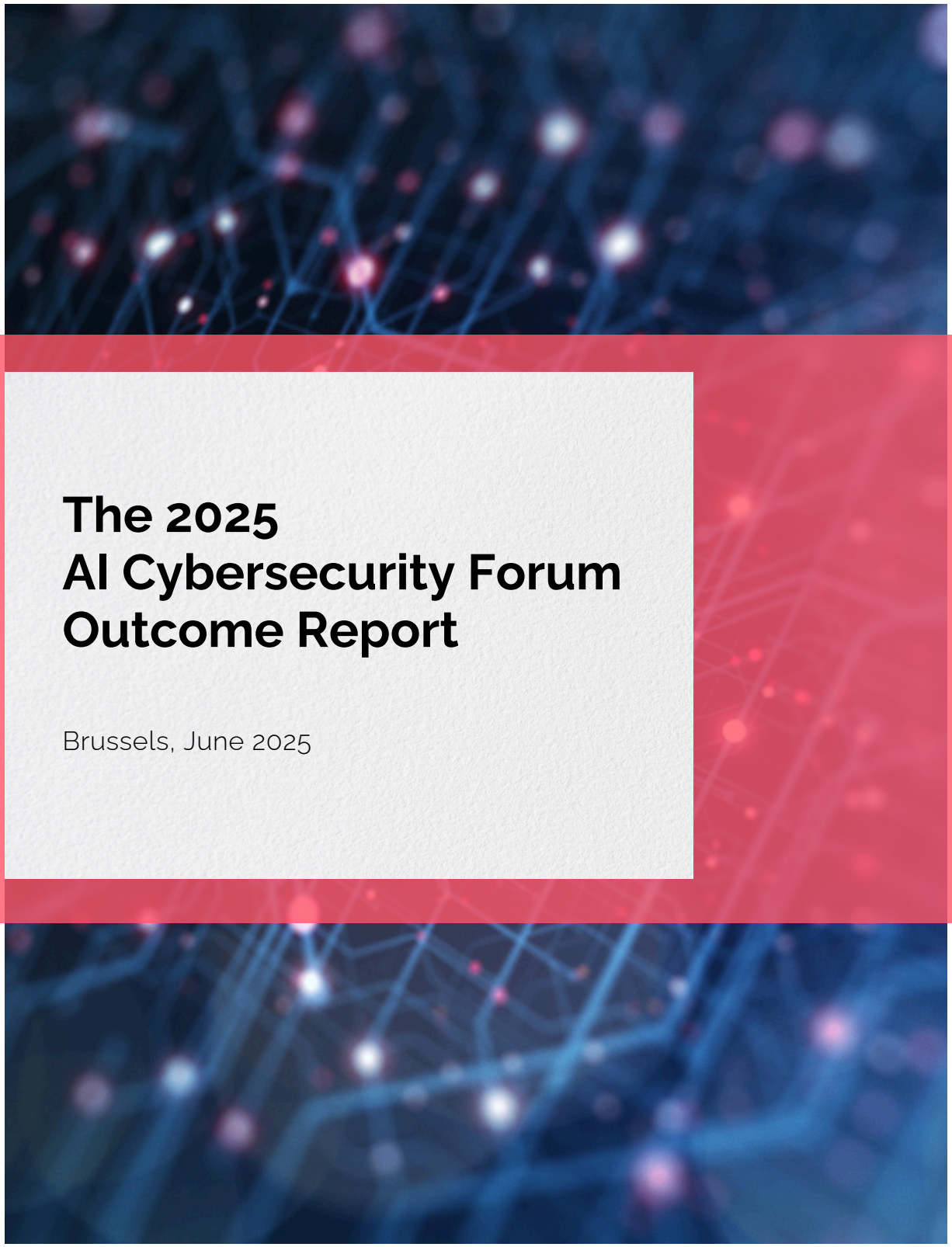
AI Cybersecurity Forum



The 2025 AI Cybersecurity Forum Outcome Report

Brussels, June 2025

AI and Cybersecurity Converge

In June 2025, Brussels hosted the Huawei AI Cybersecurity Forum, a two-day gathering of leading voices from government, industry, academia, and the standards community. The event brought together experts to address the growing interdependence between artificial intelligence and cybersecurity. Across keynote speeches, panel discussions, and live demonstrations, the sessions painted a picture of both opportunity and urgency.

AI is now a critical enabler of cyber resilience, capable of accelerating vulnerability detection, enhancing incident response, and improving supply chain oversight. Yet it is also creating new risks: AI-powered malware, deepfake-enabled social engineering, automated reconnaissance, and adversarial attacks on models are now part of the threat landscape.

These developments are forcing a recognition that AI and cybersecurity are not separate disciplines but intertwined pillars of digital trust. The forum's message was clear — resilience will depend on strategies that fuse AI capabilities, secure supply chains, and globally coherent standards.

New Frontiers in Vulnerability Management for AI

A central topic was Vulnerability Management for AI (VM for AI), an area where existing approaches fall short. Current scoring systems such as CVSS 4.0 are ill-suited to account for AI-specific threats, including data poisoning, model evasion, and risks to ethical or societal outcomes. Huawei's proposed definition of an AI system vulnerability—covering flaws in design, training, deployment, or operation that compromise confidentiality, integrity, availability, safety, or privacy—was highlighted as a foundation for the field.

Experts stressed that while ISO 23894 (AI risk management) and ISO 27034 (application security) offer starting points, AI vulnerability management is essential and inevitable. This would incorporate factors such as model robustness, data provenance, and attack surface complexity. Moreover, the stochastic nature of AI means that mitigation strategies, such as altering inputs and outputs, may currently prove more effective than model patching.

The forum also underlined the need for verification and assurance methods that integrate transparency on training datasets with rigorous testing. Predictive threat modelling — using AI to forecast likely exploitation patterns before they occur — was presented as an emerging priority.

AI as a Force Multiplier in Cyber Defence

While AI brings new risks, it also offers transformative capabilities for cyber defence. Large language models (LLMs) and smaller, domain-tuned systems are now being deployed to detect vulnerabilities, summarise and prioritise risks, and recommend remediation strategies. Tools like Cybi's SCUBA can model probable attack paths with precision, while Greenbone integrates AI-driven vulnerability scanning with live threat intelligence feeds to streamline certain parts of vulnerability management.

Notably, the forum spotlighted the integration of vulnerability prioritisation technologies such as the Exploit Prediction Scoring System (EPSS), and Cyber Risk Quantification (CRQ) into these AI workflows. This pairing allows security teams to prioritise vulnerabilities based on both exploitability and business impact, rather than severity scores alone.

A consistent theme was that AI should be viewed as a collaborator rather than a replacement. False positives, hallucinations, and limited contextual awareness mean human oversight is essential. The optimal approach blends AI's speed and scalability with human expertise, delivering both efficiency and trustworthiness.

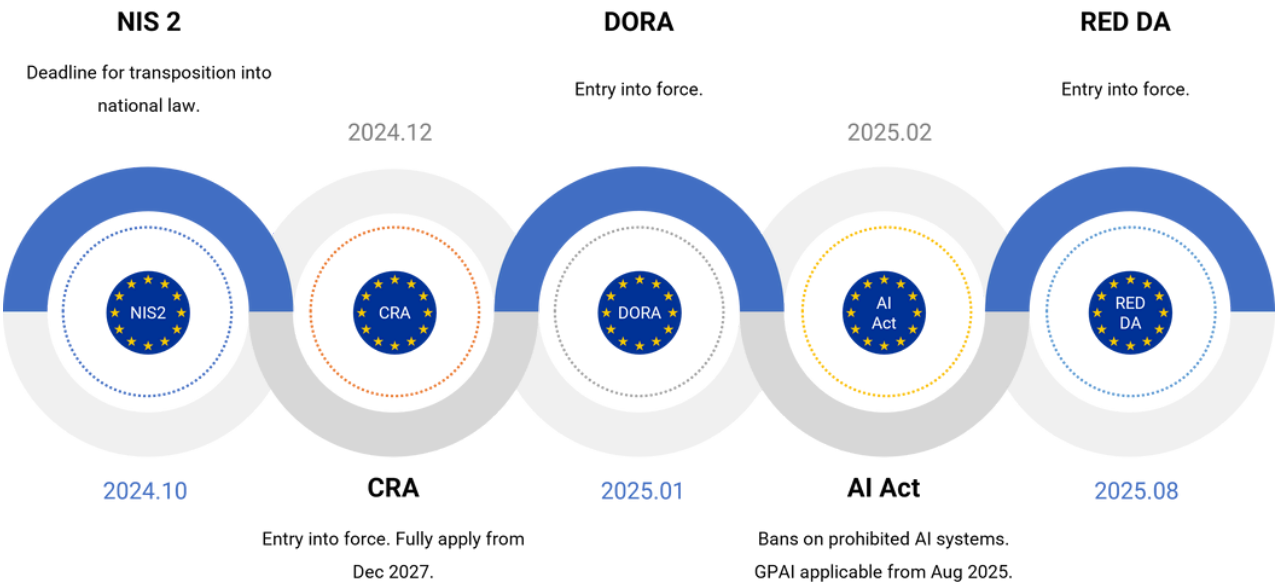
Securing the Software Supply Chain

Software supply chain security emerged as a recurring focus, particularly in light of the fact that up to 77% of enterprise software now includes open-source components, but only about 1% of these components have guaranteed long-term support. The rise in open-source poisoning attacks—up 150% in 2024—underscored the urgency.

Regulatory measures such as the Cyber Resilience Act (CRA) and the updated Network and Information Security Directive (NIS2) are extending producer responsibility to open-source elements, shifting both the legal and operational landscape. The forum examined how transparency mechanisms, such as those supporting component management, and Vulnerability Exploitability eXchange (VEX), can support proactive security, though adoption remains patchy due to costs, complexity, and maturity gaps in open-source governance.

The Linux Foundation's OpenSSF initiative, including its move to become a CVE Numbering Authority, was highlighted as a potential cornerstone for a coordinated European approach. Several speakers advocated for stronger global collaboration frameworks for coordinated vulnerability disclosure, ensuring that information flows quickly across jurisdictions and ecosystems, and de-risks reliance on a small number of central players?

Navigating the EU's Expanding Regulatory Landscape



Participants discussed the challenge of navigating the expanding and often overlapping EU regulatory framework, which includes the AI Act, CRA, NIS2, the DORA, and the Radio Equipment Directive. For many companies, compliance has become a top objective and a major challenge. Compliance can be challenging due to the combination of multiple new regulations for which potential overlaps and conflicts must be addressed; technical standards that trail these new legal requirements; and a shortage of compliance and certification resources.

Speakers argued for the adoption of unified governance frameworks to reduce duplication and enable mutual recognition of certifications. Automation in compliance processes was seen as critical for coping with the scale and speed of regulatory change as well as a widely acknowledged general skills shortage in this domain. Importantly, the discussions framed compliance not merely as an operational burden but as a potential market differentiator, signalling resilience and trustworthiness to customers and partners.

Strategic Outlook

Across all discussions, several strategic imperatives became clear. Organisations will need to adopt AI-specific vulnerability frameworks that explicitly address model-level and data-centric risks, making use of predictive threat modelling and integrated vulnerability prioritization/CRQ approaches. They will need to invest in human-machine cyber operations, where AI handles scale and repetitive analysis while skilled analysts provide judgement and context.

Supply chain security will require end-to-end measures, including robust practices for effective risk management of third-party components including standardized information, active participation in global vulnerability databases, and direct support for open-source maintainers. At the same time, companies should work to harmonise compliance activities across multiple EU regulations to reduce duplication and accelerate time-to-market.

Competing on Trust

The 2025 AI Cybersecurity Forum made it clear that in the coming years, trust will be a critical competitive currency. This trust will be built not only on technical innovation but also on the ability to embed those innovations within robust security governance, resilient supply chains, and a proactive approach to compliance with hard regulation and soft law, while staying in tune with customer expectations as they develop.

AI is no longer just an instrument for cybersecurity—it is both a target and a tool, shaping the threat landscape as much as it protects against it. Organisations that recognise this now, and adapt their strategies accordingly, will be best placed to thrive in an era where resilience is a constantly evolving capability, grounded in technology, process, and people.