Scientific and Practical Cyber Security Journal (SPCSJ) 9(3): 190 – 206 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

THE AI-HYGIENE PARADOX: FROM SILICON TO COGNITION IN THE AGE OF INTELLIGENT THREATS

Juan David Gamboa Saenz[1]

[1]Independent Researcher, Electronic Engineer, Cybersecurity Professional, Quantum Programmer

ABSTRACT: The emergence of Artificial Intelligence (AI) has created a fundamental paradox, simultaneously weaponizing cyber threats to an unprecedented degree and offering the only viable path to a resilient defense. This necessitates a paradigm shift from static, procedural hygiene to a dynamic, automated, and intelligent model. This paper synthesizes recent literature, industry reports, and empirical data to analyze this dual-use phenomenon, arguing that the paradox extends beyond software to the integrity of the hardware supply chain and the emerging frontier of neuro-security. Key findings reveal that AI-driven attacks, particularly in social engineering, are rendering traditional defenses obsolete. In response, AI-powered solutions for threat detection, automated hygiene, and adaptive user training are becoming critical. The paper presents a framework for "Intelligent Hygiene" that spans software, hardware, and cognition, arguing that for nations like Georgia, which stand at a geopolitical crossroads, navigating this paradox is a matter of national security. The analysis concludes that mastering the full spectrum of the AI-Hygiene Paradox is the central challenge for security practitioners in the current era.

KEYWORDS: *Artificial Intelligence, Cyber Hygiene, Cybersecurity, Phishing, Threat Detection, Security Automation, Machine Learning, Mind-Machine Controller, Supply-Chain Security, Deobfuscation, Cognitive Hygiene, Zero Trust, Georgia.*

1. INTRODUCTION

Artificial Intelligence (AI) stands as the most disruptive and transformative force in the modern cybersecurity landscape. It is not merely an incremental enhancement to existing tools but a foundational technology that is fundamentally reshaping the tactics, techniques, and procedures (TTPs) of both malicious actors and cyber defenders (Morgan Stanley n.d.; Shepherd Insurance 2024). The strategic importance of AI is underscored by significant economic investment; the global market for AI-based cybersecurity products, valued at approximately $15 billion in 2021, is projected to surge to an estimated $135 billion by 2030 (Tech Advisors 2025).

This paper puts forth a central thesis: the proliferation of AI has given rise to the "AI-Hygiene Paradox," a state in which the very technology that fuels the most sophisticated and scalable cyber threats is also the essential and indispensable component of their mitigation (Hoxhunt 2025; VE3 Global 2025). This paradox forces a radical departure from traditional, reactive cyber hygiene practices—which are often characterized by static checklists and manual processes—toward a new paradigm of proactive, automated, and intelligent defense. This paper will argue that this paradox is not confined to software but extends to the very silicon on which our digital world is built and even to the future of human-computer interaction itself. The core challenge for organizations is no longer simply to adopt AI but to navigate its inherent duality, harnessing its defensive power more effectively than adversaries can weaponize its offensive capabilities.

The analysis presented herein is tailored for submission to the *Scientific and practical cyber security journal* (ISSN 2587-4667). As a quarterly publication of the Tbilisi-based Scientific Cyber Security Association (SCSA), this journal provides a fitting venue for this research (SCSA n.d.). For Georgia, a nation that experienced a paradigm shift after the 2008 cyberattacks revealed the intrinsic link between digital resilience and national security, the themes of this paper are particularly resonant (Tkeshelashvili 2025). The journal's established categories in AI, hardware, and general cybersecurity align perfectly with the scope of this paper, which seeks to bridge theoretical concepts with the tangible, real-world implications for a nation actively working to secure its digital future amidst a complex geopolitical environment (SCSA n.d.).

To frame the central conflict of this paper, Table 1 provides a concise overview of AI's dual role across critical cybersecurity domains. This table serves as a conceptual anchor, illustrating the offensive and defensive applications that define the AI-Hygiene Paradox.

Table.1. AI's Dual Role Across Critical Cybersecurity Domains

Domain	Offensive AI Application (Weaponization)	Defensive AI Application (Shield)
Social Engineering	Generative AI creates hyper-realistic, personalized phishing and Business Email Compromise (BEC) emails at scale (ECI 2025; Shepherd Insurance 2024).	Natural Language Processing (NLP) and behavioral analysis detect anomalies in communication; AI-powered training simulates attacks (Cynet 2025; Morgan Stanley n.d.).
Malware	AI generates polymorphic malware that evades signature-based detection (VE3 Global 2025).	Machine Learning (ML) models analyze software characteristics to identify novel malware without prior signatures (Cynet 2025; Secureframe n.d.).
Vulnerability Mgmt.	AI automates the discovery of software vulnerabilities and zero-day exploits (Shepherd Insurance 2024).	AI automates asset discovery, vulnerability scanning, and patch management prioritization (Help Net Security 2025; Metomic n.d.).
Credential Access	AI-powered algorithms crack common passwords in seconds and rapidly analyze stolen data (Shepherd Insurance 2024; Tech Advisors 2025).	AI-driven behavioral biometrics (keystroke/mouse dynamics) and adaptive Multi-Factor Authentication (MFA) enhance authentication (VE3 Global 2025).

Analyst Operations	AI accelerates the review of stolen data for rapid exploitation (Shepherd Insurance 2024).	AI "Copilots" automate alert triage, threat hunting, and incident reporting, augmenting human analysts (Cynet 2025; Wong and Saade 2025).

2. THE WEAPONIZATION OF AI: A NEW TAXONOMY OF CYBER THREATS

The advent of accessible and powerful AI has equipped cybercriminals with a formidable arsenal, amplifying the speed, scale, and sophistication of their attacks. This weaponization is not a future-state concern but a present-day reality, creating a new class of threats that systematically dismantle traditional security controls. This section provides a taxonomy of these offensive AI applications, supported by recent empirical data.

2.1 AI-ENHANCED SOCIAL ENGINEERING AND PHISHING

Social engineering remains the most prominent and effective vector for AI weaponization. The use of Generative AI and Large Language Models (LLMs) has revolutionized phishing and Business Email Compromise (BEC) attacks by systematically eliminating the classic red flags—such as poor grammar, awkward phrasing, and generic greetings—that once betrayed their malicious intent (ECI 2025; Mobile ID World 2025; Shepherd Insurance 2024). These models can now produce highly persuasive, contextually aware, and personalized messages at an unprecedented scale, making them nearly indistinguishable from legitimate communications.

The statistical evidence of this shift is stark and alarming. In 2024, a staggering 96% of organizations were negatively impacted by phishing attacks (Mobile ID World 2025). The success rate has skyrocketed, with one report finding that enterprise employees clicked on phishing links at three times the rate in 2024 compared to 2023 (Cyber Magazine 2025). The convincing nature of these attacks is reflected in user behavior; 78% of recipients now open AI-generated phishing emails, and a concerning 21% proceed to click on the malicious content within (Tech Advisors 2025). This trend is part of a broader surge in sophisticated scams, which saw a 135% increase attributed to the influence of AI (Shepherd Insurance 2024).

Beyond simple email generation, the development of "AI spear phishing agents" marks a significant escalation. Longitudinal experiments conducted from 2023 to 2025 have demonstrated that these AI agents have not only reached parity with but have now surpassed the capabilities of elite human red teams in crafting effective phishing campaigns. As of March 2025, AI-driven phishing attacks were found to be 24% more effective than those created by human experts, representing a remarkable 55% relative performance improvement in just over two years (Hoxhunt 2025). This rapid, accelerating capability gap suggests that human-led offensive efforts will soon be rendered obsolete by their AI counterparts.

This trend extends beyond text-based attacks to multimedia deception. AI is now widely used to create hyper-realistic deepfake audio and video for advanced impersonation scams (Morgan Stanley n.d.; IEEE Transmitter 2023). These attacks are particularly pernicious, targeting high-value individuals and exploiting trust to authorize fraudulent transactions or extract sensitive information. The financial impact is already immense, with impersonation scams costing an estimated $12.5 billion in 2023 (VE3 Global 2025). A high-profile case in Hong Kong saw a finance firm lose $25 million after employees were deceived by a deepfake video call featuring a digitally recreated version of the company's Chief Financial Officer (Tech Advisors 2025).

2.2 AUTOMATED VULNERABILITY DISCOVERY AND MALWARE GENERATION

AI is also being applied to automate the technical aspects of cyberattacks, lowering the barrier to entry for less-skilled actors and increasing the operational tempo for sophisticated ones (ECI 2025). AI algorithms enable threat actors to scan for and identify software vulnerabilities across vast networks far more effectively and rapidly than is possible with manual methods (Shepherd Insurance 2024). This accelerates the process of finding exploitable weaknesses in an organization's attack surface.

Furthermore, the rise of AI chatbots and no-code development tools has led to a democratization of malice. These platforms allow threat actors with minimal technical expertise to generate functional, harmful code on demand (Shepherd Insurance 2024). This has fueled the proliferation of polymorphic malware—malicious code that can automatically alter its own structure and signatures to evade detection by traditional antivirus solutions (VE3 Global 2025). A notable example of this threat class is the "Morris II" worm, a self-replicating generative AI worm unveiled by researchers in April 2024, which demonstrated the potential for AI to autonomously spread and exfiltrate data (Tech Advisors 2025).

2.3 CREDENTIAL COMPROMISE AND DATA ANALYSIS AT SCALE

Credential-based attacks have been supercharged by AI. Modern AI-powered algorithms have demonstrated the ability to crack vast sets of common passwords with terrifying speed; one report indicated that such tools could successfully decipher over 51% of a large list of common passwords in under one minute (Shepherd Insurance 2024; Tech Advisors 2025). This capability renders weak or reused passwords almost instantly vulnerable.

The utility of AI does not end with the initial breach. Once a threat actor has successfully exfiltrated data, AI algorithms are employed to accelerate the analysis process (Shepherd Insurance 2024). These tools can rapidly sift through terabytes of unstructured data—such as emails, documents, and source code—to identify the most valuable information for exploitation or extortion. This speed compresses the timeline for defenders, significantly reducing the window of opportunity to respond and mitigate damage before the stolen information is weaponized. This threat is particularly acute in the wake of large-scale data breaches, such as the 2024-2025 incident that allegedly exposed the personal data of nearly the entire population of Georgia, creating a massive pool of information for malicious actors to exploit (Civil.ge 2025a; Cybernews 2024).

The convergence of these trends points toward a fundamental shift in the threat landscape. The combination of AI tools that lower the technical barrier to entry (ECI 2025; Shepherd Insurance 2024) and the commercial availability of attack platforms, such as Phishing-as-a-Service for as little as $250 per month (Guardz 2024), signifies the industrialization of cybercrime. This is not merely an increase in the number of attacks, but a change in their very nature. The threat actor is no longer exclusively a highly skilled, well-resourced nation-state or organized crime syndicate. It is now also a low-skill individual equipped with powerful, automated tools. This democratization of advanced attack capabilities means that defensive models can no longer be predicated on profiling a finite number of known adversaries. The focus must pivot from understanding *who* is attacking to defending against the *method* of attack itself, as these methods are now accessible to a vast, diverse, and unpredictable global actor base. Security postures must be re-architected to withstand a continuous, high-volume barrage of sophisticated, AI-generated attacks.

3. THE OBSOLESCENCE OF LEGACY CYBER HYGIENE

The AI-driven threat landscape described in the previous section renders traditional cyber hygiene practices not just inadequate, but dangerously obsolete. Legacy hygiene is largely built on a foundation of static, compliance-driven, and human-operated processes. This model is fundamentally ill-equipped to contend with the speed, scale, and adaptive nature of AI-powered attacks, which operate at machine speed and evolve faster than manual security controls can respond (VE3 Global 2025). This section deconstructs the specific failure points of conventional hygiene and presents a comparative framework to illustrate the necessary paradigm shift.

The core failure of legacy hygiene lies in its reliance on predictable, rules-based defenses against an unpredictable, intelligent adversary. Key pillars of traditional security are crumbling under the pressure of AI:

- **Password Policies:** For decades, security advice has centered on password complexity and frequent rotation. However, this is largely ineffective against AI-powered cracking algorithms that leverage pattern recognition and massive computational power to guess passwords in minutes or seconds (VE3 Global 2025). A policy that meets a compliance checkbox for rotation frequency provides a false sense of security against a threat that can brute-force credentials almost instantaneously.
- **Signature-Based Antivirus:** Traditional antivirus (AV) software operates by matching file signatures against a database of known malware. This reactive model is completely blind to the novel, polymorphic malware generated by AI, which is designed specifically to have no pre-existing signature (VE3 Global 2025). Each instance of the malware can be unique, rendering signature-based detection useless.
- **Email Filters:** Conventional Secure Email Gateways (SEGs) rely on rules-based logic, keyword filtering, and sender reputation to block malicious emails. AI-crafted phishing messages are engineered to bypass these static defenses (VE3 Global 2025). They use flawless grammar, legitimate-looking sender domains, and contextually relevant content that does not trigger traditional filters. The scale of this failure is significant, with reports indicating that over 1.5 million malicious emails successfully evaded SEGs in 2023 alone (Guardz 2024).
- **Manual Processes:** Foundational hygiene tasks like patching, configuration management, and security log review have historically been manual or semi-automated processes. These human-speed operations are far too slow and prone to error to counter threats that are discovered, weaponized, and deployed at machine speed. A vulnerability that takes a security team weeks to patch can be exploited by an automated AI scanner within hours of its disclosure (Help Net Security 2025).

To fully grasp the required evolution, it is useful to compare the legacy model directly with the principles of an AI-powered "Intelligent Hygiene" model. Table 2 provides this comparative framework, highlighting the fundamental shift in approach across key security domains.

Table.2. Legacy Hygiene vs. Intelligent Hygiene

Security Domain	Legacy Hygiene (Obsolete Model)	Intelligent Hygiene (AI-Powered Model)
Guiding Principle	Compliance-driven, static checklist.	Risk-driven, adaptive, and continuous (ChannelPro Network 2025).
Threat Detection	Signature-based (known threats),	Behavior-based (unknown threats), proactive anomaly detection (Cynet 2025;

	reactive.	Secureframe n.d.).
Patch Management	Manual or scheduled, periodic scanning.	Automated, risk-prioritized, continuous scanning and deployment (Help Net Security 2025).
Authentication	Static passwords, basic MFA.	Passwordless, adaptive MFA, behavioral biometrics (keystroke dynamics) (VE3 Global 2025).
User Training	Annual, one-size-fits-all awareness sessions.	Continuous, personalized, adaptive simulations based on real-world threats and user behavior (Keepnet Labs 2024).
Data Protection	Perimeter-focused, network-based controls.	Data-centric, Zero Trust architecture, automated classification and encryption (VE3 Global 2025).
Incident Response	Manual investigation, human-speed reaction.	Automated triage and response (SOAR), machine-speed containment (Cynet 2025; Secureframe n.d.).

The rapid adoption of public AI tools for productivity purposes, often without commensurate security oversight, is creating a new and insidious form of risk that can be termed "hygiene debt." As employees rush to leverage platforms like ChatGPT to improve efficiency, they may inadvertently paste sensitive corporate data—including proprietary source code, internal strategy documents, or personally identifiable information (PII)—into third-party models, effectively exfiltrating it outside the organization's control (TNTMAX 2025). This behavior creates a widening gap between the technologies being used and the hygiene practices meant to secure them.

This situation exposes a critical flaw in traditional audit and compliance regimes. An organization can be fully "compliant" with an outdated security standard that mandates practices like 90-day password rotation while being profoundly insecure against modern AI-driven threats (ECI 2025). It highlights an urgent need for regulatory frameworks and industry standards to evolve. They must move beyond static, procedural checks and begin to recognize, and ultimately mandate, the principles of intelligent hygiene—such as automated threat detection, risk-based patching, and adaptive controls—as the new baseline for due diligence in the age of AI.

4. THE PARADOX IN SILICON: DEOBFUSCATION AND HARDWARE INTEGRITY

The AI-Hygiene Paradox is not confined to the realm of software; its principles extend down to the very silicon upon which our digital world is built. The struggle against **deobfuscation** in the semiconductor supply chain serves as a perfect hardware-level analogue to the software-based arms race. It reveals the same dual-use dynamic, where the tools of protection and predation are inextricably linked.

Deobfuscation is the adversarial process of reverse-engineering the protective measures—such as logic locking and circuit camouflage—that designers embed within an Integrated Circuit (IC) to protect their intellectual property (IP). This creates a direct parallel with the AI paradox:

- **The "Defensive" Use (Obfuscation):** Similar to using AI for defense, logic obfuscation is a proactive measure to safeguard a design. Designers intentionally add complexity to conceal the chip's true function, protecting valuable IP from theft and preventing the insertion of malicious hardware Trojans.
- **The "Offensive" Use (Deobfuscation):** This is the adversarial counter-attack. Just as threat actors weaponize AI to bypass software defenses, adversaries use sophisticated techniques—from side-channel analysis to insider collusion—to strip away that obfuscation, steal the design, or compromise the chip's integrity.

This demonstrates that legacy assurance models are as obsolete in hardware as they are in software. Trusting a chip simply because it came from a certain foundry is no longer sufficient, especially for a nation like Georgia that faces persistent state-sponsored threats to its critical infrastructure (Binding Hook 2024; VOA News 2024). The entire AI development and hardware supply chain is vulnerable to attacks like data poisoning and data leakage, which can compromise a system before a single line of code is executed (Treasury Department n.d.).

The solution, therefore, must also mirror the principles of intelligent hygiene. An **"Automated Supply-Chain Hygiene"** is required, moving beyond static trust to a dynamic, verifiable model. This involves:

- **Automated Circuit Forensics:** Using AI and machine learning to analyze telemetry from the fabrication and testing stages. By monitoring power consumption, thermal patterns, and I/O responses, these systems can detect the subtle "fingerprints" of a deobfuscation attempt in real-time, much as a modern EDR solution detects behavioral anomalies on an endpoint (Cynet 2025; Secureframe n.d.).
- **Cryptographically-Anchored Provenance:** Applying a Zero Trust framework to the supply chain itself (VE3 Global 2025). This means every step of the design and manufacturing process must be attested to with secure, immutable cryptographic signatures (ideally post-quantum). This creates an auditable chain of custody that makes unauthorized modifications or IP theft far more difficult to conceal.

Just as the SCSA journal recognizes hardware vulnerabilities as a key area of research (SCSA n.d.), practitioners in Georgia and beyond must recognize that a holistic security posture cannot exist without addressing the integrity of the underlying hardware.

5. AI-POWERED DEFENSE: TOWARD AN AUTOMATED AND INTELLIGENT SECURITY POSTURE

In response to the weaponization of AI, a new generation of defensive technologies has emerged, leveraging the same underlying principles of machine intelligence to build a more resilient, automated, and proactive security posture. The transition from legacy hygiene to an intelligent model is not merely about acquiring new tools, but about re-architecting security operations around the core capabilities of AI. This section details the practical application of AI in modern defense, from advanced threat detection to securing the AI development pipeline itself.

5.1 ADVANCED THREAT DETECTION AND RESPONSE

The cornerstone of modern defense is the ability to detect threats that have never been seen before. This requires a move away from reactive, signature-based methods toward proactive, behavior-based analysis. The core technologies driving this shift are Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP), which are used to analyze vast and complex datasets in real time (Cynet 2025; Path of Science 2024). These systems work by first establishing a comprehensive baseline of normal activity across an organization's networks, endpoints, and user behaviors. Once this baseline is established, the AI can continuously monitor for anomalous patterns that deviate from the norm, flagging them as potential threats long before they can cause harm (Cynet 2025).
The technical application of these technologies is diverse and highly specialized:

- **Machine Learning Classifiers:** Supervised learning models, such as Support Vector Machines (SVM) and Random Forests, are trained on massive datasets of both legitimate and malicious communications. They learn to classify new, incoming data—like emails or web traffic—with a high degree of accuracy, effectively distinguishing sophisticated phishing attempts from benign messages (Path of Science 2024; Roxiler 2025).
- **Deep Learning Architectures:** More complex neural networks are used for nuanced analysis. Convolutional Neural Networks (CNNs), for instance, can analyze the visual components of a website—such as logos, fonts, and page layouts—to detect subtle signs of brand impersonation and spoofing. Recurrent Neural Networks (RNNs) are adept at analyzing sequential data, making them ideal for identifying malicious patterns in URL structures, API call sequences, and email metadata (Path of Science 2024).
- **Natural Language Processing:** NLP models are crucial for combating AI-generated social engineering. They are trained to understand the context, sentiment, and intent behind language, allowing them to detect the linguistic cues of a phishing attack—such as manufactured urgency, persuasive language, or unusual requests—that static, keyword-based filters would miss (Path of Science 2024; Roxiler 2025).

Beyond detection, AI is a critical enabler of automated incident response. By integrating with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms, AI-driven systems can trigger pre-defined response playbooks without human intervention (Cynet 2025). For example, upon detecting a known malware sample on an endpoint, the system can automatically isolate that device from the network, block the malicious IP address at the firewall, and generate a trouble ticket for a human analyst—all within milliseconds. This machine-speed containment drastically reduces incident response times and limits the potential blast radius of an attack (Secureframe n.d.).

5.2 AUTOMATING FOUNDATIONAL HYGIENE

While AI is essential for combating advanced threats, its role in perfecting foundational hygiene practices is equally critical. Many security breaches do not stem from sophisticated zero-day exploits but from basic failures in security posture management. AI-powered automation can enforce these fundamentals at a scale and with a consistency that is impossible to achieve manually (Help Net Security 2025; Metomic n.d.).

- **Asset Discovery and Management:** A core tenet of security is that you cannot protect what you cannot see. In complex, modern IT environments, maintaining a complete and accurate asset inventory is a major challenge. AI-driven automation is critical for continuously discovering all assets connected to the network, including unsanctioned "shadow IT," forgotten cloud instances, and misconfigured "dangling" DNS records, all of which represent common and dangerous hygiene failure points (Help Net Security 2025).

- **Automated Patch and Configuration Management:** Manually patching thousands of systems is a slow, laborious, and error-prone process. AI-driven systems can automate the entire patch management lifecycle. They continuously scan for vulnerabilities, prioritize patching based on dynamic risk factors (such as whether a vulnerability is being actively exploited in the wild), deploy the patches across the enterprise, and provide automated rollback capabilities in case a patch causes system instability. This closes critical windows of vulnerability far more rapidly than any manual process could (Help Net Security 2025; Plain English 2025).
- **Exposure Management:** AI-powered tools can continuously and automatically audit an organization's security posture against its defined policies. These systems can verify that critical controls like MFA are enabled on all required accounts, detect the use of weak or compromised passwords, and flag systems running outdated or unsupported software, providing a real-time view of security hygiene and compliance (Help Net Security 2025).

5.3 SECURING THE AI SUPPLY CHAIN

As organizations increasingly build and deploy their own AI models, these systems and their underlying data pipelines become high-value targets for attackers. The AI development lifecycle itself represents a new, critical attack surface that must be secured—a meta-challenge for the industry (Treasury Department n.d.).

The primary threats to AI models include:

- **Data Poisoning:** An attacker feeds malicious or biased data into the model during its training phase. This can corrupt the model's decision-making process, causing it to produce inaccurate results, create backdoors, or fail in predictable ways when presented with specific inputs (Morgan Stanley n.d.; VE3 Global 2025).
- **Model Evasion:** Attackers craft specific inputs designed to trick a trained model into making an incorrect classification. For example, slightly altering an image in a way that is imperceptible to humans can cause an image recognition model to misidentify it completely (VE3 Global 2025).

Defending the AI supply chain requires applying rigorous security principles to the development environment. A Zero Trust Framework (ZTF) is essential, ensuring that all access to training data, models, and infrastructure is strictly controlled, authenticated, and continuously monitored (VE3 Global 2025). AI development firms must practice what they preach, using their own AI-driven Intrusion Detection Systems (IDS) and SIEMs to protect their training environments from intrusion and manipulation (VE3 Global 2025). Recognizing this need, major technology providers are offering comprehensive solutions. Microsoft, for example, provides an integrated suite of tools—including Microsoft Defender for threat protection, Microsoft Purview for data governance, and Microsoft Entra for identity and access management—designed to discover, protect, and govern AI applications throughout their entire lifecycle, from code to runtime (Microsoft n.d.a).

The widespread automation of security tasks—from alert triage (Secureframe n.d.) and patch management (Help Net Security 2025) to incident response (Cynet 2025)—is fundamentally redefining the role of the human cybersecurity professional. The tedious, repetitive, and low-level work that once consumed the majority of an analyst's time is increasingly being handled by AI. This does not make the human obsolete; rather, it elevates their function. Humans are still uniquely required for the complex, creative, and context-aware tasks that are beyond the scope of current AI: setting strategic security policy, investigating truly novel threats flagged by AI systems, and making high-stakes decisions that require ethical judgment and a deep understanding of business risk (Help Net Security 2025; Secureframe n.d.).

This new collaborative model is best exemplified by the emergence of "Security Copilots" (Wong and Saade 2025). These AI assistants are designed to augment, not replace, human analysts. They act as a powerful force multiplier, streamlining investigations by summarizing complex alerts, hunting for related threats across the network, and providing guided remediation steps. The most valuable skill for a cybersecurity professional is no longer manual technical execution but the ability to strategically manage, configure, and critically interpret the outputs of a fleet of AI-driven security systems. This profound evolution carries significant implications for how organizations should approach hiring, training, and structuring their security operations centers (SOCs) in the years to come.

6. CASE STUDY: THE PHISHING ARMS RACE AND THE HUMAN FACTOR

The dynamic conflict surrounding phishing serves as a perfect microcosm of the broader AI-driven arms race in cybersecurity. It is a domain where offensive and defensive technologies are locked in a cycle of rapid, escalating innovation, with the human user caught squarely in the middle. This section uses phishing as a case study to explore this technological conflict and to analyze the transformation of the "human factor" from the weakest link into a potentially resilient, AI-hardened layer of defense.

As established in Section 2, the offensive side of this arms race is advancing at a formidable pace. AI-generated phishing campaigns are now demonstrably more effective than those crafted by human experts, achieving higher click-through rates and successfully bypassing legacy defenses (Hoxhunt 2025). This offensive push is being met by an equally sophisticated defensive response. AI-powered detection tools now analyze a multitude of vectors to identify malicious emails, including the linguistic content, sender behavior patterns, visual elements of landing pages, and the structure of embedded URLs (Path of Science 2024; Roxiler 2025). This direct, technology-on-technology confrontation defines the modern phishing landscape.

However, no technical defense is perfect. Inevitably, some malicious emails will reach an employee's inbox. For this reason, transforming the human element of security remains a critical objective. The statistics are clear: the human element is implicated in a majority of all data breaches, with phishing being a primary initial access vector (Keepnet Labs 2024). Traditional Security Awareness Training (SAT), often consisting of a single, generic annual presentation, has proven largely ineffective against the personalized and convincing nature of modern threats.

In response, AI is being leveraged to revolutionize SAT, transforming it from a static, compliance-focused exercise into a dynamic, adaptive, and continuous learning process (Keepnet Labs 2024). This new generation of training is built on several key principles:

- **Personalization and Adaptation:** AI-driven training platforms analyze an individual user's role, responsibilities, and historical performance in simulations. This data is used to create tailored learning paths that address specific knowledge gaps. For example, an employee in the finance department might receive more training on invoice fraud, while an executive might be trained to spot BEC attacks (Keepnet Labs 2024).
- **Realistic, Real-Time Simulations:** Instead of using stale, easily recognizable templates, these platforms use generative AI to create highly realistic phishing simulations based on real-time threat intelligence feeds (Keepnet Labs 2024). This means employees are trained to recognize and respond to the actual attack types that are currently circulating in the wild, making the training far more relevant and effective. Leading platforms in this space, such as KnowBe4 and Hoxhunt, explicitly leverage AI to power their simulated phishing and training modules (Gartner n.d.; KnowBe4 n.d.).
- **Behavioral Science and Gamification:** To drive genuine and lasting behavior change, these

AI platforms incorporate principles from behavioral science and gamification (Keepnet Labs 2024). They provide instant feedback, track progress over time, and use interactive elements to keep users engaged. This adaptive learning model, which reinforces correct behaviors and provides targeted remediation for mistakes, has been shown to be far more effective at building security resilience than traditional, one-size-fits-all approaches (Keepnet Labs 2024).

To underscore the urgency of this new approach to training, Table 3 provides a quantitative snapshot of the current phishing threat landscape, drawing on recent data from 2024 and 2025.

Table.3. Quantitative Snapshot of the Phishing Threat Landscape (2024-2025)

Metric	Statistic	Source
AI vs. Human Efficacy	AI spear phishing agents are **24% more effective** than elite human red teams (as of March 2025).	(Hoxhunt 2025)
Click/Open Rates	**78%** of people open AI-generated phishing emails; **21%** click on malicious content inside.	(Tech Advisors 2025)
Success Rate Increase	Enterprise employees clicked phishing links at **3x the rate** in 2024 vs. 2023.	(Cyber Magazine 2025)
Organizational Impact	**96%** of organizations reported negative consequences from phishing in 2024.	(Mobile ID World 2025)
LLM Impact	**95%** of IT professionals say LLMs make identifying fraudulent communications more challenging.	(Mobile ID World 2025)
BEC Attack Increase	**1,760%** YoY increase in social engineering-based BEC attacks in 2023.	(Guardz 2024)

While AI-powered SAT represents a significant leap forward, it also gives rise to a "Training Paradox." On one hand, security teams are using AI to create increasingly realistic training simulations to educate their users (Keepnet Labs 2024). On the other hand, threat actors are using the same underlying technology to create phishing attacks that are superior to those made by human experts (Hoxhunt 2025). This creates a situation where we are in a perpetual race to train humans to detect a threat that is evolving at the speed of AI model development.

This raises a critical question: is there a limit to human detection capability? It is conceivable that AI-generated content will become so flawlessly contextual that no amount of training will allow a human to reliably distinguish it from legitimate content. This possibility suggests that while AI-powered SAT is the best tool available, a long-term strategy cannot rely on it as the final defense. It reinforces the need for robust technical safety nets and a new paradigm of **Cognitive Hygiene**. The ultimate goal may need to evolve from "spot the phish" to cultivating a zero-trust mindset where secure procedures are paramount, potentially augmented by technology that can interpret user intent and cognitive state directly, as illustrated in the following vignette:

> *An executive receives a hyper-realistic deepfake video call. The face on the screen is her CEO, the voice a perfect imitation, the request for an urgent wire transfer plausible. The request is flawless to the human eye and ear. However, the user's Mind-Machine Controller (MMC), constantly monitoring her neural state, detects a spike in cognitive load and amygdala activity inconsistent with a routine request. The MMC's AI core cross-references this anomaly with the incoming data stream, flagging the video's subtle, computationally-generated micro-artifacts. Before the executive can even voice a command to authorize the transfer, the MMC automatically severs the connection, quarantines the communication logs, and sends a high-priority, cryptographically signed alert to the Security Copilot in the SOC (Wong and Saade 2025). The attack is stopped not by human judgment, but by automated, intelligent cognitive hygiene.*

7. STRATEGIC IMPLEMENTATION AND PRACTICAL RECOMMENDATIONS

Translating the analysis of the AI-Hygiene Paradox into a resilient security posture requires a deliberate and strategic approach. Organizations must move beyond ad-hoc tool adoption and embrace a holistic framework for intelligent hygiene that spans from silicon to software to cognition. This section provides actionable guidance for CISOs, security leaders, and IT practitioners on how to implement these principles effectively.

7.1 ADOPTING AN "INTELLIGENT CYBER HYGIENE" FRAMEWORK

The foundational step is to shift the organizational mindset from a compliance-driven, checklist-based approach to a dynamic, risk-based model. Frameworks such as the NIST Cybersecurity Framework provide a valuable roadmap for structuring this effort, but they must be interpreted through the lens of AI-driven automation (ChannelPro Network 2025).

A practical implementation should prioritize automation of the basics to build a solid foundation (Help Net Security 2025). The first and most critical tasks to automate are those that are highly repeatable, prone to human error, and foundational to all other security controls. These include:

- **Asset Discovery:** Continuously and automatically discover all hardware and software assets across the enterprise (Help Net Security 2025).
- **Vulnerability Scanning:** Automate scanning to identify weaknesses in real time (ChannelPro Network 2025; Plain English 2025).
- **Patch Management:** Implement automated, risk-prioritized patching to close vulnerability windows quickly (ChannelPro Network 2025; Help Net Security 2025).
- **User Account Governance:** Automate the lifecycle of user accounts, ensuring access is

provisioned and de-provisioned in a timely manner tied to employment status (Help Net Security 2025).

Automating these foundational tasks frees up critical human resources to focus on higher-value strategic initiatives rather than manual, repetitive work (Help Net Security 2025; Secureframe n.d.). Following this, organizations should invest in advanced AI-powered platforms for core security functions, including Managed Extended Detection and Response (XDR) for unified threat visibility, SIEM and SOAR for intelligent analysis and automated response, and Data Loss Prevention (DLP) for automated data classification and protection (ChannelPro Network 2025).

7.2 THE ROLE OF THE AI SECURITY COPILOT

To maximize the effectiveness of security teams, organizations should actively integrate AI assistants, or "Security Copilots," into their Security Operations Centers (SOCs). Tools like Microsoft Security Copilot are designed to act as a force multiplier for overstretched security teams (Wong and Saade 2025). These copilots augment human analysts by automating the initial, time-consuming phases of an investigation. They can triage and summarize thousands of alerts, correlate disparate events into a single incident narrative, hunt for related indicators of compromise across the network, and provide analysts with guided remediation plans. This human-AI teaming model allows senior analysts to focus their expertise on the most complex and novel threats, dramatically improving the efficiency and efficacy of the entire security operation (Cynet 2025; Secureframe n.d.).

7.3 DEVELOPING AI GOVERNANCE AND USAGE POLICIES

To combat the growing problem of "hygiene debt," organizations must move swiftly to establish clear, enforceable governance over the use of public AI tools. It is no longer sufficient to offer vague guidance like "use your best judgment." Instead, organizations need to develop and disseminate formal, written policies that explicitly define the acceptable use of AI (TNTMAX 2025).

These policies should, at a minimum:

- **Explicitly Forbid Sensitive Data Input:** Prohibit employees from pasting any form of confidential or sensitive information—including PII, financial data, client information, proprietary source code, or internal strategy documents—into any public or non-company-approved AI platform (TNTMAX 2025).
- **Provide Approved Alternatives:** Do not simply forbid the use of public tools; provide employees with company-sanctioned, secure AI platforms that have been vetted by the security team.
- **Mandate Safe Configurations:** Train employees on the safe usage of these tools, including how to proactively disable settings like chat history and model training to prevent their data from being used by the third-party provider (TNTMAX 2025).

7.4 A GEORGIAN CONTEXT: APPLYING INTELLIGENT HYGIENE TO NATIONAL PRIORITIES

For Georgia, the principles of intelligent hygiene are not just best practices; they are a strategic imperative. The country's National Cybersecurity Strategy (2021-2024) emphasizes fostering a cybersecurity culture, enhancing public-private partnerships, and developing national cyber capabilities—all goals that can be accelerated by AI-driven automation (Digital Watch Observatory 2021a; PMCG n.d.). The strategy's focus on digital hygiene initiatives aligns perfectly with the need to automate foundational controls to build a resilient baseline (Digital Watch Observatory 2021b).

However, Georgia faces unique challenges, including a scarcity of cybersecurity professionals, inconsistent institutional coordination, and a complex geopolitical environment that includes persistent threats from the

Russian Federation (Binding Hook 2024; GCSCC n.d.; VOA News 2024). Recent events, such as the 2024-2025 protests and alleged strains on Western partnerships, could further limit resources (Binding Hook 2024; Wikipedia n.d.). In this context, leveraging AI-powered security automation is a force multiplier. It allows a limited number of human experts to manage a vast and complex threat landscape, making the nation's defense more efficient and scalable.

Furthermore, as the Georgian government itself promotes AI innovation through the Georgia Technology Authority (GTA), it is critical to build this adoption on a secure foundation (GTA 2025). The development of a national AI strategy, as recommended by researchers, must be deeply integrated with cybersecurity principles to avoid creating new vulnerabilities (PMC Research 2022). The country's low ranking on the Global Index on Responsible AI (60th) underscores the urgent need for robust governance frameworks that address the security and ethical risks of AI from the outset (IDFI 2024).

7.5 BUSINESS OPPORTUNITY FOR MANAGED SERVICE PROVIDERS (MSPS)

The complexity and resource requirements of building an intelligent hygiene program create a significant business opportunity for Managed Security Service Providers (MSSPs) and Managed Service Providers (MSPs). Many small and mid-sized businesses (SMBs) lack the in-house expertise and capital to deploy and manage these advanced AI-driven systems. MSPs can fill this gap by offering "Intelligent Hygiene as a Service" (ChannelPro Network 2025).

This service portfolio can generate recurring revenue and attract new clients by offering a range of capabilities, including:

- In-depth security and readiness assessments.
- Managed XDR and 24/7 SOC-as-a-Service.
- Automated patch and vulnerability management.
- Recurring, AI-powered security awareness training and phishing simulations.
- Compliance consulting and virtual CISO (vCISO) services (ChannelPro Network 2025).

By providing these services, MSPs can help resource-constrained businesses protect themselves from AI-enabled threats and ensure the success of their broader digital transformation initiatives (ChannelPro Network 2025).

8. CONCLUSION AND FUTURE OUTLOOK

The analysis presented in this paper confirms that Artificial Intelligence is the definitive dual-use technology of our time in the domain of cybersecurity. Its rapid weaponization by malicious actors has rendered legacy hygiene practices, built on manual processes and static defenses, dangerously inadequate (VE3 Global 2025). The central conclusion of this research is that the defensive adoption of AI is no longer an optional strategy but a direct and urgent necessity. Navigating the AI-Hygiene Paradox—where the threat and the solution are derived from the same technological source—is the principal challenge facing security practitioners today. This paradox is not limited to software but extends across the entire technological stack, from the integrity of the silicon supply chain to the emerging frontier of human cognition.

The conflict between offensive and defensive AI should be understood as a continuously escalating arms race with no clear endpoint. As underlying AI models become more powerful and accessible, both attack and defense capabilities will grow in sophistication in a perpetual cycle of innovation and counter-innovation. This dynamic suggests that a final, decisive victory for either side is unlikely. Instead, resilience will be defined by an organization's ability to adapt and maintain a defensive posture that evolves at the same pace as the threat landscape.

Looking ahead, several emerging frontiers are poised to define the next phase of this conflict:

- **Agentic Warfare:** The current era of AI-driven automation will likely evolve into one of "agentic warfare." This involves autonomous AI agents capable of executing complex, multi-step cyber operations with minimal human oversight. These agents will not just automate simple tasks but will conduct research, plan attack paths, and adapt their TTPs in real time, presenting a challenge of unprecedented speed and complexity for defenders (Wong and Saade 2025).

- **Explainable AI (XAI):** As more critical security decisions are delegated to AI systems, the need for transparency and interpretability will become paramount. Black-box AI models, whose reasoning is opaque to human operators, will pose significant challenges for auditing and trust. The development of XAI, which aims to make AI decision-making understandable to humans, will be critical for enabling effective human oversight and ensuring that automated defenses operate as intended (Path of Science 2024).
- **Securing the Full Supply Chain:** The strategic focus of cybersecurity will continue to shift from protecting traditional IT assets to securing the entire technology lifecycle. This includes protecting AI models and data pipelines from poisoning and evasion attacks (Treasury Department n.d.; VE3 Global 2025), as well as ensuring the integrity of the underlying hardware through robust defenses against deobfuscation and other supply-chain compromises.
- **The Cognitive Frontier:** The advent of Mind-Machine Controllers (MMCs) and other neuro-technologies represents the ultimate endpoint of the AI-Hygiene Paradox, where the human nervous system itself becomes part of the attack surface. This will necessitate a new discipline of "cognitive hygiene," built on principles of zero-trust biometrics, cryptographically secure neural data transmission, and robust ethical governance to protect user agency and intent.

In conclusion, the path forward demands a strategic and wholehearted embrace of AI-driven automation, coupled with a fundamental redefinition of the human's role in the security ecosystem. The future security professional will not be a manual operator of tools but an augmented strategist, orchestrating a fleet of intelligent systems and applying human intellect to the most complex challenges. For a nation like Georgia, which has long been on the front lines of state-sponsored cyber conflict, successfully navigating the AI-Hygiene Paradox across software, hardware, and cognition is not just a technical goal—it is essential for preserving its national security and digital sovereignty (Tkeshelashvili 2025).

REFERENCES

1. Abnormal AI. 2024. "Phishing 2024 Guide: Stats and Prevention Tips." Abnormal AI. https://abnormal.ai/phishing.
2. Binding Hook. 2024. "From Ally to Outcast, What's Next for Georgia's Cyber Future?" *Binding Hook*, December 24, 2024. https://bindinghook.com/articles-binding-edge/from-ally-to-outcast-whats-next-for-georgias-cyber-future/.
3. ChannelPro Network. 2025. "Cyber Hygiene + AI = Opportunity." *ChannelPro Network*. Last modified March 31, 2025. https://www.channelpronetwork.com/2025/03/31/cyber-hygiene-ai-opportunity/.
4. Civil.ge. 2025a. "Georgian Population Allegedly Exposed in a Massive Personal Data Leak." *Civil.ge*, January 25, 2025. https://civil.ge/archives/655994.
5. Civil.ge. 2025b. "Tbilisi Public Transport Allegedly Hacked, Pro-European Messages Played on Payment Machines." *Civil.ge*, January 24, 2025. https://civil.ge/archives/655517.
6. Cyber Magazine. 2025. "Netskope Data Shows Phishing Success Rate Tripled in 2024." *Cyber Magazine*, January 7, 2025. https://cybermagazine.com/articles/netskope-data-shows-phishing-success-rate-tripled-in-2024.
7. Cybernews. 2024. "Entire Georgian Country Population Exposed in a Massive Data Leak." *Cybernews*, October 7, 2024. https://cybernews.com/security/entire-georgian-country-population-exposed/.
8. Cynet. 2025. "AI in Cybersecurity: Use Cases, Challenges, and Best Practices." *Cynet*. Last modified April 26, 2025. https://www.cynet.com/cybersecurity/ai-in-cybersecurity-use-cases-challenges-and-best-practices/.
9. Digital Watch Observatory. 2021a. "National Cybersecurity Strategy and Action Plan for 2021-2024 for Georgia." *dig.watch*. Last modified October 2021. https://dig.watch/resource/national-cybersecurity-strategy-and-action-plan-for-2021-2024-for-georgia.
10. Digital Watch Observatory. 2021b. "National Cybersecurity Strategy of Georgia for 2021-2024 and its Action Plan." *dig.watch*. Last modified September 30, 2021. https://dig.watch/resource/national-cybersecurity-strategy-of-georgia-for-2021-2024-and-its-action-plan.

11. ECI. 2025. “Cyber Hygiene and Compliance in the Age of AI.” *ECI*. https://www.eci.com/blog/cyber-hygiene-and-compliance-age-ai.
12. Gartner. n.d. “Security Awareness Computer-Based Training Reviews.” Accessed July 27, 2025. https://www.gartner.com/reviews/market/security-awareness-computer-based-training.
13. GCSCC (Global Centre for Cybersecurity Capacity). n.d. “Georgia.” *gcscc.ox.ac.uk*. Accessed July 27, 2025. https://gcscc.ox.ac.uk/georgia.
14. GTA (Georgia Technology Authority). 2025. “Georgia FY 2024 Annual State IT Report highlights AI, innovation.” *gta.georgia.gov*, February 13, 2025. https://gta.georgia.gov/news/2025-02-13/georgia-fy-2024-annual-state-it-report-highlights-ai-innovation.
15. Guardz. 2024. “33 Phishing Attack Statistics in 2024 Every MSP Should Know About.” *Guardz.com*. https://guardz.com/blog/33-phishing-attack-statistics-in-2024-every-msp-should-know-about/.
16. Help Net Security. 2025. “What's worth automating in cyber hygiene, and what's not.” *Help Net Security*, April 29, 2025. https://www.helpnetsecurity.com/2025/04/29/automating-cyber-hygiene/.
17. Hoxhunt. 2025. “AI-Powered Phishing Outperforms Elite Red Teams in 2025.” *Hoxhunt*. https://hoxhunt.com/blog/ai-powered-phishing-vs-humans.
18. IDFI (Institute for Development of Freedom of Information). 2024. “Global Index on Responsible AI and Georgia's Results.” *idfi.ge*, May 22, 2024. https://idfi.ge/en/global_center_on_ai_governance_2024.
19. IEEE Transmitter. 2023. “Is basic cyber hygiene enough in the age of AI?” *IEEE Transmitter*, August 24, 2023. https://transmitter.ieee.org/is-basic-cyber-hygiene-enough-in-the-age-of-ai/.
20. Keepnet Labs. 2024. “How AI Will Transform Security Awareness Training.” *Keepnet Labs*. Last modified November 29, 2024. https://keepnetlabs.com/blog/how-ai-will-transform-security-awareness-training.
21. KnowBe4. n.d. “Security Awareness Training.” Accessed July 27, 2025. https://www.knowbe4.com/products/security-awareness-training.
22. Metomic. n.d. “How to Automate Cyber Hygiene in Your Business.” *metomic.io*. Accessed July 27, 2025. https://www.metomic.io/resource-centre/how-to-automate-cyber-hygiene-in-your-business.
23. Microsoft. n.d.a. “Security for AI.” Accessed July 27, 2025. https://www.microsoft.com/en-us/security/business/solutions/security-for-ai.
24. Microsoft. n.d.b. “Cybersecurity Awareness.” Accessed July 27, 2025. https://www.microsoft.com/en-us/security/business/cybersecurity-awareness.
25. Mobile ID World. 2025. “AI-Powered Phishing Attacks Surge in 2024, with 96% of Organizations Impacted.” *Mobile ID World*, January 8, 2025. https://mobileidworld.com/ai-powered-phishing-attacks-surge-in-2024-with-96-of-organizations-impacted/.
26. Morgan Stanley. n.d. “AI and Cybersecurity: A New Era.” Accessed July 27, 2025. https://www.morganstanley.com/articles/ai-cybersecurity-new-era.
27. Path of Science. 2024. “AI-Powered Phishing Detection and Prevention: A Comprehensive Review.” *Path of Science* 10, no. 12. https://pathofscience.org/index.php/ps/article/download/3406/1623.
28. Plain English. 2025. “AI-Powered Cyber Hygiene: Automating Routine Security for Stronger Defense.” *AI in Plain English*, February 13, 2025. https://ai.plainenglish.io/ai-powered-cyber-hygiene-automating-routine-security-for-stronger-defense-065957dc62eb.
29. PMC Research. 2022. “Sharing the Results of Our Research on Georgia’s Artificial Intelligence (AI) Readiness.” *pmcresearch.org*, March 17, 2022.(https://www.pmcresearch.org/news_show/130/Sharing-the-Results-of-Our-Research-on-Georgia%E2%80%99s-Artificial-Intelligence-(AI)-Readiness).
30. PMCG. n.d. “Georgia Cyber Security Programme.” *pmcg-i.com*. Accessed July 27, 2025. https://pmcg-i.com/project/georgia-cyber-security-programme/.
31. Roxiler. 2025. “Phishing Detection AI: How Artificial Intelligence is Changing the Game in Email Security.” *Roxiler*. Last modified June 3, 2025. https://roxiler.com/insights/blogs/phishing-detection-ai-how-artificial-intelligence-is-changing-the-game-in-email-security/.
32. SCSA (Scientific Cyber Security Association). n.d. “Scientific and practical cyber security journal.” Accessed July 27, 2025. https://journal.scsa.ge/.
33. Secureframe. n.d. “AI in Cybersecurity: Benefits, Use Cases, and Challenges.” *secureframe.com*. Accessed July 27, 2025. https://secureframe.com/blog/ai-in-cybersecurity.
34. Shepherd Insurance. 2024. “The Rise of AI-Driven Cyber Threats.” *Shepherd Insurance*. Last modified October 24, 2024. https://www.shepherdins.com/the-rise-of-ai-driven-cyber-threats/.
35. Tech Advisors. 2025. “AI Cyber Attack Statistics 2025: Phishing, Deepfakes & Cybercrime Trends.” *Tech*

Advisors, May 27, 2025. https://tech-adv.com/blog/ai-cyber-attack-statistics/.

36. Tkeshelashvili, Eka. 2025. “Georgia's Cybersecurity Environment in the AI Era.” *Eastern Europe Regional Studies*. https://psage.tsu.ge/index.php/Easternstudies/article/view/361.
37. TNTMAX. 2025. “Cyber Hygiene for AI Tools: What Employees Need to Know in 2025.” *TNTMAX*. https://tntmax.com/cyber-hygiene-for-ai-tools-what-employees-need-to-know-in-2025/.
38. Treasury Department. n.d. “Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector.” *home.treasury.gov*. Accessed July 27, 2025.(https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf).
39. VE3 Global. 2025. “The Importance of Cyber Hygiene in the era of AI.” *VE3*. Last modified May 14, 2025. https://www.ve3.global/the-importance-of-cyber-hygiene-in-the-era-of-ai/.
40. VOA News. 2024. “Experts: Russia's Hacking Campaign Seeks to Thwart Georgia's Westward Path.” *VOA News*, October 25, 2024. https://www.voanews.com/a/experts-russia-s-hacking-campaign-seeks-to-thwart-georgia-s-westward-path-/7839572.html.
41. Wikipedia. n.d. “2024–2025 Georgian protests.” Accessed July 27, 2025. https://en.wikipedia.org/wiki/2024%E2%80%932025_Georgian_protests.
42. Wong, Haiman, and Tiffany Saade. 2025. “The Rise of AI Agents: Anticipating Cybersecurity Opportunities, Risks, and the Next Frontier.” *R Street*, May 29, 2025. https://www.rstreet.org/research/the-rise-of-ai-agents-anticipating-cybersecurity-opportunities-risks-and-the-next-frontier/.