrier to entry for malware development" and has himself explored an example of that—generating natively compiled ransomware with real anti-detection evasions using ChatGPT.[11] The bottom line is that malicious novices who previously lacked the technical proficiency to generate malware with dangerous payloads can, in this AI/LLM-mainstream world, do so effectively and efficiently using only natural language ChatGPT prompts.

Aiding Malicious Professionals

But it is not the just the malicious novices who have had a hand from ChatGPT. Technically proficient malicious professionals, who have been developing malware for exploit or sale on dark web forums long before LLMs like ChatGPT came along, are likely to also have benefitted greatly from weaponizing ChatGPT. Aaron Mulgrew, a security researcher from Forcepoint, was able to—with the help of ChatGPT—create a "new undetectable data-stealing malware" that was capable of executing "highly sophisticated zero-day attacks" previously only executable by nation-state actors.[12] First arriving on a computer disguised as a screen saver application, the malware enters a dormant period to avoid being detected before it begins stealing documents, breaking them into small chunks, hiding them via steganography, and uploading these virtually unidentifiable data pieces onto a Google Drive folder.[13] The scariest

[10] Ronen Ahdut, "CHATGPT Will Empower a New Generation of Threat Actors, Putting Pressure on Defenders to Keep Up ," SC Media, March 21, 2023, https://www.scmagazine.com/perspective/chatgpt-will-empower-a-new-generation-of-threat-actors-putting-pressure-on-defenders-to-keep-up.
[11] Asher Langton et al., "Using Chatgpt to Generate Native Code Malware," Official Juniper Networks Blogs, March 31, 2023, https://blogs.juniper.net/en-us/threat-research/using-chatgpt-to-generate-native-code-malware.
[12] Chris Smith, "A New CHATGPT Zero Day Attack Is Undetectable Data-Stealing Malware," BGR, April 6, 2023, https://bgr.com/tech/a-new-chatgpt-zero-day-attack-is-undetectable-data-stealing-malware/.
[13] Aaron Mulgrew, Lionel Menchaca, and Brice Cagle, "I Built a Zero Day Virus with Undetectable Exfiltration Using Only CHATGPT Prompts," Forcepoint, July 11, 2023, https://www.forcepoint.com/blog/x-labs/zero-day-exfiltration-using-chatgpt-prompts.

part? None but three "commercial antivirus products" were able to detect it, and it only took Mulgrew *a few hours of work*; whereas the same malware would have taken a well-resourced team of about ten highly-skilled hackers several weeks to develop. Mulgrew is highly confident that malicious professional hackers are already leveraging ChatGPT's capabilities to create equally, if not more, sophisticated types of malware capable of wreaking havoc on our security landscape if we are not taking active steps to secure it.

Introducing: ChatGPT's Malicious Cousins

Worryingly, there are already some signs supporting Mulgrew's claim. On July 13, 2023, threat researchers from security firm SlashNext revealed that they had discovered WormGPT, a "blackhat alternative to GPT models" trained on data sources with a special emphasis on malware-related data, and that it was being promoted for sale on dark web hacker forums.[14] Unlike ChatGPT, for which cybercriminals have to "jailbreak" the chatbot by coercing it into circumventing its safety guardrails, WormGPT was (according to its developers) "designed specifically for malicious activities (as it has) no ethical boundaries or limitations".[15] Offering a tiered subscription model ranging from $90 a month to $850 a month, WormGPT's developers proclaim to already have "thousands of users" in less than a month.[16] If true, it spells big trouble for the security landscape; if Mulgrew was able to develop a highly sophisticated malware in only a few hours of "jailbreaking" ChatGPT, imagine what thousands of WormGPT users could do.

More concerning, though, is what WormGPT symbolically represents. A harbinger of malicious AI/LLM products, WormGPT has shown the cybercriminal community that

[14] Daniel Kelley, "Wormgpt - the Generative AI Tool Cybercriminals Are Using to Launch Bec Attacks," SlashNext, July 13, 2023, https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.
[15] Charlie Osborne, "WormGPT: What to Know about Chatgpt's Malicious Cousin," ZDNET, July 20, 2023, https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/.
[16] Ibid.

it is possible to create AI-based cybercrime tools, inspiring them to develop other malicious variants of ChatGPT in just two weeks of its release. FraudGPT, for example, was released just about a week after WormGPT's release, and claims to expand upon WormGPT's capabilities, offering its subscribers the ability to "create hacking tools, undetectable malware, malicious code (as well as to) identify leaks and vulnerabilities in organizations' networks" for a steeper price of $200 a month.[17] And at the time of writing, SlashNext security researchers have—just a few hours ago—uncovered yet another two malicious AI products, DarkBART (allegedly a "dark version of Google's Bart") and DarkBERT, claimed to be "superior to all in a category of its own (because it was) specifically trained on the dark web", and because it boasts in-house internet access and "seamless integration with Google Lens" that allows users to send text accompanied by images.[18] Indeed, as SlashNext security researcher Daniel Kelley puts it, these are merely "the tip of the iceberg" of an incoming swarm of malicious AI products that will likely make our already precarious cyber security even more precarious.

Nevertheless, all is not doom and gloom—at least not yet. While malicious AI/LLM products are now a reality, it remains to be seen whether or not they can be sustainably trained on quality malware data, and whether or not they can ironically be secured against cyberattacks mounted by rival hackers. With the massive volume of noisy data and insecurity plaguing even legitimate AI/LLM products, security experts are less confident that malicious AI/LLM products are capable of filtering out quality training data and securing its products from rivalrous sabotage. Hence, more optimistic security experts argue, the threat posed by malicious AI/LLM products may have been overstated.

---

[17] Komal Banchhor, "AI Tool FraudGPT Empowers Cybercriminals to Plunder Your Personal Data: All You Need to Know," Microsoft Start, July 2023, https://www.msn.com/en-us/news/technology/ai-tool-fraudgpt-empowers-cybercriminals-to-plunder-your-personal-data-all-you-need-to-know/ar-AA1erbtK.

[18] Daniel Kelley, "AI-Based Cybercrime Tools Wormgpt and FRAUDGPT Could Be the Tip of the Iceberg," SlashNext, August 2, 2023, https://slashnext.com/blog/ai-based-cybercrime-tools-wormgpt-and-fraudgpt-could-be-the-tip-of-the-iceberg/.

A New Quantum Threat: Beyond Nuclear Weapons

Though the spotlight has largely been shone on AI/LLM for the most part of the year, another threat derived from the weaponization of another emerging technology lurks quietly on our horizon. The science behind this technology is not entirely new. It has, in the past, led to the development of our much-feared nuclear weapons today.

Nuclear weapons, as the name implies, is deeply rooted in quantum science. As any quantum physicist (or any average movie-goer in July 2023) would tell you, nuclear fission is (in simplified terms) the process of splitting an atomic nucleus into two smaller fragments, releasing a ton of energy and a neutron in the process.[19] The latter, in turn, splits another atomic nucleus, releasing more energy and yet another neutron, thereby creating a self-sustaining process that generates a tremendous amount of energy.[20] Nuclear weapons, as Christopher Nolan's *Oppenheimer* (2023) vividly shows us, is simply the literal weaponization of quantum fission technology.

We see on our horizon today a new kind of threat that could arise from the weaponization of quantum computing technology. Quantum computers, in short, possess the potential to completely render current encryption algorithms like the RSA asymmetric and the AES symmetric encryption algorithms obsolete. The RSA asymmetric algorithm is one of the most common public-key encryption algorithm, and it relies on the mathematically difficult process of deriving the prime factors of a large number.[21] This is known as a "trapdoor" mathematical function, as it is much easier to multiply two prime numbers to obtain a large integer than it is to perform

[19] Atomic Heritage Foundation, "Science behind the Atom Bomb," Nuclear Museum, June 5, 2014, https://ahf.nuclearmuseum.org/ahf/history/science-behind-atom-bomb/.
[20] Ibid.
[21] Emily Conover, "How to Stop Quantum Computers from Breaking the Internet's Encryption," Science News, June 28, 2023, https://www.sciencenews.org/article/quantum-computers-break-internet-save.

the reverse.[22] The AES symmetric encryption algorithm, on the other hand, uses a 128-bit key or a 256-bit key to encrypt data. The sheer number of possible keys that an attacker has to try to crack this through the brute force method means that they would probably have to "spend billions of years to test every possible key and crack the encryption"—and that is with the fastest supercomputer that we have available today.[23] Naturally, this mind-bogglingly large number is sufficient to deter even the grittiest cybercriminal from attempting to crack the AES encryption algorithm by brute force. That is why most cybercriminals today prefer to exploit the frailties of our psychology through social engineering attacks, rather than to crack the encryption through brute force attacks. By the operative logic of mathematics, therefore, we remain rather firmly secured and protected from malicious brute force attacks with the important caveat that we maintain vigilant and practice good infosec hygiene.

Quantum computers, however, could potentially destroy the protections that we currently enjoy from existing encryption algorithms like the RSA and the AES. Unlike classical binary bits that can only represent a single binary value, 0 or 1, quantum qubits can exist in a superposition of multiples states, and can therefore represent 0, 1, or "any proportion of 0 and 1 in superposition of both states".[24] Superposition, loosely characterized, refers to a qubit's ability to "simultaneously be in multiple states", and it is this ability that gives rise to quantum computers' exponentially superior computing power. 500 qubits, for instance, can represent more information than even the most sophisticated supercomputer can with more than 2^{500}

[22] Craig Gidney and Martin Ekerå, How a quantum computer could break 2048-bit RSA encryption in 8 Hours, April 2, 2020, https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.
[23] Markus Pflitsch, "Council Post: Quantum Computers Could Make Today's Encryption Defenseless," Forbes Magazine, May 5, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/05/04/quantum-computers-could-make-todays-encryption-defenseless.
[24] Microsoft Azure, What is a qubit?, n.d., https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit.

classical bits.[25] That is the sheer difference in computing power that we are talking about here—while it would take a classical computer millions of years to find the prime factors of a 2,048-bit number, a quantum computer can perform the same calculation in mere minutes.[26]

Decades in Weeks

Fortunately for us, quantum computers are still too error-prone to be reliably used for our computational purposes. Minor perturbations in their environments, such as a change in temperature or pressure caused by heat and vibration for instance, can introduce errors into the entanglement of qubits during calculations.[27] Experts estimate that it will likely be years and decades before we will see the first practical application of quantum technology.[28]

One would be remiss, however, to dismiss the disruptive potential of quantum computers as a far-flung possibility. Consider the trajectory through which AI technology developed. Despite going through several cycles of "AI winters" between the late 1970s to the 1990s—when investments into AI dried up because AI capabilities at the time were disappointedly overhyped— OpenAI's ChatGPT had garnered 100 million users in just two months. [29] Even quicker than that, the first malicious ChatGPT exploit (a Python-based Infostealer) was uncovered on the dark web less than a month into its release in December 2022. As the saying goes, "there are decades where nothing happens, and there are weeks where decades happen", and there is perhaps no better embodiment of that than what we have seen with AI

[25] Ibid.
[26] Ibid.
[27] John Zich, "'Noise-Cancelling' Qubits Can Minimize Errors in Quantum Computers," University of Chicago News, June 7, 2023, https://news.uchicago.edu/story/noise-cancelling-qubits-can-minimize-errors-quantum-computers.
[28] Bernard Marr, "Quantum Computing Now and in the Future: Explanation, Applications, and Problems," Forbes Magazine, November 8, 2022, https://www.forbes.com/sites/bernardmarr/2022/08/26/quantum-computing-now-and-in-the-future-explanation-applications-and-problems/?sh=eb4a5d11a6b5.
[29] Luciano Floridi, "Ai and Its New Winter: From Myths to Realities - Philosophy & Technology," SpringerLink, February 29, 2020, https://link.springer.com/article/10.1007/s13347-020-00396-6.

so far. With the revolutionizing potential of quantum computing technology, there is no reason to think that quantum computers will be any less disruptive than AI has been.

In fact, recent studies are suggesting that the breakthroughs in AI have contributed, and will continue to contribute, to the development of quantum computers by "cutting through the noise" of quantum measurements. [30] "High-fidelity quantum computing" therefore brings us closer to a stable, reliable, and practical application of quantum technology. Moreover, stable quantum computers can, in turn, dramatically accelerate the speed at which AI machines learn. Quantum Artificial Intelligence (QAI) is the emerging interdisciplinary discipline of "exploiting the unique properties of quantum technologies, such as superposition and quantum entanglement, to carry out AI/ML tasks that would be difficult or impossible to execute on classical computer systems".[31] There is a real possibility that quantum technologies and AI can "turbocharge" each other in ways that remain yet unimaginable to us.[32] In the case of AI and quantum technology, Alan Turing's words ring true, "we can only see a short distance ahead, but we can see plenty there that needs to be done".

A Potential Breakthrough

Already, recent signs suggest that we might be headed towards a tipping point. Just a week ago at the time of writing, South Korean researchers have dramatically released two papers on preprint research repository arXiv, in which they both

[30] Mario Krenn et al., "Artificial Intelligence and Machine Learning for Quantum Technologies," Physical Review A, January 3, 2023, https://journals.aps.org/pra/abstract/10.1103/PhysRevA.107.010101.
[31] James Dargan, "How Close Are We to Quantum Artificial Intelligence?," The Quantum Insider, March 15, 2023, https://thequantuminsider.com/2023/03/15/how-close-are-we-to-quantum-artificial-intelligence/.
[32] Susan Galer, "SAP Brandvoice: If You Think Ai Is Hot, Wait until It Meets Quantum Computing," Forbes Magazine, March 27, 2023, https://www.forbes.com/sites/sap/2023/03/21/if-you-think-ai-is-hot-wait-until-it-meets-quantum-computing/.

separately claimed to have created a groundbreaking new superconductor material.[33] LK-99, presumably named after the initials of the researchers involved and suffixed by the year 1999 in which the material was first discovered, is a compound made from lead and copper that the researchers are claiming to be a "room-temperature superconductor (capable of) working at ambient pressure".[34] A superconductor, in short, is a material that "exhibits no electrical resistance and eliminates magnetic fields" that allows electrical current to almost perpetually flow through it without losing energy to heat or light.

Most superconductors that we know of today have to be created in extremely low temperatures, which make them incredibly expensive and energy inefficient to make. LK-99—if it is indeed a "room temperature superconductor"—can be cheaply, quickly, and widely produced around the world, and could quite possibly speed up the development of quantum computers by providing a "stable and controlled environment for qubits without the need for elaborate cooling systems".[35]

Deja Vu

As I reflect on where we are now, I am reminded of the oft-quoted Mark Twain: "history", as he famously said, "may not repeat itself, but it often rhymes". In 1938, radiochemists Otto Hahn and Fritz Strassmann were bombarding elements (including and especially uranium) with the then newly discovered subatomic participle of a neutron at the Kaiser-Wilhelm Institute, Berlin, when they had unexpectedly discovered nuclear fission. What followed was a global replication campaign, and several scientists including an earnest team on the Pacific Coast of the United States at the University of California, Berkeley, were successful in

[33] Tim Culpan, "Analysis | LK-99 and the Desperation for Scientific Discovery," The Washington Post, August 3, 2023, https://www.washingtonpost.com/business/energy/2023/08/02/lk-99-and-the-desperation-for-scientific-discovery/74c4f774-317a-11ee-85dd-5c3c97d6acda_story.html.
[34] Ibid.
[35] Matt Swayne, "Researchers Claim They Developed a Room-Temperature Superconductor," The Quantum Insider, August 1, 2023, https://thequantuminsider.com/2023/07/26/researchers-claim-they-developed-a-room-temperature-superconductor/.

replicating Hahn and Strassmann's findings. This particular team's success at replicating nuclear fission in a laboratory setting, however, would come to change the global security architecture in the decades that follow, for one young scientist on this Berkeley team immediately made the prescient connection between nuclear fission and a thermonuclear bomb. The name of this young scientist was J. Robert Oppenheimer.

And we are today quite possibly experiencing our very own "nuclear fission discovery moment": if Lee, et al are right about LK-99, as we shall see in the months that follow, then the technological race to build humanity's first *stable* quantum computer might have just heated up. As exciting as that possibility may sound, I fear that a digitally existentialist period may well lie ahead of us. If we are unable to move towards Post-Quantum Cryptography in time, then we face the very real prospect of our cyber security world being destroyed by malicious threat actors exploiting the formidable capabilities of a stable quantum computer.

Bibliography

Ahdut, Ronen. "CHATGPT Will Empower a New Generation of Threat Actors, Putting Pressure on Defenders to Keep Up ." SC Media, March 21, 2023. https://www.scmagazine.com/perspective/chatgpt-will-empower-a-new-generation-of-threat-actors-putting-pressure-on-defenders-to-keep-up.

Atomic Archive. J. Robert Oppenheimer "Now I am become death...," n.d. https://www.atomicarchive.com/media/videos/oppenheimer.html.

Atomic Heritage Foundation. "Science behind the Atom Bomb." Nuclear Museum, June 5, 2014. https://ahf.nuclearmuseum.org/ahf/history/science-behind-atom-bomb/

Banchhor, Komal. "AI Tool FraudGPT Empowers Cybercriminals to Plunder Your Personal Data: All You Need to Know." Microsoft Start, July 2023. https://www.msn.com/en-us/news/technology/ai-tool-fraudgpt-empowers-cybercriminals-to-plunder-your-personal-data-all-you-need-to-know/ar-AA1erbtK

Benishti, Eyal. "Council Post: Prepare for the AI Phishing Onslaught." Forbes Magazine, March 6, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/03/03/prepare-for-the-ai-phishing-onslaught/.

Caulfield, Matt. "Chatgpt Is Changing the Phishing Game." Security Info Watch, April 18, 2023. https://www.securityinfowatch.com/cybersecurity/information-security/breach-detection/article/53057705/chatgpt-is-changing-the-phishing-game.

Conover, Emily. "How to Stop Quantum Computers from Breaking the Internet's Encryption." Science News, June 28, 2023. https://www.sciencenews.org/article/quantum-computers-break-internet-save.

Culpan, Tim. "Analysis | LK-99 and the Desperation for Scientific Discovery." The Washington Post, August 3, 2023. https://www.washingtonpost.com/business/energy/2023/08/02/lk-99-and-the-desperation-for-scientific-discovery/74c4f774-317a-11ee-85dd-5c3c97d6acda_story.html

Dargan, James. "How Close Are We to Quantum Artificial Intelligence?" The Quantum Insider, March 15, 2023. https://thequantuminsider.com/2023/03/15/how-close-are-we-to-quantum-artificial-intelligence/.

Darius von Guttner Sporzynski. "'Now I Am Become Death, the Destroyer of Worlds': Who Was Atom Bomb Pioneer Robert Oppenheimer?" The Conversation, August 3, 2023. https://theconversation.com/now-i-am-become-death-the-destroyer-of-worlds-who-was-atom-bomb-pioneer-robert-oppenheimer-209398.

Floridi, Luciano. "Ai and Its New Winter: From Myths to Realities - Philosophy & Technology." SpringerLink, February 29, 2020. https://link.springer.com/article/10.1007/s13347-020-00396-6.

Galer, Susan. "SAP Brandvoice: If You Think Ai Is Hot, Wait until It Meets Quantum Computing." Forbes Magazine, March 27, 2023. https://www.forbes.com/sites/sap/2023/03/21/if-you-think-ai-is-hot-wait-until-it-meets-quantum-computing/.

Gidney, Craig, and Martin Ekerå. How a quantum computer could break 2048-bit RSA encryption in 8 Hours, April 2, 2020. https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

Hu, Krystal. CHATGPT sets record for fastest-growing user base - analyst note, February 2, 2023. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

Kelley, Daniel. "AI-Based Cybercrime Tools Wormgpt and FRAUDGPT Could Be the Tip of the Iceberg." SlashNext, August 2, 2023. https://slashnext.com/blog/ai-based-cybercrime-tools-wormgpt-and-fraudgpt-could-be-the-tip-of-the-iceberg/.

Kelley, Daniel. "Wormgpt - the Generative AI Tool Cybercriminals Are Using to Launch Bec Attacks." SlashNext, July 13, 2023. https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.

Krenn, Mario, Jonas Landgraf, Thomas Foesel, and Florian Marquardt. "Artificial Intelligence and Machine Learning for Quantum Technologies." Physical Review A, January 3, 2023. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.107.010101.

Langton, Asher, Paul Kimayong, Ashish Joshi, and Nataraja G. "Using Chatgpt to Generate Native Code Malware." Official Juniper Networks Blogs, March 31, 2023. https://blogs.juniper.net/en-us/threat-research/using-chatgpt-to-generate-native-code-malware.

Marr, Bernard. "A Short History of Chatgpt: How We Got to Where We Are Today." Forbes Magazine, May 22, 2023. https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/.

Marr, Bernard. "Quantum Computing Now and in the Future: Explanation, Applications, and Problems." Forbes Magazine, November 8, 2022. https://www.forbes.com/sites/bernardmarr/2022/08/26/quantum-computing-now-and-in-the-future-explanation-applications-and-problems/?sh=eb4a5d11a6b5.

Microsoft Azure. What is a qubit?, n.d. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit.

Mulgrew, Aaron, Lionel Menchaca, and Brice Cagle. "I Built a Zero Day Virus with Undetectable Exfiltration Using Only CHATGPT Prompts." Forcepoint, July 11, 2023. https://www.forcepoint.com/blog/x-labs/zero-day-exfiltration-using-chatgpt-prompts.

Osborne, Charlie. "WormGPT: What to Know about Chatgpt's Malicious Cousin." ZDNET, July 20, 2023. https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/.

Pflitsch, Markus. "Council Post: Quantum Computers Could Make Today's Encryption Defenseless." Forbes Magazine, May 5, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/05/04/quantum-computers-could-make-todays-encryption-defenseless.

Roy, Sayak Saha, Krishna Vamsi Naragam, and Shirin Nilizadeh. "Generating Phishing Attacks Using Chatgpt." arXiv.org, May 9, 2023. https://arxiv.org/abs/2305.05133.

Smith, Chris. "A New CHATGPT Zero Day Attack Is Undetectable Data-Stealing Malware." BGR, April 6, 2023. https://bgr.com/tech/a-new-chatgpt-zero-day-attack-is-undetectable-data-stealing-malware/.

Swayne, Matt. "Researchers Claim They Developed a Room-Temperature Superconductor." The Quantum Insider, August 1, 2023. https://thequantuminsider.com/2023/07/26/researchers-claim-they-developed-a-room-temperature-superconductor/.

TECHx Media. "Cybercriminals Turn to Chatgpt for Help in Their Nefarious Activities - Techx Media." Online media and publishing platform for the technology community, covering top news and trends from MEA region's tech

and business world., January 26, 2023. https://techxmedia.com/cybercriminals-turn-to-chatgpt-for-help-in-their-nefarious-activities/.

Zich, John. "'Noise-Cancelling' Qubits Can Minimize Errors in Quantum Computers." University of Chicago News, June 7, 2023. https://news.uchicago.edu/story/noise-cancelling-qubits-can-minimize-errors-quantum-computers.