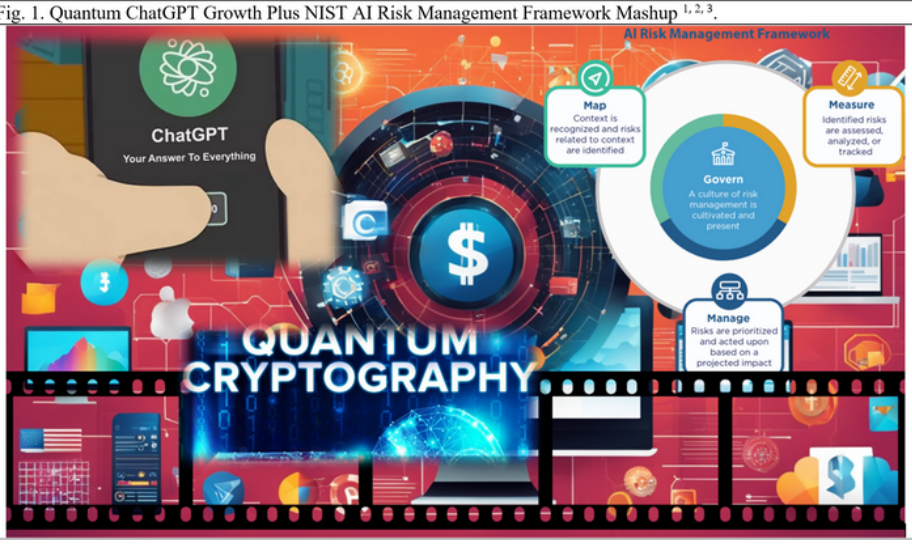
EIGHT ARTIFICIAL INTELLIGENCE (AI) CYBER-TECH TRENDS OF 2023 AND WHAT IT MEANS FOR 2024

By Jeremy Swenson & Matthew Versaggi

1. **The Complex Ethics of Artificial Intelligence (AI) Swarms Policy Makers and Industry Resulting in New Frameworks**
2. **ChatGPT and Other Artificial Intelligence (AI) Tools Have Huge Security Risk**
3. **Artificial Intelligence (AI) Powered Threat Detection Has Improved Analytics**
4. **The Zero-Trust Security Model Becomes More Orchestrated via Artificial Intelligence (AI)**
5. **Quantum-Safe Cryptography Ripens**
6. **Artificial Intelligence (AI) Streamline Cloud Security Posture Management (CSPM)**
7. **Artificial Intelligence (AI) Driven Threat Response Ability Advances**
8. **Artificial Intelligence (AI) Enhanced Authentication Arrives**

Fig. 1. Quantum ChatGPT Growth Plus NIST AI Risk Management Framework Mashup [1, 2, 3].



This year is unique since policy makers and business leaders grew concerned with artificial intelligence (AI) ethics, disinformation morphed, AI had hyper growth including connections to increased crypto money laundering via splitting / mixing. Impressively, AI cyber tools became more capable in the areas of zero-trust orchestration, cloud security posture management (CSPM), threat response via improved machine learning, quantum-safe cryptography ripened, authentication made real time monitoring advancements, while some hype remains. Moreover, the mass resignation / gig economy (remote work) remained a large part of the catalyst for all of these trends.

Every year we like to research and comment on the most impactful security technology and business happenings from the prior year. This year is unique since policy makers and business leaders grew concerned with artificial intelligence (AI) ethics [4], disinformation morphed, AI had hyper growth [5], crypto money laundering via splitting / mixing grew [6], AI cyber tools became more capable - while the mass resignation / gig economy remained a large part of the catalyst for all of these trends. By August 2023 ChatGPT reached 1.43 billion website visits per month and about 180.5 million registered users [7]. This even attracted many non-technical naysayers.

Impressively, the platform was only nine months old then and just turned a year old in November [8]. These numbers for AI tools like ChatGPT are going to continue to grow in many sectors at exponential rates. As a result, the below trends and considerations are likely to significantly impact government, education, high-tech, startups, and large enterprises in big and small ways, albeit with some surprises.

1. The Complex Ethics of Artificial Intelligence (AI) Swarms Policy Makers and Industry Resulting in New Frameworks:

The ethical use of artificial intelligence (AI) as a conceptual and increasingly practical dilemma has gained a lot of media attention and research in the last few years by those philosophy (ethics, privacy), politics (public policy), academia (concepts and principles), and economics (trade policy and patents) - all who have weighed in heavily. As a result, we find this space is beginning to mature. Sovereign nations (The USA, EU, and elsewhere globally) have developed and socialized ethical policies and frameworks [9, 10]. While major corporations motivated by profit are all devising their own ethical vehicles and structures - often taking a legalistic view first [11].

Moreover, The World Economic Forum (WEF) has weighed in on this matter in collaboration with PricewaterhouseCoopers (PWC) [12]. All of this contributes to the accelerated pace of maturity of this area in general. The result is the establishment of shared conceptual viewpoints, early-stage security frameworks, accepted policies, guidelines, and governance structures to support the evolution of artificial intelligence (AI) in ethical ways.

For example, the Department of Defense (DOD) has formally adopted five principles for the ethical development of artificial intelligence capabilities as follows [13].

1. Responsible
2. Equitable
3. Traceable
4. Reliable
5. Governable

Traceable and governable seem to be the most clear and important principles, while equitable and responsible seem gray at best and they could be deemphasized in a heightened war time context. The latter two echo the corporate social responsibility (CSR) efforts found more often in the private sector.

The WEF via PWC has issued its Nine AI Ethical Principles for organizations to follow [14], and The Office of the Director of National Intelligence (ODNI) has released their Framework for AI Ethics [15]. Importantly, The National Institute For Standards in Technology (NIST) has released their AI Risk Management Framework as outlined in Fig. 2. and 3. They also released a playbook to support its implementation and have hosted several working sessions discussing it with

industry which we attended virtually [16]. It seems the mapping aspect could take you down many AI rabbit holes, some unforeseen – inferring complex risk. Mapping also impacts how you measure and manage. None of this is fully clear and much of it will change as ethical AI governance matures.

Fig. 2. NIST AI Risk Management Framework (AI RMF) 1.0 [17].

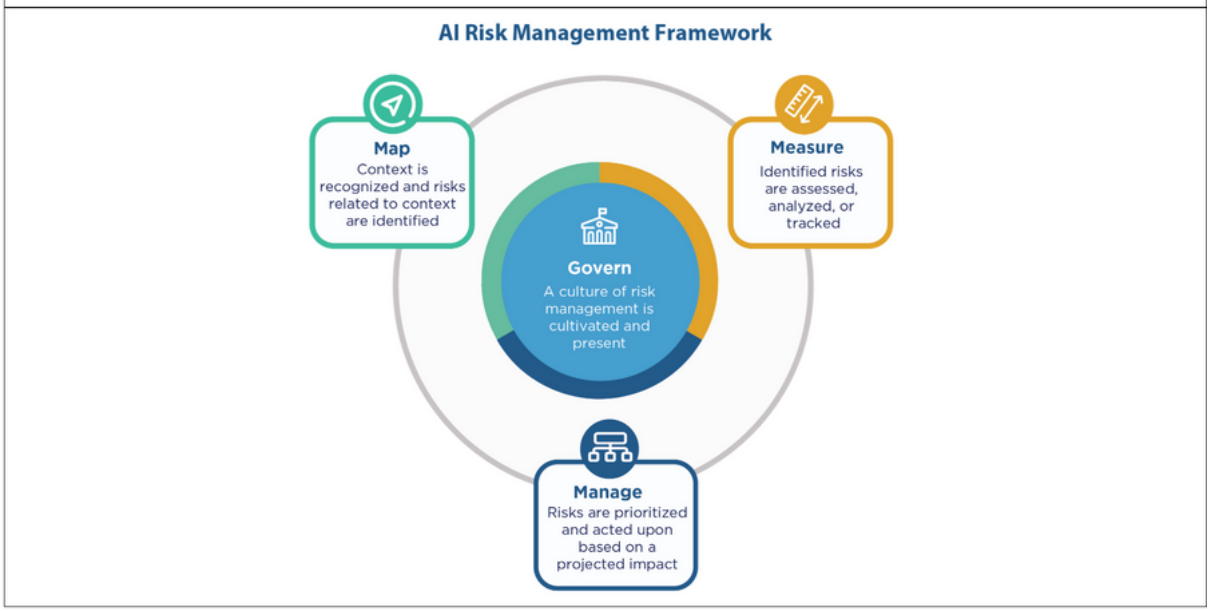


Fig. 3. NIST AI Risk Management Framework: Actors Across AI Lifecycle Stages (AI RMF) 1.0 [18].

Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle Stage	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
TEVV	TEVV includes audit & impact assessment	TEVV includes internal & external validation	TEVV includes model testing	TEVV includes model testing	TEVV includes integration, compliance testing & validation	TEVV includes audit & impact assessment	TEVV includes audit & impact assessment
Activities	Articulate and document the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.	Gather, validate, and clean data and document the metadata and characteristics of the dataset, in light of objectives, legal and ethical considerations.	Create or select algorithms; train models.	Verify & validate, calibrate, and interpret model output.	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives, legal and regulatory requirements, and ethical considerations.	Use system/ technology; monitor & assess impacts; seek mitigation of impacts, advocate for rights.
Representative Actors	System operators; end users; domain experts; AI designers; impact assessors; TEVV experts; product managers; compliance experts; auditors; governance experts; organizational management; C-suite executives; impacted individuals/ communities; evaluators.	Data scientists; data engineers; data providers; domain experts; socio-cultural analysts; human factors experts; TEVV experts.	Modelers; model engineers; data scientists; developers; domain experts; with consultation of socio-cultural analysts familiar with the application context and TEVV experts.		System integrators; developers; systems engineers; software engineers; domain experts; procurement experts; third-party suppliers; C-suite executives; with consultation of human factors experts, socio-cultural analysts, governance experts, TEVV experts,	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impact-ed individuals/commu-nities; evaluators.	End users, operators, and practitioners; impacted individu-als/communities; general public; policy makers; standards organizations; trade associations; advocacy groups; environmental groups; civil society organizations; researchers.

The actors in Fig. 3. cover a wide swath of spaces where artificial intelligence (AI) plays, and appropriately so as AI is considered a GPT (general purpose technology) like electricity, rubber, and the like – where it can be applied ubiquitously in our lives [19]. This infers cognitive technology, digital reality, ambient experiences, autonomous vehicles and drones, quantum computing, distributed ledgers, and robotics to name a few. These were all prior to the emergence of generative AI on the scene which will likely put these vehicles to the test much

earlier than expected. Yet all of these can be mapped across the AI lifecycle stages in Fig. 3. to clarify the activities, actors, dimensions, and if it gets to build, then more scrutiny will need to be applied.

Scrutiny can come in the form of DevSecOps but that is extremely hard to do with such exponentially massive AI code datasets required by the learning models, at least at this point. Moreover, we are not sure if any AI ethics framework does justice to quality assurance (QA) and secure coding best practices much at this point. However, the above two NIST figures at least clarify relationships, flows, inputs and outputs, but all of this will need to be greatly customized to an organization to have any teeth. We imagine those use cases will come out of future NIST working sessions with industry.

Lastly, the most crucial factor in AI ethics governance is what Fig. 3. calls "People and Planet". This is because the people and planet can experience the negative aspects of AI in ways the designers did not imagine, and that feedback is valuable to product governance to prevent bigger AI disasters. For example, AI taking control of the air traffic control system and causing reroutes or accidents, or AI malware spreading faster than antivirus products can defend it creating a cyber pandemic. Thus, making sure bias is reduced and safety increased (DOD five AI principles) is key but certainly not easy or clear.

2. ChatGPT and Other Artificial Intelligence (AI) Tools Have Huge Security Risks:

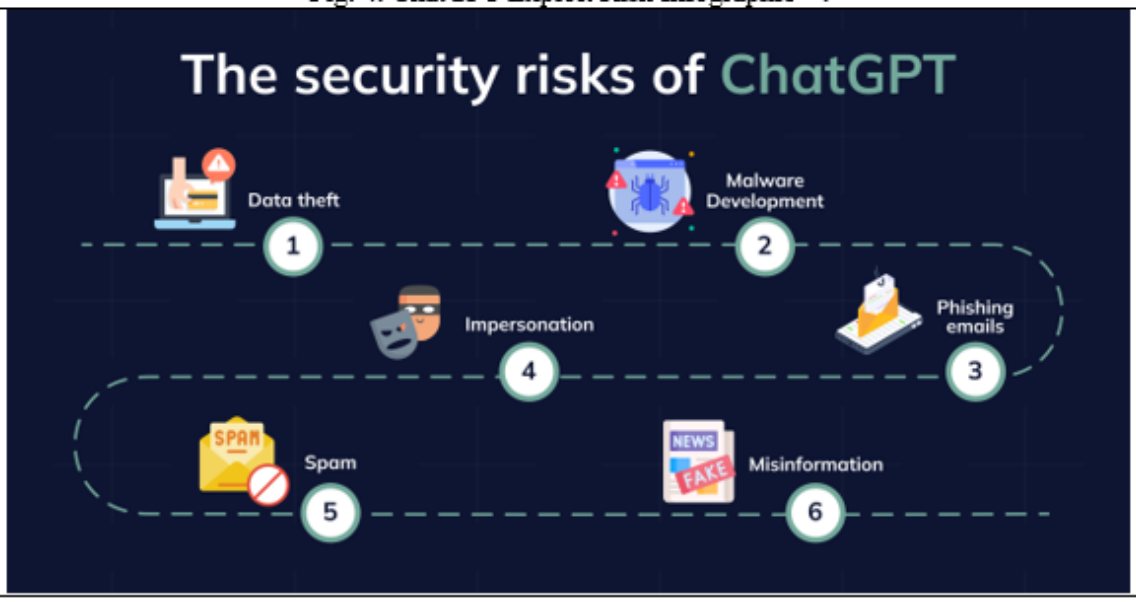
It is fair to start off discussing the risks posed by ChatGPT and related tools to balance out all the positive feature coverage in the media and popular culture in recent months. First of all, with artificial intelligence (AI), every cyber threat actor has a new tool to better send spam, steal data, spread malware, build misinformation mills, grow botnets, launder cryptocurrency through shady exchanges [20], create fake profiles on multiple platforms, create fake romance chatbots, and to build the most complex self-replicating malware that will be akin to zero-day exploits much of the time.

One commentator described it this way in his well circulated LinkedIn article, "It can potentially be a formidable social engineering and phishing weapon where non-native speakers can create flawlessly written phishing emails. Also, it will be much simpler for all scammers to mimic their intended victim's tone, word choice, and writing style, making it more difficult than ever for recipients to tell the difference between a genuine and fraudulent email" [21]. Think of MailChimp on steroids with a sophisticated AI team crafting millions and billions of phishing e-mails / texts customized to impressively realistic details including phone calls with fake voices that mimic your loved ones building fake corroboration [22].

SAP's Head of Cybersecurity Market Strategy, Gabriele Fiata, took the words out of our mouths when he described it this way, "The threat landscape surrounding artificial intelligence (AI) is expanding at an alarming rate. Between January to February 2023, Darktrace researchers have observed a 135% increase in "novel social engineering" attacks, corresponding with the widespread adoption of ChatGPT" [23]. This is just the beginning. More malware as a service propagation, fake bank sites, travel scams, and fake IT support centers will multiply to scam and extort the weak including, elders, schools, local government, and small businesses. Then there

is the increased likelihood that antivirus and data loss prevention (DLP) tools will become less effective as AI morphs. Lastly, cyber criminals can and will use generative AI for advanced evidence tampering by creating fake content to confuse or dirty the chain of custody, lessen reliability, or outright frame the wrong actor – while the government is confused and behind the tech sector. It is truly a digital arms race.

Fig. 4. ChatGPT Exploit Risk Infographic [24].



In the next section we will discuss the possibilities of how artificial intelligence (AI) can enhance information security increasing compliance, reducing risk, enabling new features of great value, and enabling application orchestration for threat visibility.

3. Artificial Intelligence (AI) Powered Threat Detection Has Improved Analytics:

Artificial intelligence (AI) is increasingly being used to enhance threat detection capabilities. Machine learning algorithms analyze vast amounts of data to identify patterns indicative of potential security threats. This enables quicker and more accurate identification of malicious activities. Security information and event management (SIEM) systems enhanced with improved machine learning algorithms can detect anomalies in network traffic, application logs, and data flow – helping organizations identify potential security incidents faster.

There will be reduced false positives which has been a sustained issue in the past with large overconfident companies repeatedly wasting milling of dollars per year fine tuning useless data security lakes (we have seen this) that mostly produce garbage anomaly detection reports [25], [26]. Literally the kind good artificial intelligence (AI) laughs at - we are getting there. All the while, the technology vendors try to solve this via better SIEM functionality for an increased price at present. Yet we expect prices to drop really low as the automation matures.

With improved natural language processing (NLP) techniques, artificial intelligence (AI) systems can analyze unstructured data sources, such as social media feeds, photos, videos, and news articles - to assemble useful threat intelligence. This ability to process and understand textual data empowers organizations to stay informed about indicators of compromise (IOCs) and new

attack tactics. Vendors that provide these services include Dark Trace, IBM, CrowdStrike, and many startups will likely join soon. This space is wide open and the biases of the past need to be forgotten if we want innovation. Young fresh minds who know web 3.0 are valuable here. Thus, in the future more companies will likely not have to buy but rather can build their own customized threat detection tools informed by advancements in AI platform technology.

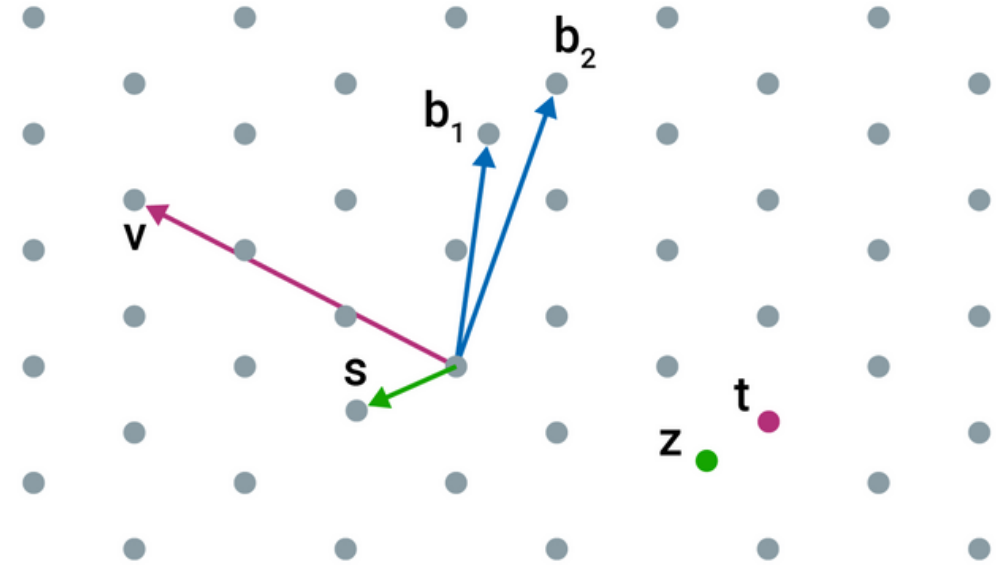
4. The Zero-Trust Security Model Becomes More Orchestrated via Artificial Intelligence (AI):

The zero-trust model assumes that no user or system, even those within the corporate network, should be trusted by default. Access controls are strictly enforced, and continuous verification is performed to ensure the legitimacy of users and devices. Zero-trust moves organizations to a need-to-know-only access mindset (least privilege) with inherent deny rules, all the while assuming you are compromised. This infers single sign-on at the personal device level and improved multifactor authentication. It also infers better role-based access controls (RBAC), firewalled networks, improved need-to-know policies, effective whitelisting and blacklisting of applications, group membership reviews, and state of the art privileged access management (PAM) tools. Password check out and vaulting tools like CyberArk will improve to better inform toxic combination monitoring and reporting. There is still work in selecting / building the right tech components that fit into (not work against) the infrastructure orchestra stack. However, we believe rapid build and deploy AI based custom middleware can alleviate security orchestration mismatches in many cases easily. All of this is likely to better automate and orchestrate zero-trust abilities so that one part does not hinder another part via complexity fog.

5. Quantum-Safe Cryptography Ripens:

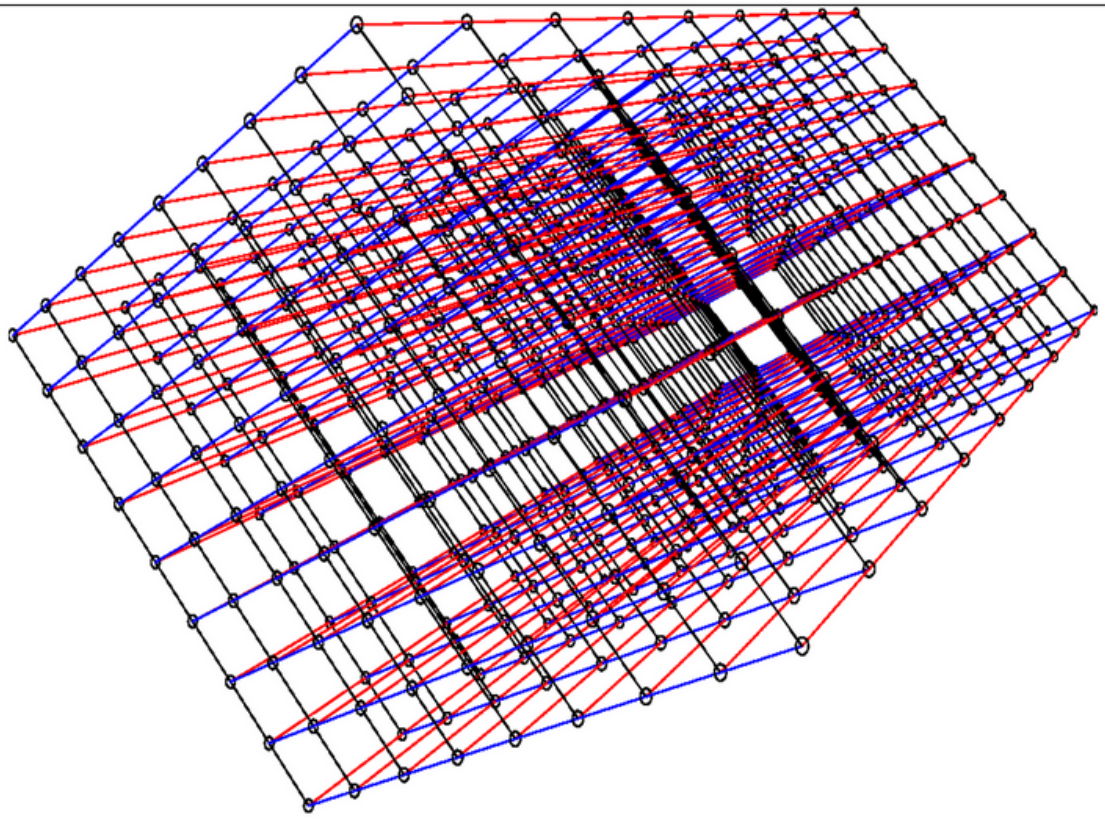
Quantum computing is a quickly evolving technology that uses the laws of quantum mechanics to solve problems too complex for traditional computers, like superposition and quantum interference [27]. Some cases where quantum computers can provide a speed boost include simulation of physical systems, machine learning (ML), optimization, and more. Traditional cryptographic algorithms could be vulnerable because they were built and coded with weaker technologies that have solvable patterns, at least in many cases. “Industry experts generally agree that within 7-10 years, a large-scale quantum computer may exist that can run Shor’s algorithm and break current public-key cryptography causing widespread vulnerabilities” [28]. Quantum-safe or quantum-resistant cryptography is designed to withstand attacks from quantum computers, often artificial intelligence (AI) assisted – ensuring the long-term security of sensitive data. For example, AI can help enhance post-quantum cryptographic algorithms such lattice-based cryptography or hash-based cryptography to secure communications [29]. Lattice-based cryptography is a cryptographic system based on the mathematical concept of a lattice. In a lattice, lines connect points to form a geometric structure or grid (Fig. 5).

Fig. 5. Simple Lattice Cryptography Grid [30].



This geometric lattice structure encodes and decodes messages. Although it looks finite, the grid is not finite in any way. Rather, it represents a pattern that continues into the infinite (Fig. 6).

Fig. 6. Complex Lattice Cryptography Grid [31].



Lattice based cryptography benefits sensitive and highly targeted assets like large data centers, utilities, banks, hospitals, and government infrastructure generally. In other words, there will likely be mass adoption of quantum computing based encryption for better security. Lastly, we used ChatGPT as an assistant to compile the below specific benefits of quantum cryptography albeit with some manual corrections [32]:

a. Detection of Eavesdropping:
Quantum key distribution protocols can detect the presence of an eavesdropper by the disturbance introduced during the quantum measurement process, providing a level of security beyond traditional cryptography.

b. Quantum-Safe Against Future Computers
Quantum computers have the potential to break many traditional cryptographic systems. Quantum cryptography is considered quantum-safe, as it relies on the fundamental principles of quantum mechanics rather than mathematical complexity.

c. Near Unconditional Security:
Quantum cryptography provides near unconditional security based on the principles of quantum mechanics. Any attempt to intercept or measure the quantum state will disturb the system, and this disturbance can be detected. Note that ChatGPT wrongly said "unconditional Security" and we corrected to "near unconditional security" as that is more realistic.

6. Artificial Intelligence (AI) Streamline Cloud Security Posture Management (CSPM):

As organizations increasingly migrate to cloud environments, ensuring the security of cloud assets becomes key. Vendors like Microsoft, Oracle, and Amazon Web Services (AWS) lead this space; yet large organizations have their own clouds for control as well. Cloud security posture management (CSPM) tools help organizations manage and secure their cloud infrastructure by continuously monitoring configurations and detecting misconfigurations that could lead to vulnerabilities [33]. These tools automatically assess cloud configurations for compliance with security best practices. This includes ensuring that only necessary ports are open, and that encryption is properly configured. "Keeping data safe in the cloud requires a layered defense that gives organizations clear visibility into the state of their data. This includes enabling organizations to monitor how each storage bucket is configured across all their storage services to ensure their data is not inadvertently exposed to unauthorized applications or users" [34]. This has considerations at both the cloud user and provider level especially considering artificial intelligence (AI) applications can be built and run inside the cloud for a variety of reasons. Importantly, these build designs often use approved plug ins from different vendors making it all the more complex.

7. Artificial Intelligence (AI) Driven Threat Response Ability Advances:

Artificial intelligence (AI) is used not only for threat detection but also in automating response actions [35]. This can include automatically isolating compromised systems, blocking malicious internet protocol (IP) addresses, closing firewalls, or orchestrating a coordinated response to a cyber incident – all for less money. Security orchestration, automation, and response (SOAR) platforms leverage AI to analyze and respond to security incidents, allowing security teams to automate routine tasks and respond more rapidly to emerging threats. Microsoft Sentinel, Rapid7 InsightConnect, and FortiSOAR are just a few of the current examples. Basically, AI tools will help SOAR tools mature so security operations centers (SOCs) can catch the low hanging fruit; thus, they will have more time for analysis of more complex threats. These AI tools will employ the observe, orient, decide, act (OODA) Loop methodology [36]. This will allow them to stay up to date, customized, and informed of many zero-day exploits. At the same time, threat actors will constantly try to avert this with the same AI but with no governance.

8. Artificial Intelligence (AI) Enhanced Authentication Arrives:

Artificial intelligence (AI) is being utilized to strengthen user authentication methods. Behavioral biometrics, such as analyzing typing patterns, mouse movements and ram usage, can add an extra layer of security by recognizing the unique behavior of legitimate users. Systems that use AI to analyze user behavior can detect and flag suspicious activity, such as an unauthorized user attempting to access an account or escalate a privilege [37]. Two factor authentication remains the bare standard with many leading identity and access management (IAM) application makers including Okta, SailPoint, and Google experimenting with AI for improved analytics and functionality. Both two factor and multifactor authentication benefit from AI advancements with machine learning via real time access rights reassignment and improved role groupings [38]. However, multifactor remains stronger at this point because it includes something you are, biometrics. The jury is out on which method will remain the security leader because biometrics can be faked by AI [39]. Importantly, AI tools can remove fake accounts or orphaned accounts much more quickly, reducing risk. However, it likely will not get it right 100% of the time so there is a slight inconvenience.

Conclusion and Recommendations:

Artificial intelligence (AI) remains a leading catalyst for digital transformation in tech automation, identity and access management (IAM), big data analytics, technology orchestration, and collaboration tools. AI based quantum computing serves to bolster encryption when old methods are replaced. All of the government actions to incubate ethics in AI are a good start and the NIST AI Risk Management Framework (AI RMF) 1.0 is long overdue. It will likely be tweaked based on private sector feedback. However, adding the DOD five principles for the ethical development of AI to the NIST AI RMF could derive better synergies. This approach should be used by the private sector and academia in customized ways. AI product ethical deviations should be thought of as quality control and compliance issues and remediated immediately.

Organizations should consider forming an AI governance committee to make sure this unique risk is not overlooked or overly merged with traditional web / IT risk. ChatGPT is a good

encyclopedia and a cool Boolean search tool, yet it got some things wrong about quantum computing in this article for which we cited and corrected. The Simplified AI text to graphics generator was cool and useful but it needed some manual edits as well. Both of these generative AI tools will likely get better with time.

Artificial intelligence (AI) will spur many mobile malware and ransomware variants faster than Apple and Google can block them. This in conjunction with the fact that people more often have no mobile antivirus on their smart phone even if they have it on their personal and work computers, and a culture of happy go lucky application downloading makes it all the worse. As a result, more breaches should be expected via smart phones / watches / eyeglasses from AI enabled threats.

Therefore, education and awareness around the review and removal of non-essential mobile applications is a top priority. Especially for mobile devices used separately or jointly for work purposes. Containerization is required via a mobile device management (MDM) tool such as JAMF, Hexnode, VMWare, or Citrix Endpoint Management. A bring your own device (BYOD) policy needs to be written, followed, and updated often informed by need-to-know and role-based access (RBAC) principles. This requires a better understanding of geolocation, QR code scanning, couponing, digital signage, in-text ads, micropayments, Bluetooth, geofencing, e-readers, HTML5, etc. Organizations should consider forming a mobile ecosystem security committee to make sure this unique risk is not overlooked or overly merged with traditional web / IT risk. Mapping the mobile ecosystem components in detail is a must including the AI touch points.

The growth and acceptability of mass work from home (WFH) combined with the mass resignation / gig economy remind employers that great pay and culture alone are not enough to keep top talent. At this point, AI only takes away some simple jobs but creates AI support jobs, yet the percents of this are not clear this early. Signing bonuses and personalized treatment are likely needed for those with top talent. We no longer have the same office and thus less badge access is needed. Single sign-on (SSO) will likely expand to personal devices (BYOD) and smart phones / watches / eyeglasses. Geolocation-based authentication is here to stay with double biometrics, likely fingerprint, eye scan, typing patterns, and facial recognition. The security perimeter remains more defined by data analytics than physical / digital boundaries, and we should dashboard this with machine learning tools as the use cases evolve.

Cloud infrastructure will continue to grow fast creating perimeter and compliance complexity / fog. Organizations should preconfigure artificial intelligence (AI) based cloud-scale options and spend more on cloud-trained staff. They should also make sure that they are selecting more than two or three cloud providers, all separate from one another. This helps staff get cross-

trained on different cloud platforms and plug in applications. It also mitigates risk and makes vendors bid more competitively. There is huge potential for AI synergies with Cloud Security Posture Management (CSPM) tools, and threat response tools - experimentation will likely yield future dividends. Organization should not be passive and stuck in old paradigms. The older generations should seek to learn from the younger generations without bias. Also, comprehensive logging is a must for AI tools.

In regard to cryptocurrency, non-fungible tokens (NFTs), initial coin offerings (ICOs), and related exchanges – artificial intelligence (AI) will be used by crypto scammers and those seeking to launder money. Watch out for scammers who make big claims without details, no white papers or filings, or explanations at all. No matter what the investment, find out how it works and ask questions about where your money is going. Honest investment managers and advisors want to share that information and will back it up with details in many documents and filings [40]. Moreover, better blacklisting by crypto exchanges and banks is needed to stop these illicit transactions erroring far on the side of compliance. This requires us to pay more attention to knowing and monitoring our own social media baselines – emerging AI data analytics can help here. If you are for and use crypto mixer and / or splitter services then you run the risk of having your digital assets mixed with dirty digital assets, you have high fees, you have zero customer service, no regulatory protection, no decent Terms of Service and / or Privacy Policy if any, and you have no guarantee that it will even work the way you think it will.

As security professionals, we are patriots and defenders of wherever we live and work. We need to know what our social media baseline is across platforms. IT and security professionals need to realize that alleviating disinformation is about security before politics. We should not be afraid to talk about this because if we are, then our organizations will stay weak and outdated and we will be plied by the same artificial intelligence (AI) generated political bias that we fear confronting. More social media training is needed as many security professionals still think it is mostly an external marketing thing.

It's best to assume AI tools are reading all social media posts and all other available articles, including this article which we entered into ChatGPT for feedback. It was slightly helpful pointing out other considerations. Public-to-private partnerships (InfraGard) need to improve and application to application permissions need to be more scrutinized. Everyone does not need to be a journalist, but everyone can have the common sense to identify AI / malware-inspired fake news. We must report undue AI bias in big tech from an IT, compliance, media, and a security perspective. We must also resist the temptation to jump on the AI hype bandwagon but rather should evaluate each tool and use case based on the real-world business outcomes for the foreseeable future.

About the Authors:

Jeremy Swenson is a disruptive-thinking security entrepreneur, futurist / researcher, and senior management tech risk consultant. He is a frequent speaker, published writer, podcaster, and even does some pro bono consulting in these areas. He holds an MBA from St. Mary's University of MN, an MSST (Master of Science in Security Technologies) degree from the University of Minnesota, and a BA in political science from the University of Wisconsin Eau Claire. He is an alum of the Federal Reserve Secure Payment Task Force, the Crystal, Robbinsdale and New Hope Citizens Police Academy, and the Minneapolis FBI Citizens Academy.

Matthew Versaggi is a senior leader in artificial intelligence with large company healthcare experience who has seen hundreds of use-cases. He is a distinguished engineer, built an organization's "College of Artificial Intelligence", introduced and matured both cognitive AI technology and quantum computing, has been awarded multiple patents, is an experienced public speaker, entrepreneur, strategist and mentor, and has international business experience. He has an MBA in international business and economics and a MS in artificial intelligence from DePaul University, has a BS in finance and MIS and a BA in computer science from Alfred University. Lastly, he has nearly a dozen professional certificates in AI that are split between the AI, technology, and business strategy.

References:

[1] Swenson, Jeremy, and NIST; Mashup 12/15/2023; "Artificial Intelligence Risk Management Framework (AI RMF 1.0)". 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.
[2] Swenson, Jeremy, and Simplified AI; AI Text to graphics generator. 01/08/24: https://app.simplified.com/
[3] Swenson, Jeremy, and ChatGPT; ChatGPT Logo Mashup. OpenAI. 12/15/23: https://chat.openai.com/auth/login
[4] The White House; "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." 10/30/23: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
[5] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[6] Sun, Zhiyuan; "Two individuals indicted for $25M AI crypto trading scam: DOJ." Cointelegraph. 12/12/23: https://cointelegraph.com/news/two-individuals-indicted-25m-ai-artificial-intelligence-crypto-trading-scam
[7] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[8] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[9] The White House; "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." 10/30/23: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
[10] EU. "EU AI Act: first regulation on artificial intelligence." 12/19/23: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[11] Jackson, Amber; "Top 10 companies with ethical AI practices." AI Magazine. 07/12/23: https://aimagazine.com/ai-strategy/top-10-companies-with-ethical-ai-practices
[12] Golbin, Ilana, and Axente, Maria Luciana; "9 ethical AI principles for organizations to follow." World Economic Forum and PricewaterhouseCoopers (PWC). 06/23/21 https://www.weforum.org/agenda/2021/06/ethical-principles-for-ai/
[13] Lopez, Todd C; "DOD Adopts 5 Principles of Artificial Intelligence Ethics". DOD News. 02/25/20: https://www.defense.gov/News/News-Stories/article/article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/
[14] Golbin, Ilana, and Axente, Maria Luciana; "9 ethical AI principles for organizations to follow." World Economic Forum and PricewaterhouseCoopers (PWC). 06/23/21 https://www.weforum.org/agenda/2021/06/ethical-principles-for-ai/
[15] The Office of the Director of National Intelligence. "Principles of Artificial Intelligence Ethics for the Intelligence Community." 07/23/20: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/3468-intelligence-community-releases-artificial-intelligence-principles-and-framework#:~:text=The%20Principles%20of%20AI%20Ethics,resilient%20by%20design%2C%20and%20incorporate
[16] NIST; "NIST AI RMF Playbook." 01/26/23: https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook

[17] NIST; "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[18] NIST; "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[19] Crafts, Nicholas; "Artificial intelligence as a general-purpose technology: an historical perspective." Oxford Review of Economic Policy. Volume 37, Issue 3, Autumn 2021: https://academic.oup.com/oxrep/article/37/3/521/6374675
[20] Sun, Zhiyuan; "Two individuals indicted for $25M AI crypto trading scam: DOJ." Cointelegraph. 12/12/23: https://cointelegraph.com/news/two-individuals-indicted-25m-ai-artificial-intelligence-crypto-trading-scam
[21] Patel, Pranav; "ChatGPT brings forth new opportunities and challenges to the Cybersecurity industry." LinkedIn Pulse. 04/03/23: https://www.linkedin.com/pulse/chatgpt-brings-forth-new-opportunities-challenges-industry-patel/
[22] FTC; "Preventing the Harms of AI-enabled Voice Cloning." 11/16/23: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/preventing-harms-ai-enabled-voice-cloning
[23] Fiata, Gabriele; "Why Evolving AI Threats Need AI-Powered Cybersecurity." Forbes. 10/04/23: https://www.forbes.com/sites/sap/2023/10/04/why-evolving-ai-threats-need-ai-powered-cybersecurity/?sh=161bd78b72ed
[24] Patel, Pranav; "ChatGPT brings forth new opportunities and challenges to the Cybersecurity industry." LinkedIn Pulse. 04/03/23: https://www.linkedin.com/pulse/chatgpt-brings-forth-new-opportunities-challenges-industry-patel/
[25] Tobin, Donal; "What Challenges Are Hindering the Success of Your Data Lake Initiative?" Integrate.io. 10/05/22: https://www.integrate.io/blog/data-lake-initiative/
[26] Chuvakin, Anton; "Why Your Security Data Lake Project Will … Well, Actually …" Medium. 10/22/22. https://medium.com/anton-on-security/why-your-security-data-lake-project-will-well-actually-78e0e360c292
[27] Amazon Web Services; "What are the types of quantum technology?" 01/07/23: https://aws.amazon.com/what-is/quantum-computing/
[28] ISARA Corporation; "What is Quantum-safe Cryptography?" 2023: https://www.isara.com/resources/what-is-quantum-safe.html
[29] Swenson, Jeremy, and ChatGPT; OpenAI. 12/15/23: https://chat.openai.com/auth/login
[30] Utimaco; "What is Lattice-based Cryptography? 2023: https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-lattice-based-cryptography
[31] D. Bernstein, and T. Lange; "Post-quantum cryptography - dealing with the fallout of physics success." IACR Cryptology. 2017: https://www.semanticscholar.org/paper/Post-quantum-cryptography-dealing-with-the-fallout-Bernstein-Lange/a515aad9132a52b12a46f9a9e7ca2b02951c5b82
[32] Swenson, Jeremy, and ChatGPT; OpenAI. 12/15/23: https://chat.openai.com/auth/login
[33] Microsoft; "What is CSPM?" 01/07/24: https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm
[34] Rosencrance, Linda; "How to choose the best cloud security posture management tools." CSO Online. 10/30/23: https://www.csoonline.com/article/657138/how-to-choose-the-best-cloud-security-posture-management-tools.html