MAYER | BROWN

CYBERSECURITY & AI: A LAWYER'S BIBLIOGRAPHY

AUTHORS: STEPHEN LILLEY, ANA HADNES BRUDER

This bibliography is intended as a resource for lawyers working in cybersecurity and artificial intelligence. The following tables loosely group relevant publicly available materials into five general (and, in some cases, overlapping) categories. The following materials are not intended to be comprehensive and are primarily issued by government agencies, technology think tanks, and industry consortiums. The materials below are only meant to provide a starting point in a very dynamic field: numerous other resources are available, including those that are more technical in nature or that are provided by developers of AI systems.

Please note that the materials below may have been updated or moved since this document was last updated in July 2025.

CYBER THREATS AND AI SYSTEMS

ORGANIZATION	PUBLICATION
NIST	NIST AI 100-2e2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (March 2025)
FBI	FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence (May 2024)
New York Department of Financial Services	Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks (October 2024)
Federal Office for Information Security (Germany)	AI Security Concerns in a Nutshell (September 2023)
Federal Office for Information Security (Germany)	How is AI Changing the Cyber Threat Landscape? (April 2024)

ORGANIZATION	PUBLICATION
OECD	Defining AI Incidents and Related Terms (May 2024)
OWASP	OWASP Top 10 for LLM Applications 2025 (November 2024)
OWASP	Agentic AI - Threats and Mitigations, OWASP Top 10 for LLM Apps & Gen AI Agentic Security Initiative (February 2025)
MITRE	ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)
Center for Security and Emerging Technology	Issue Brief: Cybersecurity Risks of AI-Generated Code (November 2024)
Center for Security and Emerging Technology	Policy Brief: Anticipating AI's Impact on the Cyber Offense-Defense Balance (May 2025)
Center for Security and Emerging Technology	Issue Brief: How to Assess the Likelihood of Malicious Use of Advanced AI Systems (March 2025)

RISK MANAGEMENT

ORGANIZATION	PUBLICATION
NIST	NIST AI 100-1, Artificial Intelligence Risk Management Framework (January 2023)
NIST	NIST AI 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024)
CISA	Mitigating Artificial Intelligence (AI) Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators (April 2024)

SECURE DEVELOPMENT, TRAINING, AND TESTING

ORGANIZATION	PUBLICATION
NIST	NIST SP 800-218A, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile (July 2024)
NSA, CISA, and Global Partners	AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems (May 2025)
UK NCSC, CISA and Global Partners	Guidelines for Secure AI System Development (November 2023)
UK Department for Science, Innovation & Technology	Code of Practice for the Cyber Security of AI (January 2025)
Center for Security and Emerging Technology	How to Improve AI Red-Teaming: Challenges and Recommendations (March 2025)

SECURE DEPLOYMENT

ORGANIZATION	PUBLICATION
NSA, CISA, and Global Partners	Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems (April 2024)
UK NCSC	Principles for the Security of Machine Learning (August 2022)
Australian Cyber Security Centre, CISA and Global Partners	Engaging with Artificial Intelligence (AI) (January 2024)
European Parliamentary Research Service	At a Glance: Artificial Intelligence and Cybersecurity (April 2024)

ORGANIZATION	PUBLICATION
ENISA	Multilayer Framework for Good Cybersecurity Practices for AI (June 2023)
ENISA	Securing Machine Learning Algorithms (December 2021)
European Telecommunications Standards Institute (ETSI)	ETSI GAR SAI 009, Group Report, Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework (February 2023)
European Telecommunications Standards Institute (ETSI)	ETSI GR SAI 007, Group Report, Security Artificial Intelligence (SAI); Explicability and Transparency of AI Processing (March 2023)
SANS Institute	DRAFT: Critical AI Security Guidelines, v1.1 (April 2025)
Center for Security and Emerging Technology	Workshop Report: Securing Critical Infrastructure in the Age of AI (October 2024)

INCIDENT PREPARATION

ORGANIZATION	PUBLICATION
CISA	Scenario Document: Joint Cyber Defense Collaborative Artificial Intelligence Cyber Tabletop Exercise (June 2024)
CISA	JCDC AI Cybersecurity Collaboration Playbook (January 2025)

*****

For questions relating to this bibliography, please contact Partners Stephen Lilley or Ana Hadnes Bruder.

AUTHORS

PARTNER

ANA HADNES BRUDER

FRANKFURT +49 69 7941 1778

ABRUDER@MAYERBROWN.COM

PARTNER

STEPHEN LILLEY

WASHINGTON DC +1 202 263 3865

SLILLEY@MAYERBROWN.COM

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively, the “Mayer Brown Practices”). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong & Nair LLC (“PKWN”) is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong & Nair Pte. Ltd. More information about the individual Mayer Brown Practices and PKWN can be found in the Legal Notices section of our website.

Attorney Advertising. Prior results do not guarantee a similar outcome.