AI Cyber Insights

AI in Cybersecurity

Q2 2024 INSIGHTS

A quarterly comprehensive whitepaper on the latest advancements at the intersection of Artificial Intelligence and Cybersecurity

Table of Contents

This whitepaper is provided for informational purposes only and does not constitute professional advice. The insights and analyses contained herein are based on data and trends publicly available as of Q2 2024. While efforts have been made to ensure the accuracy and completeness of the information, the dynamic nature of Artificial Intelligence and cybersecurity may lead to changes or obsolescence or omission. The authors and publishers accept no liability for any losses or damages arising from the use of this publication.

This report reveals a rapidly evolving cybersecurity landscape where AI presents both unprecedented opportunities and significant challenges.

Executive Summary

The second quarter of 2024 has seen significant advancements in the integration of Artificial Intelligence (AI) into cybersecurity. This report offers a comprehensive analysis of key trends, developments, and implications observed during this period. Key findings include:

- **AI Integration:** AI's role is evolving from an assistive tool to an autonomous actor in cybersecurity, significantly impacting Security Operations Center (SOC) analysis and malware analysis. (1) (2)
- **Election Security:** The emergence of AI-powered deepfakes has posed a substantial threat to election integrity, with several notable incidents. (3) (4) (5)
- **Technological Advancements:** Breakthroughs such as OpenAI's GPT-4o and Google's LLM-powered fuzzing framework highlight AI's expanding capabilities. (6) (7)
- **Security Vulnerabilities:** New AI-specific threats like the "Morris II" AI worm and critical vulnerabilities in AI-as-a-Service platforms have emerged. (8) (9)
- **Ethical Considerations:** The community is addressing issues of bias, explainability, and transparency in AI. (10)
- **Regulatory Landscape:** Global approaches to AI regulation remain fragmented, with the EU leading in comprehensive legislation and other regions adopting more flexible frameworks. (11) (12)

This report reveals a rapidly evolving cybersecurity landscape where AI presents both unprecedented opportunities and significant challenges.

Introduction

As we progress through 2024, the integration of AI into cybersecurity is a transformative reality. AI enhances threat detection capabilities [13] and automates routine security tasks [14], proving to be a powerful tool in the cybersecurity domain. However, this integration also brings challenges, with AI systems becoming more sophisticated and the threats they combat [15] evolving in complexity.

This white paper provides a comprehensive analysis of the AI cybersecurity landscape in Q2 2024, covering:

Funding trends in AI-focused cybersecurity initiatives

- The changing role of AI in cybersecurity operations
- The impact of AI on election security
- Notable technological breakthroughs and their implications
- Emerging AI-specific security vulnerabilities
- Ethical considerations in AI-driven cybersecurity
- The evolving global regulatory landscape for AI in cybersecurity

The insights presented are based on extensive desk research, industry reports, and comprehensive analyses, aimed at providing cybersecurity professionals, policymakers, and technology leaders with a thorough understanding of the current state of AI in cybersecurity.

Funding Landscape

The investments shown below reflect only publicly disclosed funding and do not include any that have not been publicly revealed by the funded companies or their investment partners.

Q2 2024 saw significant investment in the cybersecurity sector, with AI playing an increasingly critical role. Key observations include:

Q2 TOTAL FUNDING

$3.3 billion

raised over 98 rounds. [17]

Q1 TOTAL FUNDING

$2.3 billion

raised over 77 rounds. [21]

Q2 AI SECURITY/GOVERNANCE/PRIVACY SPECIFIC:

$100 million

raised across 12 deals. [18] [19] [20]

Q2 AI SECURITY/GOVERNANCE/PRIVACY SPECIFIC:

$35 million

raised across 6 deals. [22] [23] [24]

The relatively modest investment in standalone AI security ($100 million out of $3.3 billion total) may indicate that while the potential of AI in cybersecurity is widely recognized, the market is still in the early stages of defining and valuing pure AI security solutions. It may also reflect a cautious approach from investors aware of the rapid pace of change in AI technology and the volatility in the space.

Overall funding increased by 43.5% from Q1 to Q2, with the number of funding rounds increasing by 27.3%. AI-specific security funding nearly tripled with a 185.7% increase, and the number of AI-specific deals doubled.

Investors appear to prioritize companies that integrate AI capabilities into broader established cybersecurity categories rather than focusing on pure-play AI security firms. This suggests a preference for proven business models enhanced by AI over entirely new AI-centric approaches. [25]

The relatively modest investment in standalone AI security ($100 million out of $3.3 billion total) may indicate that while the potential of AI in cybersecurity is widely recognized, the market is still in the early stages of defining and valuing pure AI security solutions. It may also reflect a cautious approach from investors aware of the rapid pace of change in AI technology and the volatility in the space.

AI in Cybersecurity Roles

The integration of AI into cybersecurity is not only changing the tools and technologies used but also transforming job roles within the industry. Significant developments highlight both the benefits and risks of AI in cybersecurity

4.1 AI-Powered SOC Analysts

One of the most groundbreaking developments in Q2 2024 has been the emergence of the industry's first AI-powered Security Operations Center (SOC) analysts [1] by Dropzone AI which purportedly reduces time spent on manual alert analysis by 95% [26]. Dropzone AI secured $3.5 million in funding [27] and was named a top 10 finalist in the RSA Conference Innovation Sandbox contest [28].

Other AI-Powered SOC innovators include:

ANVILOGIC™

A US-based security operations and analytics platform. They raised a

$45.0 million

Series C funding in April [29].

Bricklayer AI

A US-based AI-agent-enabled security operations platform raised a

$2.5 million

pre-seed funding in April [30].

SEVEN AI

Another US-based startup built an AI agent enabled security operations platform, raising

$36.0 million

in seed funding [31].

4.2 Threat Intelligence/ Modelling

AI is transforming threat intelligence and modeling capabilities as evidenced by significant investments during the quarter:

BforeAI

A France-based brand protection and threat intelligence platform raised

$15.0 million

million in Series A funding in April [32].

CYWRECK

A Singapore-based professional services firm focusing on threat modeling and application security raised

$2.0 million

million in pre-seed funding in May [33].

ThreatModeler

A US-based threat modeling platform raised

$60.0 million

in private equity funding in May [34].

4.3 Security Incident Response

AI can automate incident response tasks such as containment, investigation, and remediation, improving response times and reducing human error. Research indicates a significant reduction in response time when using AI tools [35].

4.4 Vulnerability Management

AI-powered tools can automate vulnerability scanning, prioritize risks, and recommend remediation strategies, enhancing the efficiency of vulnerability management processes [36].

4.5 Social Engineering Detection

AI can analyze communication patterns and language to identify attempts at social engineering, a common tactic used in cyberattacks. Studies have demonstrated AI's effectiveness in detecting phishing attempts and fraudulent communications [37, 38].

4.5 AI-Assisted Malware Development

While AI shows great promise in enhancing cybersecurity defenses, it also presents new challenges in the form of malware creation using AI. A recent case in Japan [2] highlights this concerning trend:

AI can automate incident response tasks such as containment, investigation, and remediation, improving response times and reducing human error. Research indicates a significant reduction in response time when using AI tools [35].

An individual used AI tools to gather information and code for developing ransomware designed to encrypt data and demand cryptocurrency payments. While no actual damages were reported in this case, it serves as a stark warning of AI's potential misuse in cybercrime.

As AI becomes more accessible and powerful, it can be leveraged by malicious actors to create more sophisticated and potentially more damaging cyber threats. The contrasting developments of AI-powered SOC analysts and AI-assisted malware creation illustrate the double-edged nature of AI in cybersecurity. As the industry moves forward, it must balance the transformative potential of AI with the need for robust security measures, ethical guidelines, and adaptive regulatory frameworks to ensure that AI remains a force for good in cybersecurity.

Insights

Current Landspacpe:

- Partial AI Integration: Vulnerability Management, Social Engineering Detection
- High AI Autonomy: SOC Analysis, Incident Response, Threat Intelligence/Modeling

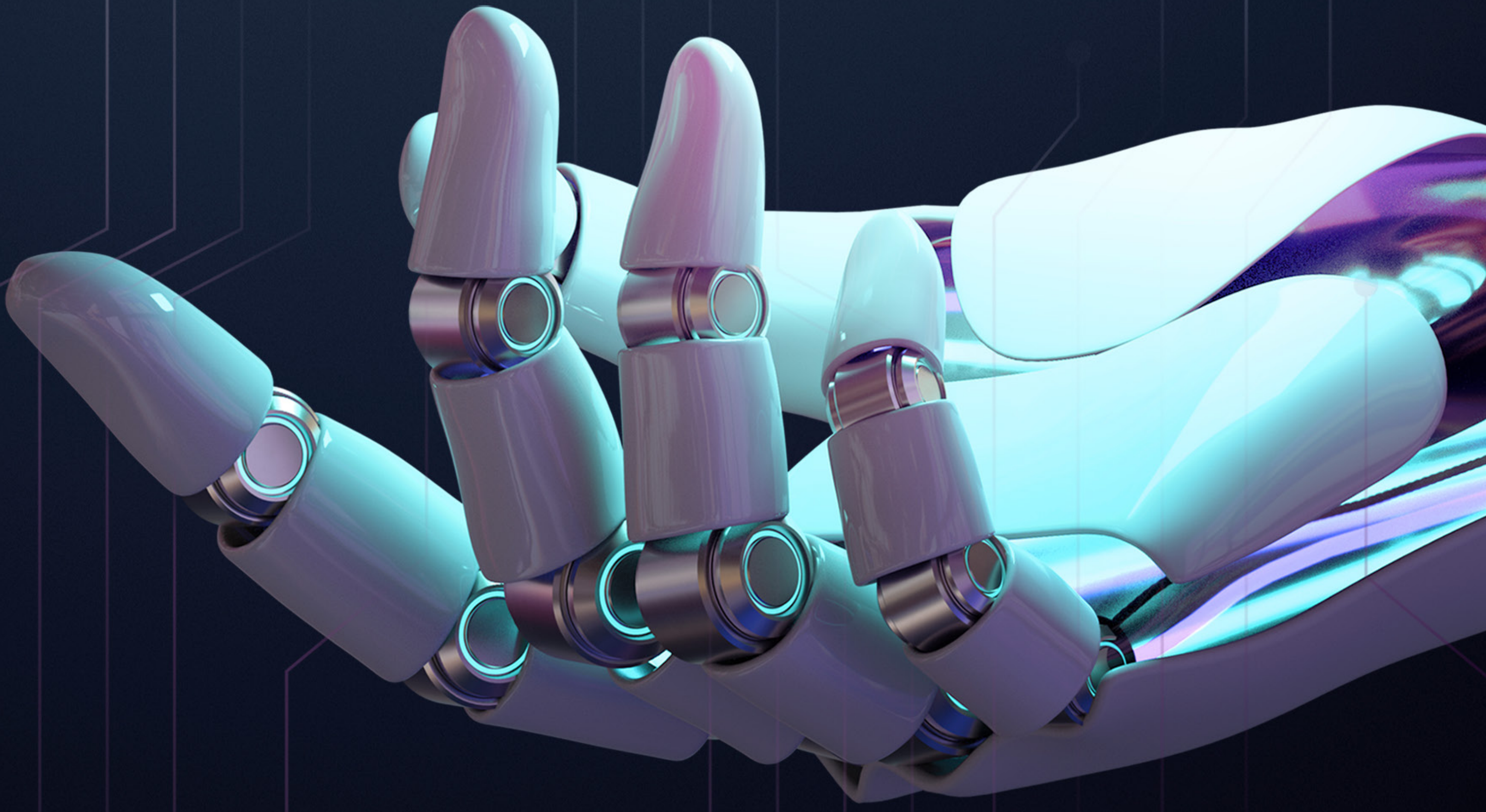
Trends:

1. AI is moving from assistive to autonomous roles, particularly in data-intensive tasks.
2. Human-AI collaboration is emerging as a key model, especially in complex decision-making scenarios.
3. AI is excelling in speed and pattern recognition, outperforming humans in many routine tasks.

Predictions:

1. Full AI autonomy is likely to materialize in the near future to handle routine alert triage, initial incident response, and basic threat intelligence gathering.
2. Human oversight is crucial in strategy development, ethical decision-making, and handling of novel, complex threats.
3. Emerging hybrid roles: We may see the rise of "AI Supervisors" - cybersecurity professionals specifically trained to manage and optimize AI systems.

The cybersecurity industry is moving towards a model where AI handles the bulk of routine, data-intensive tasks, allowing human experts to focus on strategic, creative, and ethically complex aspects of cybersecurity.



AI and Election Security

As we progress through 2024, a critical year for global elections, the intersection of AI and cybersecurity has shown significant impact on electoral processes. This section explores the emerging threats, notable incidents, and countermeasures around AI-influenced election security.

5.1 Deepfake Threats

The rise of sophisticated AI-generated deepfakes poses a significant threat to election integrity. These artificial media can be used to:

- Advance misinformation/disinformation campaigns
- Manipulate public opinion
- Suppress voter turnout
- Damage candidates' reputations

The rapid advancement of deepfake technology continues to outpace regulatory frameworks, making it a prime concern for election security experts [39].

5.2 Notable Incidents

Several incidents in early 2024 have highlighted the potential for AI misuse in elections:

- **New Hampshire Primary Robocall (January 2024):** A fake robocall campaign mimicking President Biden's voice attempted to suppress voter turnout. This incident set a concerning precedent for AI-generated voice deepfakes in electoral interference [3].

- **Baltimore County School Incident (April 2024):** A former athletic director used AI-generated audio to impersonate Principal Eric Eiswert. The fake audio broadcast racist and antisemitic comments, leading to Eiswert's temporary removal and a wave of hate-filled messages targeting the school [4].

- **Fake Donald Trump Live Stream (June 2024):** A convincing AI-generated deepfake video of Donald Trump was live streamed on a fake YouTube channel before the U.S. Presidential debate, quickly gaining 1.38 million subscribers. The deepfake video promoted cryptocurrency donations with promises of rewards, directing viewers to a fraudulent website mimicking official campaign branding [5].

These incidents underscore the World Economic Forum's 2024 Global Risks Report, which highlighted cyberattacks and AI-driven disinformation as top risks to the integrity of democratic processes [40].

5.3 Countermeasures and Recognition

The cybersecurity community is actively developing solutions to combat deepfake threats:

- **Deepfake Detection Technology:** At the RSA Conference in May 2024, Reality Defender, an AI security firm, won the "Most Innovative Startup" award for its deepfake detection technology Source. This recognition highlights the growing importance of tools to identify and mitigate AI-generated fake content [41].
- **Increased Awareness and Education:** Cybersecurity experts are emphasizing the need for public education on identifying deepfakes and verifying information sources [42].
- **Collaborative Efforts:** Tech companies, government agencies, and cybersecurity firms are increasingly collaborating to develop comprehensive strategies for combating AI-driven election interference [43].
- **Regulatory Discussions:** Policymakers are beginning to address the need for updated regulations to account for AI-generated content in political campaigns and election processes [44].

As we move into Q3 and beyond, with numerous significant elections on the horizon, the lessons learned from these early 2024 incidents will be crucial. The cybersecurity community faces the ongoing challenge of staying ahead of rapidly evolving AI capabilities while protecting the integrity of democratic processes.

Insights

Current Landscape:

1. Deepfakes dominate: The majority of AI-related election security incidents involve deepfake technology.
2. Diverse attack trajectories: From voter suppression to financial scams, AI is being weaponized in multiple ways.
3. Rapid escalation: The sophistication and scale of AI-driven attacks are increasing at an alarming rate.

Trends:

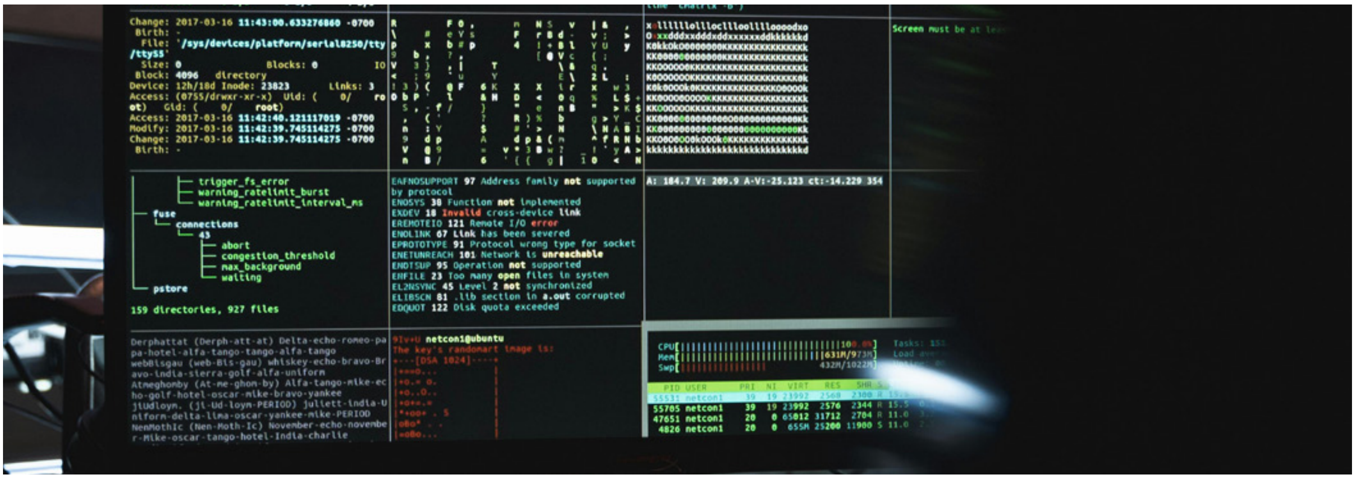
1. Reactive to proactive: The cybersecurity community is shifting from reactive measures to proactive strategies.
2. Multi-stakeholder approach: Collaboration between tech companies, government agencies, and cybersecurity firms is becoming crucial.
3. Emphasis on public education: There's a growing recognition of the need to educate the public about AI-generated misinformation.

Predictions:

1. AI arms race: We're likely to see an escalating contest between AI-powered attacks and AI-driven defenses.
2. Regulatory catch-up: Expect a surge in AI-specific election security regulations in the near future.
3. AI-native election processes: Future elections may incorporate AI from the ground up, both for security and efficiency.

AI is simultaneously the greatest threat and the most promising solution for election security. The challenge lies in staying ahead of malicious AI applications while leveraging AI's potential to safeguard democratic processes.

Key Developments in Q2 2024



The second quarter of 2024 has seen several significant advancements and challenges in the AI and cybersecurity landscape. This section outlines the most notable developments across technological advancements, security vulnerabilities, and ethical considerations.

6.1 Technological Advancements

- **OpenAI Unveils GPT-4o:** OpenAI released GPT-4o ("o" for "omni"), a cutting-edge AI model with exceptional audio-visual capabilities. The model demonstrates seamless reasoning across various media, including audio, vision, and text in real-time. Potential applications in cybersecurity include advanced threat detection, multi-factor authentication, and enhanced security analytics [(6)].

- **Google's LLM-Powered Fuzzing Framework:** Google made public a framework that leverages Large Language Models (LLMs) to enhance vulnerability discovery. This fuzzing framework, previously used internally, is now available to developers and security researchers worldwide. The release potentially revolutionizes the field of vulnerability detection, allowing for more efficient and thorough security testing [(7)].

- **AI Agents Approaching Junior Hacker Skill Level:** HackerOne co-founder Jobert Abma revealed the development of an AI agent capable of solving Hacker101's CTF challenges. This advancement suggests AI may soon match the skills of junior hackers, raising questions about the future role of entry-level human professionals in ethical hacking and vulnerability detection [(45)].

6.2 Security Vulnerabilities

- **Morris II: The AI Worm:** Researchers discovered a new form of malware dubbed "Morris II," named after the infamous 1988 Morris worm. This AI-powered worm exploits vulnerabilities in generative AI applications, posing a novel threat to systems designed for creative text generation, language translation, and image creation [(8)].

6.2 Security Vulnerabilities

- **Critical Vulnerability in AutoGPT:** A severe Cross-Site Request Forgery (CSRF) vulnerability (CVE-2024-1879) was discovered in AutoGPT version 0.5.0. This flaw allows attackers to execute arbitrary commands on the AutoGPT server by exploiting weaknesses in the API endpoint. The discovery highlights the security challenges in AI-powered automation tools [(46)].

- **CWiz Uncovers Vulnerability in AI-as-a-Service Platform:** Cybersecurity firm Wiz reported a critical vulnerability in Replicate, an AI-as-a-service platform. This flaw could potentially expose proprietary AI models and sensitive customer data to malicious actors, underscoring the importance of robust security measures in AI services [(9)].

6.3 Ethical Considerations

- **Pope Francis Addresses G7 Summit on AI Ethics:** At the G7 Summit in Apulia, Italy, Pope Francis delivered a landmark address on AI regulation and ethics. He emphasized the risks of AI dependency and called for increased human control and ethical oversight to preserve human dignity. The address echoed principles from the Rome Call for AI Ethics, highlighting the growing importance of ethical considerations in AI development and deployment within cybersecurity [(47)].

- **Bias in AI Algorithms:** Research studies have revealed persistent biases in AI models. Some studies found that these models were more likely to flag communications from certain ethnic groups as potential threats, raising concerns about fairness and discrimination. These biases have become a major concern in cybersecurity and are very hard to fix [(48)] [(49)] [(10)].

- **Explainability and Transparency:** The EU AI Act mandates disclosure of AI-generated content, such as deepfakes or other artificially manipulated content. High-risk AI systems, including those used in cybersecurity, must now provide comprehensive technical documentation demonstrating compliance and be registered in an EU database. Organizations are encouraged to implement standards and good practices for AI system development that align with the Act's requirements for transparency and explainability [(50)].

Current AI Regulatory Landscape

As AI technology rapidly advances, governments and international bodies are grappling with how to regulate its development and use.

Regulating AI presents unique challenges due to its rapid evolution and dual-use nature. As the World Economic Forum notes [51], AI regulation must focus on outcomes and require "eternal vigilance" to keep pace with technological advancements. Despite these challenges, many jurisdictions are taking steps to create comprehensive regulatory frameworks.

This section provides an overview of the current regulatory approaches across different regions.

7.1 European Union

The EU is at the forefront of AI regulation with its passing of the AI Act, which is the world's first comprehensive law on Artificial Intelligence. [11]
Key priorities include:

- Ensuring AI systems are safe, transparent, traceable, non-discriminatory, and environmentally friendly
- Mandating human oversight to prevent harmful outcomes
- Establishing a technology-neutral, uniform definition for AI.

7.2 United States

The U.S. has adopted a more decentralized approach to AI regulation:

- No specific federal law governs AI, but several states have enacted AI-related legislation [12].
- Sector-specific federal agencies address AI challenges in their domains:
- Federal Trade Commission (FTC) focuses on consumer protection [52].
- National Highway Traffic Safety Administration (NHTSA) regulates AI in autonomous vehicles [53] [54].
- Federal Aviation Administration considers AI in aviation through the Reauthorization Act [55].

7.3 Australia

Australia is in the process of developing its AI regulatory framework:

- Currently, no generally applicable AI law exists (56).
- A voluntary framework of eight AI Ethics Principles has been in place since 2019 [57].
- The New South Wales state government has issued AI-related guidance, including an AI Assurance Framework [58].
- In 2023, the federal government launched a consultation on "Safe and Responsible AI in Australia" [59].
- The government's 2024 interim response suggests major reforms are likely, with a focus on a risk-based framework and mandatory safeguards [60].

7.4 Middle East

Gulf countries are taking a "business-friendly" approach to AI regulation: (61)

- UAE and Saudi Arabia have been pioneers in AI adoption and promotion. Both countries have adopted a "soft law" approach through guidelines and principles [62].
- UAE established an AI strategy for 2031 and issued AI Ethics and Principles in 2022 [63].
- Saudi Arabia created the Saudi Data & AI Authority (SDAIA) and a National Strategy for Data & AI [64] [65].
- Several countries in the region have recently enacted data protection laws which will influence AI regulation [66] [67] [68].

7.5 Africa

The African Union (AU) is working to create a continent-wide approach to AI regulation:

- In February 2024, the AU Development Agency published a draft policy for AI regulation.
- Individual countries are also taking action:
- **Mauritius:** Published an AI Strategy in 2018 [69].
- **Kenya:** Formed an AI Task Force and launched a National Digital Master Plan [70].
- **Egypt:** Developed a national AI Strategy in phases [71].
- **South Africa:** Proposed a discussion document on AI in late March 2024 [72].
- **Nigeria:** Moving towards AI-specific policies while relying on existing legislation [73].
- **Morocco:** Using existing data protection laws while progressing in AI integration [74].

7.6 China

China's approach to AI regulation combines specific regulations with voluntary frameworks:

- The Cyberspace Administration of China (CAC) released Interim Measures for the Management of Generative Artificial Intelligence Services [75].
- The National Information Security Standardization Technical Committee (NISSTC) issued Practice Guidelines for Cybersecurity Standards [76].
- The Chinese Cybersecurity Law and New Generation AI Development Plan provide measures for data protection and cybersecurity in AI [77] [78].

7.7 Southeast Asia

The Association of Southeast Asian Nations (ASEAN) is working on regional AI guidelines:

- In January 2024, ASEAN released a set of guidelines on AI Governance and Ethics for all member nations. This effort aims to create a cohesive approach across Singapore, Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Thailand, and Vietnam [79].

7.8 Insights

As we reflect on the global AI regulatory landscape in Q2 2024, several key trends and insights emerge:

- Divergent Regulatory Approaches: The global approach to AI regulation remains fragmented. While the EU pushes forward with comprehensive legislation, other regions like the US and Middle East favor more flexible, sector-specific or principle-based approaches. This divergence could lead to regulatory arbitrage and challenges for companies operating across multiple jurisdictions.

- Shift from Voluntary to Mandatory Frameworks: There's a clear trend towards more binding regulations. Australia's move from voluntary principles to considering mandatory safeguards and the EU's progress on the AI Act signal a global shift towards stricter oversight. This trend is likely to accelerate as AI capabilities and associated risks continue to grow.

- Focus on High-Risk Applications: Regulators are increasingly adopting risk-based approaches with a focus on high-risk AI applications. This is evident in the EU's AI Act and Australia's interim response. In the context of cybersecurity, we can expect increased scrutiny of AI systems used in critical infrastructure, financial services, and national security.

- Emphasis on Ethical AI and Transparency: Ethical considerations and transparency requirements are becoming central to AI regulations worldwide. The ASEAN guidelines, China's approach to generative AI, and the EU's emphasis on "trustworthy AI" all reflect this trend. For cybersecurity applications, this could mean increased requirements for explainable AI in threat detection and response systems.

- Regulatory Catch-Up: The rapid pace of AI development, particularly in areas like generative AI, is outstripping regulatory efforts. This is evident in the reactive nature of some regulations, such as China's interim measures for generative AI services. Regulators are likely to face ongoing challenges in keeping pace with technological advancements.

- Global Cooperation vs. Digital Sovereignty: While there are efforts towards global cooperation (e.g., the ASEAN guidelines), we're also seeing a trend towards digital sovereignty, particularly in regions like China and the Middle East.

- Impact on Innovation and Competitiveness: The varying regulatory approaches could significantly impact global competitiveness in AI. Regions with more flexible regulations (like some Middle Eastern countries) may see accelerated AI adoption and innovation, while those with stricter rules may prioritize safety and ethical considerations at the potential cost of rapid development.

- **Cybersecurity Implications: In the cybersecurity context, these regulatory trends suggest:**
- Increased scrutiny of AI-powered security tools, particularly those used in critical infrastructure or handling sensitive data.
- Potential challenges in deploying global AI-based cybersecurity solutions due to varying regional requirements.
- A growing need for cybersecurity professionals with expertise in AI ethics and compliance.
- Possible limitations on the use of certain AI techniques in cybersecurity (e.g., restrictions on data use for training AI models).

- Emerging Role of International Bodies: We're seeing increased activity from international organizations like the EU, ASEAN, and African Union in shaping AI governance. This trend may lead to more harmonized regional approaches, potentially simplifying compliance for multinational corporations.

- Adaptive Regulation: Given the rapid pace of AI development, there's a growing recognition of the need for adaptive regulatory frameworks. Australia's approach of ongoing consultation and interim responses exemplifies this trend, which we may see replicated in other jurisdictions.

Conclusion

Q2 2024 has been a critical period for the integration of AI into cybersecurity, showcasing both immense potential and significant challenges. AI is rapidly transitioning from an assistive tool to an autonomous actor, fundamentally reshaping the landscape of cybersecurity operations. This shift is particularly evident in the deployment of AI-powered Security Operations Center (SOC) analysts and advanced threat intelligence platforms. However, as AI enhances defensive capabilities, it also introduces new vulnerabilities and attack vectors. Notable developments like AI-assisted malware and the discovery of AI-specific security flaws underscore the need for continuous vigilance and adaptive security measures.

The rise of AI-powered deepfakes presents a substantial threat to election integrity, emphasizing the urgent need for robust countermeasures and public education initiatives. As the global regulatory landscape for AI remains fragmented, we anticipate a shift towards more comprehensive and stringent regulations, potentially affecting the development and deployment of AI-powered cybersecurity solutions. Ethical considerations, including bias, transparency, and accountability, are increasingly crucial for maintaining public trust and ensuring the responsible development of AI in this field.

Looking ahead, the cybersecurity community must remain proactive, leveraging AI's transformative potential while addressing its inherent risks. Collaboration among technology developers, policymakers, and cybersecurity professionals will be essential to navigate the complex challenges and opportunities that lie ahead.

Appendix A:
Q2 2024 Funding Overview

April 2024 Funding Summary

WEEK 1

Total Funding

$563.7M

across 14 companies in 4 countries Source

Key Deals:

- **Cyera:** $300.0M Series C (Data Security Posture Management, USA) Source
- **Cohesity:** $150.0M Series F (Data Protection and Disaster Recovery, USA) Source
- **Alethea:** $20.0M Series B (Disinformation Mitigation, USA) Source
- **Andesite AI:** $15.3M Seed (National Security and Cyber Defense Readiness, USA) Source
- **StrikeReady:** $12.0M Series A (Contextual Awareness and Collaboration for Security Operations, USA) Source
- **Simbian:** $10.0M Seed (Security Operations LLM, USA) Source
- **PVML:** $8.0M Seed (Data Access Governance and Protection, Israel) Source
- **Knostic:** $3.3M Seed (Identity and Access Management for GenAI Applications, Israel) Source
- **Nymiz:** $3.0M Seed (GDPR Compliance Privacy Platform, Spain) Source
- **Upstream Security:** Undisclosed Venture Round (CAVS Fleet Security, Israel) Source

WEEK 2

Total Funding

$104.9M

across 8 companies in 3 countries Source

Key Deals:

- **Anvilogic:** $45.0M Series C (Security Operations and Analytics, USA) Source
- **Cynomi:** $20.0M Series A (vCISO Platform, UK) Source
- **NightVision:** $5.4M Seed (Web Application and API Protection, USA) Source

WEEK 3

Total Funding

$315.6M

across 15 companies in 4 countries Source

Key Deals:

- **Tines:** $50.0M Series B (Low-Code SOAR, Ireland) Source
- **Sublime Security:** $20.0M Series A (Email Security, USA) Source
- **Qohash:** $17.4M Series B (Data Security Posture Management, Canada) Source
- **Dropzone AI:** $16.9M Series A (AI-Agent-Enabled Security Operations Monitoring, USA) Source
- **BforeAI:** $15.0M Series A (Brand Protection and Threat Intelligence, France) Source
- **Prophet Security:** $11.0M Seed (AI-Assisted Security Operations, USA) Source
- **Amplifier Security:** $3.3M Pre-Seed (AI Copilot-Assisted Security Operations, USA) Source
- **TLA Innovation:** $500.0K Grant (Identity Authentication and Verification, USA) Source

WEEK 4

Total Funding

$628.5M

across 23 companies in 4 countries Source

Key Deals:

- **Corelight:** $150.0M Series E (Network Traffic Analysis, USA) Source
- **Elisity:** $37.0M Series B (Secure Remote Access, USA) Source
- **SafeBase:** $33.0M Series B (Security Program Presentation Platform, USA) Source
- **LayerX Security:** $26.0M Series A (Remote Browser Isolation, Israel) Source
- **Apptega:** $15.0M Private Equity (Security and Compliance Automation, USA) Source
- **DefenseStorm:** $13.0M Series C (MSSP for Financial Services, USA) Source
- **DeepKeep:** $10.0M Seed (AI Application Lifecycle Defense, Israel) Source
- **APEX:** $7.0M Seed (Generative AI Governance and Security, Israel) Source
- **Teleskope:** $5.0M Seed (Data Security Posture Management, USA) Source
- **Bricklayer AI:** $2.5M Pre-Seed (AI-Agent-Enabled Security Operations, USA) Source
- **Apptega:** Undisclosed Debt Financing (Security and Compliance Automation, USA) Source
- **Harmonic Security:** Undisclosed Seed (GenAI Platforms Usage Control, USA) Source

May 2024 Funding Summary

WEEK 1

Total Funding

$1.1B

across 15 companies in 6 countries Source

Key Deals:

- **Nudge Security:** $9.5M Seed (SaaS Security Posture Management, USA) Source
- **CyWreck:** Undisclosed Pre-Seed (Threat Modeling and Application Security, Singapore) Source
- **Treacle Technologies:** $478.8K Pre-Seed (Deception Technologies and IT/OT Security Consulting, India) Source

WEEK 2

Total Funding

$18.6M

across 5 companies in 3 countries Source

Key Deals:

- **c/side:** $1.7M Seed (Client-Side Security Platform, USA) Source

WEEK 3

Total Funding

$290.9M

across 14 companies in 4 countries Source

Key Deals:

- **Lumos:** $35.0M Series B (Identity and Access Management, USA) Source
- **WitnessAI:** $27.5M Series A (AI Governance and Safety, USA) Source
- **Patronus AI:** $17.0M Series A (Adversarial Testing and Risk Assessment of LLMs, USA) Source
- **Bolster AI:** $14.0M Series B (Anti-Fraud and Anti-Counterfeit, USA) Source
- **Averlon:** $8.0M Seed (Cloud-Native Application Protection, USA) Source
- **HoundDog.ai:** $3.1M Seed (Static Code Analysis for Sensitive Data Risks, USA) Source
- **Anvilogic:** Undisclosed Venture Round (Security Operations and Analytics, USA) Source
- **Velotix:** Undisclosed Seed (Data Access Governance, Israel) Source

WEEK 4

Total Funding

$44.7M

across 4 companies in 2 countries Source

Key Deals:

- **Transcend:** $40.0M Series B (Data Privacy Governance and Management, USA) Source
- **Zendata:** $2.0M Seed (AI Data Risk Governance, USA) Source

WEEK 5

Total Funding

$198.6M

across 14 companies in 4 countries Source

Key Deals:

- **ThreatModeler:** $60.0M Private Equity (Threat Modeling, USA) Source
- **Seven AI:** $36.0M Seed (AI-Agent-Enabled Security Operations, USA) Source
- **Stacklet:** $14.5M Series B (Cloud Posture and Governance, USA) Source
- **AirMDR:** $5.0M Venture Round (Managed Detection and Response, USA) Source
- **Liminal:** $5.0M Seed (Generative AI Governance, USA) Source
- **Alinia AI:** $2.4M Pre-Seed (Generative AI Governance Safety and Compliance, Spain) Source
- **ioAire:** $740.0K Seed (OT Network Management and Security, USA) Source
- **Almanax:** Undisclosed Pre-Seed (Cryptocurrency and Smart Contract Auditing, USA) Source
- **Brightside AI:** Undisclosed Grant (Personalized Security Awareness Training, Switzerland) Source

June 2024 Funding Summary

WEEK 1

Total Funding

$161.7M

across 9 companies in 5 countries Source

Key Deals:

- **Ohalo:** $3.6M Private Equity (Data Access Governance, UK) Source

WEEK 2

Total Funding

$377.2M

across 11 companies in 5 countries

Key Deals:

- **Aim Security:** $18.0M Series A (Securing Generative AI Applications, Israel) Source
- **Avaneidi:** $8.7M Series A (Secure Hosted Storage, Italy) Source
- **Trustwise AI:** $4.0M Seed (AI Governance Compliance and Safety, USA) Source

WEEK 3

Total Funding

$315.6M

across 12 companies in 3 countries Source

Key Deals:

- **HydroX AI:** $4.0M Angel (Artificial Intelligence (AI) security and safety, USA) Source
- **Co Guard:** Undisclosed Grant (Using LLMs to assess the security posture of infrastructure services, Canada) Source
- **Cloudian:** $23.0M Private Equity Round (file and object data protection, USA) Source

WEEK 4

Total Funding

$23.7M

across 6 companies in 5 countries Source

Key Deals:

- **Abnormal Security:** Undisclosed Venture Round (Email security, USA) Source
- **MicroSec:** Undisclosed Grant (Operational technology (OT) security, Singapore) Source

Contributors

Lead author

Confidence Staveley

Editor-In-Chief – AI Cyber Insights

Co-authors

Isu Abdulrauf

AI Researcher – AI Cyber Insights

Elizabeth Ekedoro

AI Researcher – AI Cyber Insights

Endnotes

1. https://aicyberinsights.com/meet-the-first-ai-soc-analyst/
2. https://www.japantimes.co.jp/news/2024/05/28/japan/crime-legal/man-arrested-malware-generative-ai
3. https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5
4. https://aicyberinsights.com/ai-deepfake-landed-school-principal-in-trouble
5. https://thecyberexpress.com/fake-trump-crypto-scam-presidential-debate/#google_vignette
6. https://aicyberinsights.com/openais-gpt-4o-flagship-model-and-everything-you-need-to-know
7. https://aicyberinsights.com/google-open-sources-ai-fuzzing-framework
8. https://aicyberinsights.com/unveiling-morris-ii-the-first-generation-ai-worm-targeting-generative-ai-systems
9. https://www.wiz.io/blog/wiz-research-discovers-critical-vulnerability-in-replicate
10. https://chiefexecutive.net/why-ai-bias-is-a-growing-cybersecurity-concern/
11. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
12. https://www.bclplaw.com/en-US/events-insights-news/2023-state-by-state-artificial-intelligence-legislation-snapshot.html
13. https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection
14. https://www.darkreading.com/cybersecurity-operations/automate-routine-operational-workflows-with-generative-ai
15. https://www.weforum.org/agenda/2023/06/cybersecurity-and-ai-challenges-opportunities/
16. https://www.youtube.com/watch?v=BvYXwpHWiWU
17. https://pinpointsearchgroup.com/cyber-security-vendor-funding-report-q2-2024/
18. https://www.returnonsecurity.com/p/cyber-market-update-april-2024#funding-insights
19. https://www.returnonsecurity.com/p/cyber-market-update-may-2024#funding-insights
20. https://pinpointsearchgroup.com/cyber-security-vendor-funding-report-q1-2024/
21. https://www.returnonsecurity.com/p/cyber-market-update-january-2024
22. https://www.returnonsecurity.com/p/cyber-market-update-february-2024#funding-insights
23. https://www.returnonsecurity.com/p/cyber-market-update-march-2024#funding-insights
24. https://www.institutedata.com/blog/ai-in-cyber-security/#:~:text=AI%20has%20become%20integral%20to,efficient%20risk%20assessment%20and%20management.
25. https://www.dropzone.ai/use-case/cloud
26. https://www.businesswire.com/news/home/20240425006696/en/Dropzone-AI-Raises-16.85-Million-Series-A-to-Equip-Cyber-Defenders-With-247-Generative-AI-powered-Autonomous-Investigations
27. https://www.dropzone.ai/blog/dropzone-ai-at-rsa-2024-pioneering-cybersecurity-innovation
28. https://www.anvilogic.com/learn/series-c
29. https://www.prnewswire.com/news-releases/bricklayer-ai-announces-2-5m-pre-seed-investment-to-bring-autonomous-ai-security-analysts-into-the-soc-302134689.html
30. https://aicyberinsights.com/ai-cybersecurity-startup-seven-ai-raises-36-million/
31. https://blog.bfore.ai/bforeai-announces-15-million-in-series-a-funding-led-by-syn-ventures

Endnotes

32. https://www.crunchbase.com/organization/cywreck
33. https://threatmodeler.com/threatmodeler-raises-60-million-from-invictus-growth-partners/?utm_source=returnonsecurity.com&utm_medium=newsletter&utm_campaign=security-funded-147-ai-hype-or-hope
34. https://www.researchgate.net/publication/372404024_USING_ARTIFICIAL_INTELLIGENCE_FOR_AUTOMATED_INCIDENCE_RESPONSE_IN_CYBERSECURITY
35. https://www.advantage.tech/role-ai-next-gen-vulnerability-scanning/
36. https://portal.bazeuniversity.edu.ng/staff/assets/uploaded_publications/20240324202221254586340.pdf
37. https://www.researchgate.net/publication/380806733_AI-Driven_Solutions_for_Social_Engineering_Attacks_Detection_Prevention_and_Response
38. https://his.diva-portal.org/smash/get/diva2:1880041/FULLTEXT01.pdf
39. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
40. https://www.realitydefender.com/blog/reality-defender-wins-most-innovative-startup-at-rsa-conference-innovation-sandbox
41. https://www.weforum.org/agenda/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond
42. https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
43. https://aicyberinsights.com/impact-and-counter-measures-against-ai-powered-electoral-scam
44. https://aicyberinsights.com/ai-agents-might-eventually-replace-junior-hackers
45. https://aicyberinsights.com/critical-vulnerability-identified-in-popular-open-source-ai-agent
46. https://aicyberinsights.com/key-address-on-ai-regulation-and-ethics-at-the-g7-summit-2024
47. https://www.weforum.org/agenda/2021/07/ai-machine-learning-bias-discrimination/
48. https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/
49. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/02/decoding-the-eu-artificial-intelligence-act.pdf
50. https://www.weforum.org/agenda/2024/05/why-regulating-ai-can-be-surprisingly-straightforward-providing-you-have-eternal-vigilance/
51. https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals
52. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/automated_vehicles_policy.pdf
53. https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf
54. https://www.congress.gov/bill/118th-congress/house-bill/3935/text
55. https://www.dentons.com/en/insights/articles/2024/april/26/the-current-state-of-play-for-the-regulation-of-ai-in-australia-in-2024#:~:text=There%20is%20currently%20no%20generally,Principles%20has%20existed%20since%202019
56. https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles
57. https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assessment-framework

Endnotes

58. https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/Safe-and-responsible-AI-in-Australia-discussion-paper.pdf
59. https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/safe-and-responsible-ai-in-australia-governments-interim-response.pdf
60. https://www.pinsentmasons.com/out-law/analysis/gulf-governments-approach-to-ai-regulation
61. https://www.york.ac.uk/assuring-autonomy/news/blog/ai-regulation-middle-east/
62. https://ai.gov.ae/publications/
63. https://www.researchgate.net/publication/350732938_The_Saudi_Data_Artificial_Intelligence_Authority_SDAIA_Vision_Leading_the_Kingdom's_Journey_toward_Global_Leadership
64. https://ai.sa/Brochure_NSDAI_Summit%20version_EN.pdf
65. https://en.incarabia.com/bahrain-approves-comprehensive-ai-regulation-law-652890.html
66. https://www.mcit.gov.qa/en/about-us/qatar%E2%80%99s-national-ai-strategy
67. https://www.businessstartupqatar.com/news/qatar-committed-protecting-personal-data/#:~:text=Law%20number%2013%2C%20ratified%20in,importance%20of%20protecting%20personal%20data.
68. https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf
69. https://cms.icta.go.ke/sites/default/files/2022-04/Kenya%20Digital%20Masterplan%20 2022-2032%20Online%20Version.pdf
70. https://ai.gov.eg/Egypt%20National%20AI%20Strategy%20(6-4-2021)4.pdf
71. https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf
72. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-nigeria#:~:text=There%20is%20currently%20no%20specific,Artificial%20Intelligence%20Policy%20(NAIP).
73. https://www.advoc.com/news/morocco-artificial-intelligence-in-the-moroccan-legal-framework
74. https://www.chinalawtranslate.com/en/generative-ai-interim/
75. https://www.tc260.org.cn/front/postDetail.html?id=20230825190345
76. https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
77. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/
78. https://asean.org/book/asean-guide-on-ai-governance-and-ethics/

www.aicyberinsights.com