SANS

From Asymmetry to Parity: Building a Safe Harbor for AI-Driven Cyber Defense

Expanded Insights from the SANS Keynote at RSAC 2025 Conference

White Paper Series, Volume 2 of 4

By **Rob T. Lee**
SANS Chief AI Officer and
Chief of Research

October 2025



sans.org

©2025 SANS™ Institute

Introduction

AI serves as both an asset and a threat in cybersecurity. AI tools deliver faster threat detection, automated responses, and stronger infrastructure protection. However, privacy rules and AI laws limit firms' data and AI use. Attackers face no such limits. This paper analyzes limits on AI cyber defense. It covers the European Union's (EU's) General Data Protection Regulation (GDPR) and AI Act, the US California Consumer Privacy Act/ California Privacy Rights Act (CCPA/CPRA), guidelines, and research.

We highlight 13 key issues:

- **Strict data privacy rules in the EU—**The GDPR permits data processing for cybersecurity (Recital 49), but only if necessary. The EU AI Act labels most defensive AI, like spam filters, low-risk and exempt. High-risk systems demand compliance. The GDPR's minimization and transfer rules block European firms from using personal data in detection and response.
- **US legal advantages for cyber defense—**The United States lacks a unified privacy law but includes cybersecurity exemptions in statutes. The CCPA allows the use of personal data for detection and fraud prevention, which exepts organizations from some restrictions.[1] CISA 2015 created sharing protections via the Department of Homeland Security's Automated Indicator program. When a firm follows the protocols for data removal, they gain liability immunity.[2] This gives US firms more AI freedom for phishing, intrusion, and data defense than EU ones. White House directives and National Institute of Standards and Technology (NIST) frameworks promote voluntary responsible AI practices, which demonstrate that privacy and ethical concerns must always be considered, even without formal legal requirements.
- **Divergent regimes burden global companies—**Multinational enterprises need to handle multiple conflicting laws, which leads them to implement the strictest standard (GDPR) worldwide to prevent compliance gaps. Privacy and AI rules delay innovation for 77% of CISOs.[3] Security organizations perform legal assessments before utilizing particular data or AI systems, which causes delays for both incident response operations and international threat

[1] https://oag.ca.gov/privacy/ccpa

[2] "Automated Indicator Sharing (AIS) Participant Protections," Cybersecurity and Infrastructure Security Agency, www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais/automated-indicator-sharing-ais-participant-protections

[3] "AI Cybersecurity Regulations: What CISOs Need to Know," April 2025, www.zscaler.com/cxorevolutionaries/insights/ai-cybersecurity-regulations-what-cisos-need-know

assessment. Security teams face difficulties with EU user data investigations because GDPR prohibits unsecured transfers of personal logs across borders. This forces investigators to obtain legal approval or perform data anonymization during emergency situations. The implementation of GDPR led domain registrars to hide registrant information from WHOIS data, which investigators used to identify malicious domains connected to criminal actors. IBM Security specialists stated that the absence of WHOIS—now known as Registration Directory Service (RDS)—data would extend malicious domain cluster detection time beyond 30 days, making defenders defenseless against attackers during that period.[4] Organizations operating across multiple jurisdictions encounter specific challenges in their cybersecurity readiness because of well-meaning regulations.

- **Phishing and malware detection—**AI-powered email filters and web scanners must analyze message content alongside URLs and sender information to identify phishing attempts. These systems automatically process personal data when they evaluate emails, texts, and names. According to GDPR and EU ePrivacy rules, organizations can lawfully process content when the purpose is strictly security-related. Companies need to anonymize or remove personal information from emails before storage because strict data retention limits may affect detection performance. Cloud-based email security providers encounter additional obstacles when performing EU data scans from outside EU cloud systems due to established data transfer regulations.
- **Incident response and forensics—**AI assistants analyze system logs, network traffic, and disk images during security breach investigations. These normally include user identifiers as well as communication data and personal information. Breach forensic analysis must follow privacy laws, analyzing only the data related to the security incident.[5] The analysis requires removing unnecessary personal data from the results while preventing any additional uses beyond breach mitigation. Teams that handle cross-border incidents must establish procedures to stop illegal EU log exports to US analysis tools. The investigation process can become delayed because responders require legal permission and data handling agreements before AI analysis of pooled data, even when the attack is active.

[4] "GDPR impact on Whois data raising concern," Computer Weekly, May 2018, www.computerweekly.com/news/252441275/GDPR-impact-on-Whois-data-raising-concern

[5] "Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data," 2018, www.whiteandwilliams.com/assets/htmldocuments/Threat%20Information%20Sharing%20and%20GDPR_FS-ISAC%20Branded_1.2.19_Final_TLP%20WHITE.pdf

- **Threat intelligence sharing—**The fundamental base of collaborative cyber defense relies on organizations sharing threat indicators, including malicious IP addresses, file hashes, and attacker tactics, techniques, and procedures (TTPs). Threat indicators that consist of IP addresses or email addresses qualify as personal data, according to privacy laws. According to the GDPR, organizations can share security-related data as part of their legitimate network security interests, while Recital 49 specifically approves this practice for cyberattack prevention. Organizations need to handle shared indicators exclusively for defense purposes after removing victim-identifying information. Organizations tend to choose cautious data sharing approaches that involve bilateral lawyer-reviewed agreements over participating in real-time industry exchanges because of privacy concerns. The EU's NIS2 Directive recognizes this issue by requiring member states to support the creation of cyber threat information-sharing communities.[6] Unclear protections require caution. Delays hit AI feeds.
- **Supply chain risk monitoring—**AI scans open data for signs of compromise and leaks pre-attack. The process of data compilation includes personal information such as employee names found in leaks. Under the GDPR, a business using AI to monitor suppliers would likely violate the privacy rights of third-party organizations because it processes personal data without consent or proper authority. The organization requires a strong legal foundation to proceed and might need to disclose the information to both the individuals and partners, but this process is not feasible. Organizations avoid extensive monitoring because they understand that uniting detailed partner network data risks violating privacy regulations.
- **WHOIS data restrictions—**Domain registrars have had to hide registrant information in WHOIS databases because of GDPR regulations. Thus, security teams cannot immediately identify criminal actors. Attackers prolong their stay while security teams attempt to respond. The lack of visibility in threat hunting creates blind spots for defenders.[7]

[6] "The NIS 2 Directive, Final Text," www.nis-2-directive.com/NIS_2_Directive_Article_29.html

[7] "Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World," February 2024, https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

- **Purpose limitation barriers—**GDPR Article 5 establishes barriers that prevent data from being used for new threat detection purposes. AI systems detect new attack patterns but then stop because the data collection purpose does not match. Organizations need to find legal authorization or perform fresh anonymization before being able to respond. The risks associated with health data repurposing for insurance pricing demonstrate similar threats in cybersecurity scenarios. However, attackers use stolen data without any restrictions.
- **Automated decision oversight—**The GDPR requires human oversight for AI decisions that have significant effects. For example, the AI system requires human supervision to perform threat isolation in cyber defense operations, increasing the time it takes to contain breaches from seconds to minutes. The explainability challenges become more complex because opaque machine learning (ML) models cannot be easily reverse engineered. The defenders experience delays while threats continue to move at a faster pace.
- **Right to erasure impacts—**Users erase data under GDPR Article 17, disrupting AI training sets. Key logs vanish from anomaly detection models. Insider threats slip through weakened patterns. The risks of maintaining robust datasets become evident through re-identification cases such as the connection between Netflix data and IMDb. Models thus need to be rebuilt constantly.

Challenges of Using AI for Cyber Defense

Legal Frameworks

Consider contrasting laws and their implications:

- **Strict data privacy rules in the EU**
  GDPR restricts processing, transfer, and high-risk AI, limiting defensive uses.
- **US legal advantages for cyber defense**
  Cyber exemptions, liability protections, and voluntary frameworks give US firms more AI freedom.
- **Divergent regimes burden global companies**
  Multinationals adopt strictest standards (GDPR), slowing innovation and cross-border defense.

Operational Challenges

Regulations can complicate day-to-day security operations:

- **Phishing and malware detection**
  AI filters process personal data but must anonymize and follow strict transfer rules.
- **Incident response and forensics**
  AI analysis is slowed by legal approvals, especially for cross-border cases.
- **Threat intelligence sharing**
  Personal data concerns create delays, replacing fast exchanges with lawyer-reviewed agreements.
- **Supply chain risk monitoring**
  AI scans risk violating GDPR when personal or partner data is included, discouraging adoption.
- **WHOIS data restrictions**
  Hidden registrant data weakens threat hunting, leaving attackers hidden longer.

AI Limitations Under GDPR

Understand how core AI functions are directly affected:

- **Purpose limitation barriers**
  Data can't be reused for new threats without fresh authorization or anonymization.
- **Automated decision oversight**
  Human review of AI containment delays responses and adds explainability challenges.
- **Right to erasure impacts**
  Data deletion disrupts AI training sets, weakening anomaly detection and forcing retraining.
- **Data fragmentation in the EU**
  Lack of cross-border datasets limits collective defense and slows intelligence sharing.
- **Data misuse precedents**
  Scandals like Cambridge Analytica show risks of misuse, but GDPR penalties also restrict defenders.

- **Data fragmentation in the EU—**The Draghi report identifies GDPR as a cause of data fragmentation that hinders the creation of extensive AI datasets.[8] EU firms experience reduced threat intelligence capabilities because of their inability to transfer data freely. The inability to conduct cross-border analysis creates delays in the development of collective defense strategies. Defenders compete with one hand tied behind their back.
- **Data misuse precedents—**The Cambridge Analytica scandal involved using Facebook data to create AI profiles that affected election outcomes. The same risks of data misuse exist in cyber defense operations because of GDPR regulations. The ability to profile threats becomes restricted by consent requirements, yet attackers continue their activities. Defenders face significant financial penalties from these fines.[9]

These examples demonstrate that defensive AI requires design-based privacy engineering through user ID hashing and anonymization techniques alongside data analysis in local systems and post-threat data elimination practices. Security analytics *lose their fidelity through these protective measures, which also decrease the speed at which AI-driven defensive systems respond*. Security teams face additional challenges when performing compliance procedures that include documenting AI model data usage and conducting data protection impact assessments and obtaining managerial approvals. Experimental ML models must complete their approval process *after attackers may have already developed new attack methods*, which reduces the defender's strategic advantage.

[8] "The future of European competitiveness (Draghi Report)," September 2024, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[9] "Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World," February 2024, https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

Asymmetry: Unregulated Attackers vs. Regulated Defenders

AI boosts attackers but limits defenders. Outlaw actors use data and tools freely. No law or ethics binds them.

The main security problem in cyber defense stems from the increasing difference between the capabilities that AI provides to attackers and the limitations imposed on defenders. Threat actors who operate outside the law have complete freedom to utilize any available data and tools because they face no restrictions from data protection laws or ethical AI guidelines. Cybercriminal groups started employing home-built "rogue" AI chatbots like WormGPT and FraudGPT in 2023. These black-market versions of large language models (developed from open-source GPT-J) function without safety measures because they are marketed specifically for unlawful activities.[10] The unauthorized AIs generate spear-phishing emails, malicious code, and even full attack guides on demand. The EU police agency Europol warns that the scale-based text generation of ChatGPT enables criminals to use it effectively for phishing attacks and propaganda activities.[11] The ability of ChatGPT to produce fluent text at scale allows attackers to easily create malicious code and automate their cybercrime operations.[12] AI technology makes it easier for cybercriminals to perform complex phishing and malware attacks through its "expertise," which bad actors do not possess.

Advanced adversaries, including nation-states, utilize stolen personal datasets to enhance their targeting capabilities (defenders cannot do this without violating privacy regulations) and operate AI agents that conduct real-time attack adaptations. This creates an unbalanced security environment because attackers enjoy unrestricted AI development along with large-scale data collection, while defenders must operate under legal and ethical restrictions when implementing AI systems and threat information sharing. Security teams face GDPR violations or lawsuits when using AI to analyze employee emails; attackers do not face such restrictions when using stolen emails to develop personalized scams. The current unbalanced regulations may create a safer environment for attackers to operate in than for defenders who seek to protect themselves against attacks.

---

[10] "Open source, open risks: The growing dangers of unregulated generative AI," IBM, June 2024, www.ibm.com/think/insights/unregulated-generative-ai-dangers-open-source

[11] "Europol sounds alarm about criminal use of ChatGPT, sees grim outlook," March 2023, www.reuters.com/technology/europol-sounds-alarm-about-criminal-use-chatgpt-sees-grim-outlook-2023-03-27/

[12] "Europol sounds alarm about criminal use of ChatGPT, sees grim outlook"

Policy Solution: A Cybersecurity Safe Harbor

The concept of a cybersecurity exception as a safe harbor is gaining momentum among experts as a way to balance AI use and privacy regulations. This legal exception would establish explicit permission for organizations to use personal data with AI systems for cybersecurity needs that follow strict protective measures. The initiative maintains general privacy rights while creating a legal path for defenders to stop breaches, fraud, and other threats without unnecessary barriers. A well-crafted cybersecurity exception could include:



- **Protected threat intelligence sharing—** The exchange of cyber threat indicators among companies and computer emergency readiness teams/information sharing and analysis centers (CERTs/ISACs) should remain protected under privacy laws so they can share attacker IPs along with malicious URLs, hash values, and phishing email headers. The permission of defense activities for information sharing would enable defenders to share threat data through their AI detection systems in real time while using global threat intelligence. The implementation of appropriate safeguards, including the Traffic Light Protocol for sensitivity and victim data anonymization and restricted access to vetted partners, would protect data from misuse. The EU's NIS2 Directive supports voluntary cyber information-sharing arrangements among companies because it recognizes their ability to enhance collective security.[13] A safe harbor policy would enhance data sharing by clearing up the existing confusion that stops companies from exchanging information.

[13] "The NIS 2 Directive, Final Text," www.nis-2-directive.com/NIS_2_Directive_Article_29.html

- **Privacy-preserved defensive analytics—**Organizations can process personal data through AI for security incident detection, prevention, and response if they establish strong privacy protection measures. An enterprise can allow its security operations center (SOC) to use AI for network traffic and user account behavior monitoring to detect compromises through pattern analysis of login locations and email content, as long as personal data remains protected within the security function. The legal framework would demand organizations adopt pseudonymization (user IDs instead of names) and encryption of sensitive fields and access controls, as well as data destruction after completing security tasks. The legal framework would protect the fundamental rights of individuals while preventing any nonsecurity purpose use of data processed under this exception. The rules of the US Department of Homeland Security Automated Indicator Sharing (AIS) program establish guidelines for companies to share indicators with personal information removed when necessary. Data must be kept for only as long as needed to address threats and used exclusively for network defense.[14] A legal safe harbor with established privacy-preserving requirements would enable companies to implement advanced AI defense systems (such as user behavior analytics for insider threat detection) because they would understand the legal boundaries as long as they follow the specified guardrails.
- **Emergency response flexibility—**Fast-moving cyber incidents like ransomware outbreaks demand immediate action, yet organizations need to consider compliance issues when they want to send EU office log data to their US incident response AI system. A cybersecurity exception would feature an emergency clause that lets organizations bypass specific restrictions when actively fighting cyberattacks to achieve quick containment. Organizations have the right to move and analyze data across borders and implement new AI tools on sensitive information without approval during active attacks when such actions protect against higher risks of harm. Afterward, the incident teams should maintain logs of these activities and submit them to regulators as part of their reporting. Some privacy laws enable restricted data usage during emergencies, and law enforcement agencies can bypass regular procedures during urgent situations. The legal process should not interfere with immediate defensive operations because defenders should not face delays for legal opinions while an attack continues. The emergency safe harbor system ensures that stopping the breach takes precedence while maintaining proper oversight after the incident.

---

[14] "Automated Indicator Sharing (AIS) Participant Protections," CISA, www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais/automated-indicator-sharing-ais-participant-protections

[15] "Automated Indicator Sharing (AIS) Participant Protections," CISA, www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais/automated-indicator-sharing-ais-participant-protections

- **Facilitation of collaborative defense AI—**A safe harbor would allow organizations to establish AI-based security measures through collaborative efforts because no single entity possesses complete knowledge of threats. The safe harbor framework should establish explicit rules for organizations to work together on developing AI models for cybersecurity purposes. The process of creating ML models to detect attacks becomes possible when companies from multiple sectors combine anonymized threat data; current privacy and liability restrictions prevent this collaboration. An exception should enable industries or public–private partnerships to build collective "defense AI" solutions that would feature a financial sector model trained by fraud attempts across multiple banks. Small businesses need access to AI models that process datasets that exceed their individual capacities. The present data sharing restrictions between companies remain in place because organizations avoid potential violations of privacy or confidentiality rules. Under this safe harbor, participants who follow a certified code of conduct can guarantee their protection when using data for security purposes with appropriate anonymization methods. Security AI defenses would become accessible across the board instead of existing in isolated pockets of capability.
- **Liability protections for defensive measures—**Protections from liability for defensive measures serve the same important purpose as obtaining permission does. The safe harbor must establish a protection system that grants immunity to entities performing cybersecurity defense in good faith and staying within defined boundaries of defense activities. CISA 2015 in the United States grants companies liability protection when they share threat data according to its specified requirements. The GDPR enables regulatory sandboxing and code of conduct creation for protecting both innovation and compliance. A formal cyber defense exception would establish an oversight process that requires organizations to register or follow an approved "cybersecurity data use" code for automatic compliance. The paradigm shift establishes a clear legal framework for defenders who use data to secure systems, as long as they operate within established boundaries. The system contains built-in protective measures to stop improper usage through operations conducted under the exception, which must remain specific to security needs and be proportional to threats and subject to audit. The regulatory body maintains the power to review organizations that use "cybersecurity" as a cover for extensive employee surveillance. Under this approach, the law would shift from its current restrictive stance to a supportive one that acknowledges cyber defense as a vital public interest.

The "security data corridor" concept establishes a controlled area that allows personal information to enter AI defense systems and threat intelligence to move between peers while being monitored. The goal is to eliminate the unfair advantage attackers currently enjoy when using data and AI systems freely.

The implementation of a carefully managed safe harbor enables cyber defenders to use AI effectively in their defense while privacy regulators enforce compliance with established guidelines.

The proposed solution gives specific relief that enables crucial security operations without compromising transparency and accountability. The proposed cybersecurity exception provides a solution to resolve privacy–security conflicts during the AI era by allowing defenders to use advanced tools for intelligence sharing while upholding responsible practices. Both sides of the Atlantic are currently studying this concept because it presents a solution to address the existing legal framework problems that inadvertently restrict those who protect citizens.

Recommendations and Next Steps

Achieving the right balance will require action from lawmakers, regulators, and industry. Key recommendations include:



Enacting clear cybersecurity exceptions in law—Legislatures need to modify privacy laws and upcoming AI regulations by establishing specific exceptions for cybersecurity purposes. The United States should establish a "defense of networks and threat prevention" exception in its future national privacy law, because this provision holds bipartisan support. Congress needs to extend CISA 2015 threat sharing liability protections before they expire, so they can maintain their role in encouraging collaboration.[16] Lawmakers and member states should use the GDPR's Recital 49 to create an exception for information system security data processing within the operative articles and upcoming privacy regulation of the EU. The EU should create a limited cybersecurity exemption that applies to all digital legislation while ensuring AI applications for recognized security purposes stay outside restricted areas.

[16] "The Clock's Ticking: Why CISA 2015 Must Be Renewed Now," June 2025, www.centerforcybersecuritypolicy.org/insights-and-research/the-clocks-ticking-why-cisa-2015-must-be-renewed-now



Regulatory guidance and sandboxes—Regulatory bodies that combine cybersecurity agencies with data protection authorities must create joint guidance that explains how security-focused interpretations of existing laws should be applied. The European Data Protection Board should create guidance to show companies how they can use "legitimate interests" for threat intelligence sharing under GDPR regulations. The White House, together with the US Federal Trade Commission, should provide explanations about how standard network defense operations do not qualify as unfair privacy violations. Both regulatory bodies need to increase their use of regulatory sandboxes for AI in cybersecurity, as mentioned in the EU AI Act.[17] Through these sandboxes, supervised companies gain permission to test new AI-based defensive methods while developing enhanced privacy safeguards simultaneously. The knowledge gained during these operations will help establish permanent regulations or certification frameworks to establish cybersecurity exceptions.



Industry self-regulation and standards—The industry should have coalitions (such as ISACs and standards bodies) work together to establish codes of conduct and technical standards for AI security operations. The guidelines should outline the most effective methods for data anonymization, data handling, and oversight of defensive AI training processes that involve personal data. An organization should create a privacy-compliant protocol for email threat sample distribution that protects user identities but keeps threat patterns intact. Such codes, which regulators would approve, can establish the criteria for organizations to receive safe harbor status. AI security control guidelines developed by the Institute of Electrical and Electronics Engineers (IEEE) and SANS need to integrate data governance controls that protect privacy rights while maintaining effective defensive capabilities. According to the SANS Critical AI Security Guidelines, not implementing AI for security and privacy reasons represents a major security threat.[18] The industry needs to actively show that defensive AI implementations can operate within controlled parameters.

[17] "The EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act," https://artificialintelligenceact.eu

[18] "Critical AI Security Guidelines," www.sans.org/mlp/critical-ai-security-guidelines

Transatlantic cooperation—The United States and EU should work together to create compatible security solutions, because cyber threats operate across borders worldwide. Security operations should receive unique attention according to the mutual understanding of both parties. The two parties should create a collaborative group to determine the definition of a "cybersecurity exception," which would enable US companies to help EU subsidiaries with incident response and threat intelligence sharing under both frameworks. The EU–US Trade and Technology Council should host discussions about digital trust where this initiative can serve as part of the broader dialogue. The alignment of standards between jurisdictions will decrease the barriers that slow down international security operations.

Education and advocacy—Security leaders and privacy officers need to present policymakers with practical evidence about how current regulations affect operational security activities. The presentation of concrete WHOIS data cases and anonymized attack studies shows how legal delays lead to security risks. Policymakers will take action based on pressing matters. The current rise in AI-driven cyberattacks (ransomware, deepfake scams, etc.) presents an opportunity to persuade defenders to gain more operational flexibility. Security experts need to maintain continuous involvement because they should participate in AI regulation development to protect cybersecurity requirements. The White House Executive Order on AI demands privacy and security analysis together and requests Congress to create privacy legislation that addresses AI risks.[19] The current privacy legislation framework allows for the possibility of incorporating cybersecurity exceptions in future regulatory developments. The EU should enable industry to advocate for additional guidelines or legislative changes that will strengthen the legal framework for conducting cyber defense operations as NIS2 and the AI Act become operational. AI tools enhance cyber defenses through automated threat detection at machine speed as well as vast dataset analysis to detect attack patterns and augment human analyst resources. The current legal ambiguity and restrictions surrounding these tools prevent defenders from using them fully, but cyber adversaries utilize them with complete freedom. The present security situation has reached its breaking point as we enter a time when AI will speed up cyber threats. The protection of citizens through privacy laws creates an ironic situation where these measures could actually give power to cybercriminals through their restrictions on defenders' data access and technology utilization.

[19] "Safe, secure, and trustworthy: White House publishes Executive Order setting the foundations for future AI regulation in the US," www.dlapiper.com/en-us/insights/publications/ai-outlook/2023/safe-secure-and-trustworthy-white-house-publishes-executive-order

Conclusion

The solution to this paradox is to enact innovative policies with a delicate approach. Modern cyber warfare requires legal frameworks to evolve while protecting citizens' fundamental privacy rights because citizens trust the system. A small-scope cybersecurity safe harbor provides a solution by allowing valid network defense activities and excusing honest mistakes—while continuing to prohibit exploitation and overreach. The recommendations outlined in this paper enable lawmakers and regulators to establish an environment that unites security and privacy instead of forcing them against each other. The proper implementation will enable defenders to use AI for sharing essential information at the same level as attackers while maintaining transparency and oversight that respect our core values. A failure to adjust security measures according to privacy regulations will lead to decreased security that actually puts the protected data at risk.

Government and leaders must act now. AI technology in cybersecurity should avoid the destructive choice between privacy protection and defense measures. The implementation of appropriate legal protections alongside cooperative activities will enable "blue teams" to develop innovative defensive strategies that match the unlawful capabilities of adversaries. Digital interconnection demands security as an essential foundation for protecting privacy. Our laws should be updated to support this truth because such updates will enhance both security and privacy protection. The time has arrived to eliminate artificial restrictions on defensive AI systems so they can perform their mission of protecting businesses' infrastructure and citizens from intelligent threats. This paper provides a path to achieve this goal by ensuring AI remains an ally to network and data defenders during the cyber-battlefield evolution.

Learn more >> sans.org