TLP:CLEAR

G7 CYBER EXPERT GROUP STATEMENT ON Artificial Intelligence and Cybersecurity September 2025

The G7 Cyber Expert Group (CEG) advises G7 Finance Ministers and Central Bank Governors on cybersecurity policy issues critical to the security and resilience of the financial system. Recognizing the rapid evolution of artificial intelligence (AI) technologies, including Generative AI (GenAI), agentic AI, and other advanced systems, the CEG encourages jurisdictions to monitor ongoing developments, promote public-private-academic collaboration, and proactively address the emerging and evolving cybersecurity risks AI may pose.

Artificial Intelligence and Cybersecurity: Navigating Risk and Resilience in the Financial System

AI is the latest in a continuum of significant innovations that have the potential to transform the financial sector. AI capabilities have long been used across the sector, with increasing complexity, integration, and sophistication. These technologies offer significant opportunities to enhance the operational, analytical, and risk management capabilities of financial institutions and authorities.

AI uptake by malicious actors, however, could increase the frequency and impact of malicious cyber activity. And the increasing complexity and autonomy of AI systems, particularly generative and agentic AI, introduce novel cybersecurity risks.

This statement does not set guidance or regulatory expectations. Rather, it aims to raise awareness of AI's cybersecurity dimensions and outlines key considerations for financial institutions, regulatory authorities, and other stakeholders that support security and resilience in the financial sector. The CEG encourages financial authorities to collaborate closely with financial institutions, AI developers, technology firms, academic researchers, and other stakeholders to promote a shared understanding of AI-related cybersecurity issues and to develop strategies that mitigate cyber risks while embracing innovation. The CEG remains committed to advancing dialogue across G7 jurisdictions.

This Statement should be read in conjunction with the G7's Fundamental Elements series, which serve to guide internal and external discussions on cybersecurity risk management decisions critical to cybersecurity, promoting conversations across jurisdictions and sectors to drive effective cyber risk management practices.

TLP:CLEAR

Illustrating the Cyber Impact of AI

AI is reshaping the cybersecurity landscape. The following examples highlight AI's potential to strengthen cyber defenses, amplify existing threats, and expose vulnerabilities rooted in AI system design and data usage.

(1) Ways AI Can Enhance Cyber Resilience

AI can strengthen cybersecurity operations by ingesting, transforming, and learning from vast datasets, identifying patterns and anomalies that might otherwise go unnoticed, and accelerating response times.

- **Anomaly Detection and Response**: AI can identify subtle network anomalies and power adaptive defenses such as AI-enabled web application firewalls (WAFs), addressing threats in real time at machine speed.
- **Fraud Detection and Response**: AI can detect evolving fraud patterns in payments, identify deepfakes used in Know Your Customer evasion, and flag AI-generated phishing emails.
- **Predictive Maintenance and Patching**: AI can anticipate system failures, detect software vulnerabilities, and prioritize vulnerability patching.
- **SOC Efficiency**: GenAI can assist security operations centers (SOCs) by summarizing incidents and recommending responses.
- **Vendor and Supply Chain Risk Monitoring**: AI tools can analyze third-party risks using financial indicators and public data.

(2) Ways AI Could Amplify Existing Cyber Risk

AI can enable attackers to operate with greater precision, speed, and scale.

- **AI-Powered Phishing or Impersonation**: Generative and agentic AI can generate hyper-personalized phishing messages and deepfakes, complicating detection efforts.
- **Automated Exploit Development**: Reinforcement learning techniques can assist attackers by searching a network, software packages and libraries to perform reconnaissance faster, which could lead to increased effectiveness of attacks.
- **Malware Development and Evasion**: AI may be able to create malware that evolves in real-time to avoid detection, lowering the bar for cybercriminals, and increasing both attack volume and sophistication.

(3) Risks Stemming from Attacks That Embed or Exploit Vulnerabilities in AI

AI itself may be a direct target or vector for cyber threats.

- **Data Poisoning**: Manipulated data, both in training and production, can degrade model performance or lead to hidden vulnerabilities that attackers can exploit later.
- **Data Leaks**: Interactions with public AI tools may lead to inadvertent disclosure or extraction of sensitive data.
- **Prompt Injection**: Attackers can exploit system prompts to manipulate outputs or retrieve sensitive information.

Implications for Safety, Soundness Compliance, and Supervision

AI's potential to both mitigate and amplify cyber risks directly affects regulated firms and supervisory authorities.

- **Operational Risk and Resilience**: Adversarial AI may increase exposure to outages, data breaches, and fraud.
- **Human Oversight**: Weak human oversight may delay incident detection or response.
- **Model Risk**: Poorly trained or governed AI models may behave unpredictably or degrade over time.
- **Supply Chain Risk:** AI systems often rely on third-party libraries, datasets, or cloud services. If these are compromised, they can introduce backdoors or vulnerabilities into cybersecurity defenses, amplifying risks across interconnected systems.
- **AI Literacy**: Lack of institutional expertise can compromise effective deployment and oversight.

Maximizing Opportunities While Managing Risks

Financial institutions and authorities may benefit from a proactive approach to safe AI adoption by:

- Identifying where and how AI can be used to manage and address both cyber and non-cyber risks.
- Investing in secure and responsible AI development, particularly for defensive applications.
- Promoting AI systems that are fit-for purpose, appropriately risk-managed, and robust.
- Supporting workforce development through knowledge sharing and training.

TLP:CLEAR

Financial Sector Considerations

AI may influence cybersecurity-related risks in the financial sector in several ways depending on the trajectory and maturity of AI adoption:

- **Malicious Use:** AI uptake by malicious actors could make it easier for them to facilitate, accelerate, and broaden their exploitation of cyber vulnerabilities.
- **Third-Party Dependencies and Service Provider Concentration**: A significant cyber incident at a widely used AI provider could have the potential to affect many financial institutions. The impact on the financial sector and potential for system-wide disruptions will depend on the nature and criticality of the AI services used, including the substitutability of the AI services.
- **Expertise and Specialist Resources**: Institutions lacking AI expertise may be disproportionately vulnerable to associated cybersecurity risk.

Key Considerations for Financial Institutions and Authorities

To manage AI-related cyber risks, financial institutions may consider the following questions:

- **Strategy, Governance, and Oversight**: Are governance frameworks responsive to emerging AI risks?
- **Cybersecurity Integration**: Are AI systems aligned with secure-by-design principles?
- **Data Security and Lineage**: Are data sources vetted and is lineage tracked?
- **Logging and Monitoring**: Are anomalies and edge-cases logged and reviewed?
- **Identity and Authentication**: Are systems resilient against impersonation and AI-enabled fraud?
- **Incident Response**: Are incident response plans and playbooks updated to account for AI-enhanced attacks and AI-specific incidents?
- **Resources, Skills, and Awareness**: What is the path to ensure adequate expertise to evaluate and monitor AI use?

Financial authorities may consider the following strategies for addressing AI and cybersecurity risks:

- Strengthen internal capabilities to understand AI-specific cybersecurity risks.
- Encourage strong governance and leadership engagement related to AI and cybersecurity.
- Engage with technology firms, academia, and financial industry partners to track evolving AI capabilities, and discuss opportunities and risks.

- Integrate AI-related risks into existing risk management processes.

When deployed effectively, AI can bolster cyber resilience by enhancing the speed and precision of detection and response and revealing hidden system vulnerabilities.

Next Steps

As AI becomes more deeply embedded in software systems and financial operations, the cybersecurity implications will continue to evolve. The CEG encourages financial sector stakeholders to:

- Explore AI's potential for enhancing cyber defense capabilities.
- Update risk frameworks to reflect AI-specific cybersecurity vulnerabilities and mitigation strategies.
- Engage in collaborative research and policy development with technology firms and academia.
- Promote public-private dialogue to promote secure and trustworthy AI in the financial sector.

With a deliberate, risk-informed approach, AI can be an effective tool for cybersecurity and resilience, while helping preserve the integrity and stability of the financial system.

Reference Materials: financial institutions may benefit from consulting with frameworks such as:

- ANSSI: Building trust in AI through a cyber risk-based approach; February 2025
- EC: The General-Purpose AI Code of Practice
- EU: EU Artificial Intelligence Act, Regulation - EU - 2024/1689
- FATF: Opportunities and Challenges of New Technologies for Anti-Money Laundering and Countering the Financing of Terrorism
- MITRE ATLAS: Adversarial Threat Landscape for AI Systems
- NCSC/CISA: Guidelines for Secure AI Development
- NIST AI 100-2e2025: Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations
- NIST: Artificial Intelligence Risk Management Framework
- NIST SP 800-218A: Secure Software Development Practices for Generative AI and Dual-Use Foundation Models
- OECD: Principles for trustworthy AI
- OWASP: AI Security and Privacy Guide