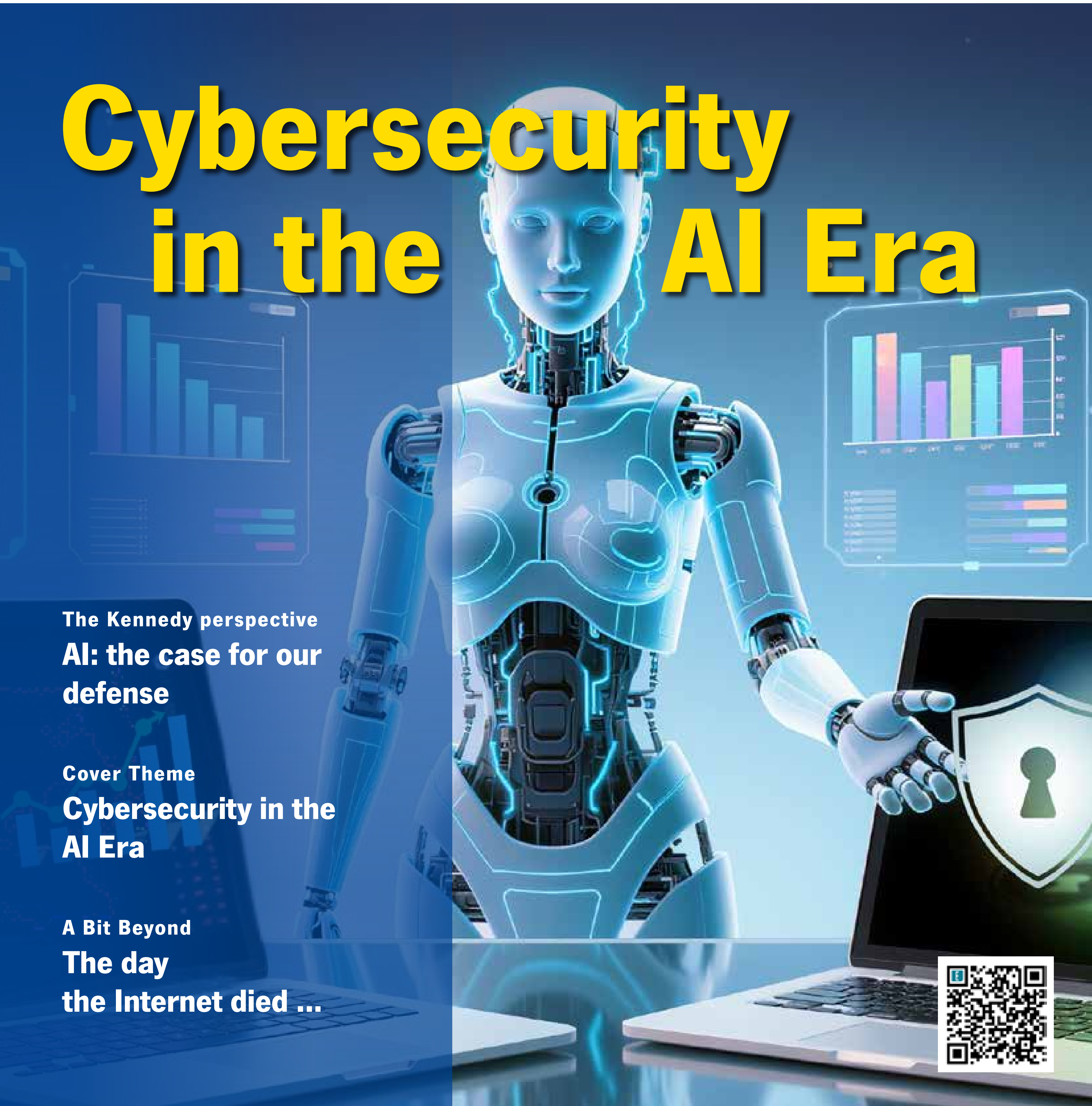
Winter 2025

EURESCOM message

The magazine for telecom insiders

CELTIC News 2/2025

CELTIC-NEXT



Cybersecurity in the AI Era

The Kennedy perspective

AI: the case for our defense

Cover Theme

Cybersecurity in the AI Era

A Bit Beyond

The day the Internet died ...

CELTIC-NEXT

eureka Cluster

Join the Industry-Driven Research Programme of next-generation communications for a secured, trusted, and sustainable digital society

CELTIC-NEXT Spring Call 2026 for Project Proposals – Deadline: 24 April 2026

Here is the opportunity to participate in CELTIC-NEXT, the industry-driven European ICT and telecommunications research programme under the umbrella of EUREKA. Do not miss the submission deadline for the next call for project proposals, on the 24 April 2026!

CELTIC-NEXT projects are collaborative private-public partnership R&D projects. All EUREKA member countries and associated countries can financially support them. More information on public funding and national contacts per country can be found on the CELTIC-NEXT Public Authorities Website. Please talk to your national contact early in the process.

Easy proposal process

Preparing and submitting a CELTIC-NEXT project proposal is easy. Just register via the CELTIC-NEXT online proposal tool, fill in the Web forms, and upload your proposal in pdf. Access to the proposal tool and to a proposal template is available via our Call Information page (https://www.celticnext.eu/call-information).

Benefits of participating in CELTIC-NEXT

- You are free to define your project proposal according to your own research interests and priorities.
- Your proposals are not bound by any call texts, as long as it is within the ICT/telecommunications area see: CELTIC-NEXT Scope and Research Areas.
- CELTIC-NEXT projects are close to the market and have a track record of exploiting their results soon after the end of the project.
- High-quality proposals have an excellent chance of receiving funding, with an average success rate higher than 50%.
- The results of the evaluation will be known by **24 April 2026**.

If you have any questions or need help, do not hesitate to contact us; we would be pleased to support you.

Contact:

CELTIC-NEXT Office
Xavier Priem
office@celticnext.eu
Website: www.celticnext.eu

Dear readers,

Pooja Mohnani
Eurescom GmbH
mohnani@eurescom.eu

As Europe accelerates its digital and AI ambitions, cybersecurity stands as both the enabler and threat! Artificial intelligence is transforming the digital landscape exponentially! It is redefining how we create, communicate, and secure information — while simultaneously expanding our vulnerability. As algorithms grow more capable, so do the threats that exploit them. Cybersecurity in the AI era is no longer a question of defence alone, but of foresight, adaptability, and trust. This new frontier calls for coordinated action: bringing technology enthusiasts, researchers, policymakers, and industry leaders around a shared vision of technological sovereignty and trust. In the AI era, security cannot be an afterthought; it must be the cornerstone of innovation and digital governance.

The **Kennedy's perspective** leads to a thought-provoking reflection on the time when innovation and risk evolve hand in hand. Drawing inspiration from the classic "ambulance in the valley," the article challenges us to rethink whether we are investing enough in prevention rather than repairing the consequences. In his article he includes Scott Adams Six Filters of Truth that help us to reflect i.e., what's true and what's false; read the article and share your thoughts!

The invited article on the **Cybersecurity in the AI era** presents the dual role of AI through a three-dimensional framework: cybersecurity for AI, AI for cybersecurity, and AI against cybersecurity. It highlights key technical challenges and calls for a proactive, interdisciplinary approach to embed secure AI practices across the lifecycle, thereby positioning cybersecurity as a strategic enabler.

Gain insights into the evolving **Digital Partnership on Cybersecurity in the Indo-Pacific region** through the article *"INPACE – Emerging Cybersecurity Architecture of Digital Partnership Countries."* The piece highlights how India, Japan, South Korea, and Singapore are shaping comprehensive cybersecurity frameworks to safeguard critical information infrastructure, strengthen public–private collaboration, and advance cyber resilience. Together, these nations are building a robust digital foundation — one that blends policy, regulation, and innovation to address the complex challenges of the connected world.

The foundations of cybersecurity must evolve with Artificial Intelligence reshaping the digital world. At the core lies the secure boot process — the mechanism that ensures only trusted software runs on a device, protecting systems from tampering and unauthorized access. Eurescom led EU-funded **FORTRESS** project is developing a hybrid secure boot architecture that combines classical and post-quantum cryptography. By reinforcing digital trust at the root, FORTRESS contributes to a new generation of AI-ready cybersecurity, where resilience begins not in reaction to threats, but in the very design of secure, intelligent systems.

As cyber threats grow in scale and sophistication, the European Union is advancing on framework to ensure that trust, resilience, and security remain at the core of its digital transformation. The article "EU Cybersecurity Framework" presents how the EU is building a unified defence through initiatives such as the EU Cybersecurity Act, the Cyber Resilience Act (CRA), and the NIS 2 Directive — supported by key institutions. These efforts form the backbone of Europe's mission to safeguard its digital future and empower citizens, businesses, and public institutions to thrive securely in the digital age.

In the article **"A bit beyond"** the author explores whether AI is quietly undermining its own future in the Internet era. As generative AI increasingly trains on AI-created content, researcher warns of **"model collapse,"** where systems lose diversity, accuracy, and coherence. With synthetic data now saturating the web and ad-based revenue models under strain, both AI reliability and the digital economy face growing uncertainty. The article calls for authentic, human-generated content and transparent data practices to sustain trust, creativity, and truth in the AI-driven Internet.

This edition of **Eurescom's Message** continues our mission to share insights and perspectives that shape the future of connectivity. We warmly invite your **feedback and ideas** for upcoming issues. Write to us at *message@eurescom.eu* and let us know which topics you'd like us to explore next. Your input helps us make each edition more relevant, inspiring, and impactful.

Enjoy reading!

EVENTS CALENDAR

1 December 2025
CELTIC-NEXT Launch Event
Online Event
https://www.celticnext.eu/event/launch-event-of-the-celtic-next-spring-call-2026/

8 – 12 December 2025
IEEE Global Communications Conference
Taipei, Taiwan
https://globecom2025.ieee-globecom.org/

2 – 5 March 2026
Mobile World Congress (MWC) 2026
Barcelona, Spain
https://www.mwcbarcelona.com/

23 – 27 March 2026
Second EU-Japan Digital Week 2026
Tokyo, Japan
https://inpacehub.eu/

13 – 16 April 2026
IEEE Wireless Communications and Networking Conference
Kuala Lumpur, Malaysia
https://wcnc2026.ieee-wcnc.org/

6 May 2026
EUREKA Global Innovation Summit 2026
Basel, Switzerland
https://www.b2match.com/e/global-innovation-summit-2026

18 – 21 May 2026
IEEE INFOCOM 2026
Tokyo, Japan
https://infocom2026.ieee-infocom.org/

2 – 5 June 2026
2026 EuCNC & 6G Summit
Málaga, Spain
https://www.eucnc.eu/

SNAPSHOTS

Techritory participants and SNS CO-OP Partners at the Opening Reception: Antonio de la Oliva (UC3M), Albena Mihovska (SmartAvatar), Egon Schulz (Huawei), Jose Almodovarcho (TNO), Colin Willcock (6G-IA), Uwe Herzog (Eurescom), Miguel Gonzalez Sancho (EC DigitConnect), Carole Manero (IDATE), Hakon Lønsethagen (Telenor), Barbara Pareglio (GSMA), Valeriya Fetisova (TRUST-IT), Veronica Vuotto (TRUST-IT), Audrey Bienvenu (Eurescom), Didier Bourse (Nokia), Pooja Mohnani (Eurescom) & Kostas Trichias (6G-IA)

The Techritory Forum 2025 once again proved itself as a key meeting point for action-oriented experts, policymakers, and industry leaders. This year's edition gathered more than 2,000 participants from 63 countries, featured over 100 speakers, 22 co-creation sessions, and included the signing of a new Memorandum of Understanding. The forum demonstrated strong momentum in shaping Europe's digital future and advancing practical collaboration.

In this dynamic environment, SNS CO-OP held its second face-to-face plenary meeting in Riga, hosted by the Electronic Communication Office of Latvia. The project, coordinated by Eurescom, supports the Smart Networks and Services Joint Undertaking (SNS JU) in connecting research excellence with industrial innovation and ensuring that next-generation connectivity reflects European values. By working closely with the SNS JU Office and the 6G Industry Association, SNS CO-OP promotes the European perspective on 6G and highlights achievements across the SNS initiative.

This made SNS CO-OP's participation at Techritory Forum 2025 especially meaningful, contributing to Europe's vision for secure, sovereign, and future-ready connectivity. We extend our thanks to all who engaged at the forum, and we look forward to continuing this shared effort at Techritory Forum 2026 in Riga.

Further information

- SNS CO-OP project: *https://smart-networks.europa.eu/call-3-stream-csa/#SNS-CO-OP*
- Techritory forum 2025: *https://www.techritory.com/*

Contents

THE KENNEDY PERSPECTIVE

COVER THEME: Cybersecurity in the AI Era

CELTIC NEWS 02/2025

EVENTS

A BIT BEYOND

CELTIC-NEXT
Eureka Cluster
CELTIC News 2/2025
The issue of Eureka ICT-Cluster CELTIC-NEXT
Words from the Director
What CELTIC-NEXT Cluster has delivered in the second half of 2025 and what is coming in 2026?
Projects Highlights
6G-SKY Mobility management, cybersecurity and explainable AI for aerospace communications
AIComHealth – 5G-based collective intelligence for health crisis management
USWA: Ultra Scalable Wireless Access
CELTIC-NEXT Event
Proposer's Day in Aveiro: AI, the Heart of the CELTIC Community – the European AI-ACT & 6G Fuelling the AI Compute Continuum

Imprint

Eurescom message, Winter 2025
ISSN 1618-5196 (print edition)
ISSN 1618-520X (Internet edition)

Editors: Pooja Mohnani (editor-in-chief), Audrey Bienvenu (co-editor), Anastasius Gavras, Uwe Herzog, Luitgard Hauer (Reviewers)

Submissions are welcome, including proposals for articles and complete articles, but we reserve the right to edit.
If you would like to contribute, or send any comments, please contact:
Eurescom message · Wieblinger Weg 19/4 · 69123 Heidelberg, Germany · Phone: +49 6221 989–0 · Fax: +49 6221 989–209 · E-mail: message@eurescom.eu

Eurescom message is published twice a year. Eurescom message on the Web: http://www.eurescom.eu/message

Data Protection Declaration: https://www.eurescom.eu/data-protection-declaration.html

Some of the images used in this edition of the Eurescom Message are from the license subscription of the Tool Canva Pro, all rights are reserved by the tool Canva.

AI: the case for our defense

David Kennedy
Eurescom GmbH
kennedy@eurescom.eu

Introduction

Many years ago, John Denver read a poem about the ambulance down in the valley which highlighted the small-town struggle to decide between putting a fence on top of the cliff to stop people falling or to buy an ambulance in the valley to pick up those who fell. It ends with a local sage observing that *"That people give far more attention to repairing the results than to stopping the cause, when they'd much better aim at prevention"*. As I look at AI and Cybersecurity discussions today, I somehow get the feeling that we revisiting this principled discussion but fuelling the arms race on both sides.

I understand that AI focuses on building intelligent systems through automation and learning to support our lives and decisions. Cybersecurity, on the other hand, focuses on protecting our digital assets from threats. Obviously, we will need the cybersecurity skills to protect our AI systems from being hacked or misused and AI could be used to enhance cybersecurity by improving threat detection capabilities and auto-responses – but the bad guys could also use AI to learn how to attack systems. This means that it is not a simple decision between the fence and the ambulance but an ongoing struggle to keep the balance between the forces for good and evil.

New definition of Cybersecurity in the AI era.

We are slowly becoming aware that our realities are being subtily altered. The stream of news we get over the internet is being tailored to make money for someone and to do this they profile us and send us each more of what "they" think we like. This means our news stream can be very unbalanced as the search engine, browsing algorithm or even friends' postings get screened to what the system believes we want to see. It gets more problematic if the content we're being offered is AI generated and not based on reality at all.

So maybe we need a new generation of Cybersecurity tools that tell us when we are being send modified data – or worse, selective data where we don't get to see the full picture.

The misuse of AI tools is not just limited to the criminal classes – it is now pervasive in the production of many research papers, business plans and strategic views. This is fine as long as we know what we are doing. If we are just asking a tool to paraphrase the text OK, but if we are asking the tool to do more, we need to be careful. Large language models can be used to summarize text or translate text between languages, but accuracy is not guaranteed and requires checking by a human — particularly when working in languages other than English.

Somehow many of us seem to learn the vital swear words and bad language when learning languages and particularly if we allow AI to learn dialogue from our TV programs, we may risk the tool learns improper language use.

The second new use of the AI tools is to help regulate from where AI tools learn. Just like people, there are sources you can't trust and should not take as references for future behaviour.

So my new approach is to use AI supported Cybersecurity not only to keep the bad guys out but also to filter out the bias and misinformation in what I allow into my world.

How to train our AI Cybersecurity

We need to adopt some logic and methodology now to help us navigate our complex information space and the basic rule is to use many sources to get a good clear picture. Scott Adams (famous for creating Dilbert) proposed the Six Filters of Truth[1] to capture how we try to see what's true and what's false: *personal experience, experiences of people you know, experts, scientific studies, common sense, and pattern recognition.* Of course, each of these can be flawed so depending on one alone is a risk. The more filters something can pass the greater the likelihood that it is true.

We still need a new AI tool to tell us when something has been modified, when people are lying and when things are being hidden – only then will I feel Cyber secure.

[1] How to Fail at Almost Everything and Still Win Big: Kind of the Story of My Life, Scott Adams ISBN-13 978-1591846918

Cybersecurity in the AI Era

Siemens AG, Foundational Technologies, Cybersecurity and Trust department, Munich, Germany

Dr. Anita Aghaie
anita.aghaie@siemens.com

Dr. Fabienne Bruendl
fabienne.bruendl@siemens.com

Artificial Intelligence (AI) fundamentally reshapes cybersecurity by enhancing defensive capabilities while introducing new attack vectors. This article explores the dual role of AI through a three-dimensional framework: cybersecurity for AI, AI for cybersecurity, and AI against cybersecurity. It highlights key technical challenges and calls for a proactive, interdisciplinary approach to embed secure AI practices across the lifecycle, thereby positioning cybersecurity as a strategic enabler.

Introduction

AI has rapidly become a core pillar of digital business and is driving a fundamental shift in cybersecurity approaches across industries. As AI models and agents become more capable, they introduce both defensive opportunities and novel attack surfaces. Summarizing the central theme of the 2025 RSA conference, McKinsey succinctly captured this duality:

"AI is the greatest threat - and defence - in cybersecurity today."[1]

For stakeholders across IT/OT, the question is no longer whether or how to 'adopt AI', but how to adopt it securely. The cybersecurity landscape is being reshaped not only by how AI is used, but also by how it must be protected and how it can be used against cybersecurity itself. Understanding and addressing the challenges of these three interrelated dimensions is essential for securing the digital infrastructure of modern industry and telecommunication.

The weakest link might be the smartest one: Cybersecurity for AI

In Europe, Article 15 of the EU AI Act mandates high-risk AI systems to ensure accuracy, robustness, and cybersecurity[2], which in practice requires implementing technical safeguards, resilience strategies, and auditable processes. While this applies to high-risk AI systems, these principles are essential for all AI systems, covering the entire AI lifecycle.

A three-pillar framework for securing AI systems can be derived from the principles outlined in the EU AI Act, IEEE research on data integrity[3], and operational threat models such as the OWASP Top 10 for Large Language Models (LLMs)[4].

The first pillar is cryptographic technologies, such as secure multi-party computation (MPC) for collaborative analytics on sensitive data and fully homomorphic encryption (FHE) for privacy-preserving inference on encrypted inputs, along with complementary approaches like trustworthy execution platforms and federated learning (FL) with secure aggregation to protect model updates.

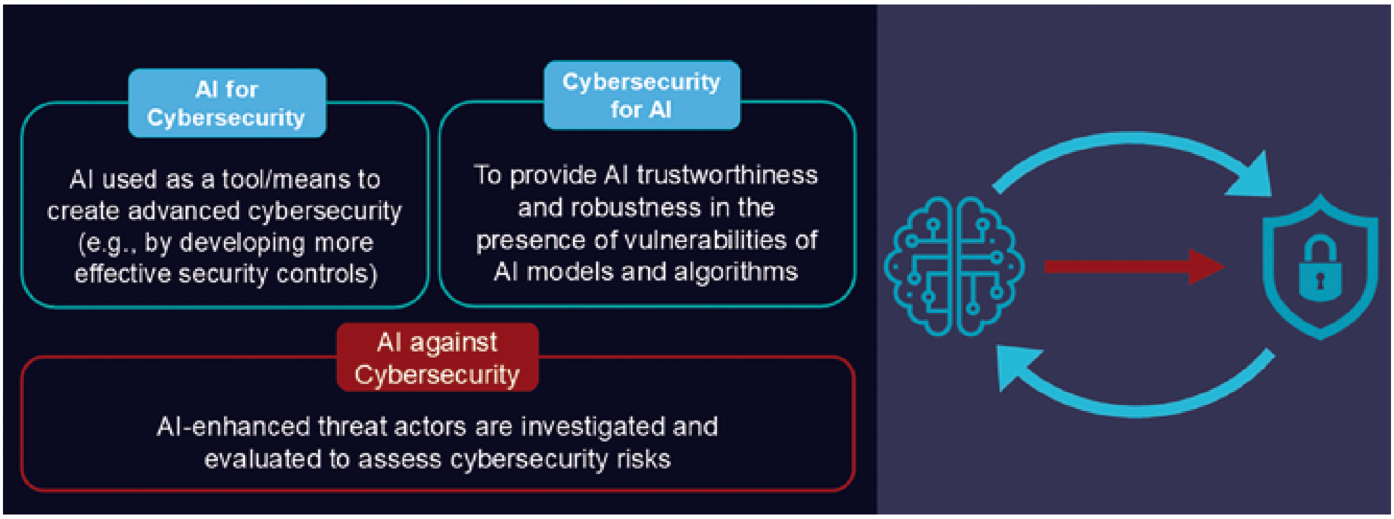
The second pillar is secure engineering practices, guided by standards like ISO/IEC 42001[5], the NIST AI Risk Management Framework (AI RMF) Generative AI (GenAI) Profile (NIST AI 600-1)[6], and the Secure Software Development Framework (SSDF) for GenAI (NIST SP 800-218A)[7].

Operational safeguards form the third pillar. Models should be treated as executable content, using sandboxing and provenance tracking. Continuous testing should be an integral part of operations to detect jailbreaks, model drift, and data exfiltration. These safeguards also address the OWASP Top 10 for LLM applications, including prompt injection, data poisoning, and supply-chain vulnerabilities.

As European standards, e.g., CEN-CENELEC JTC 21[8], evolve, organizations should align with existing frameworks to turn regulatory intent into concrete, testable controls for IT/OT environments.

AI for Cybersecurity: AI joins the blue team

AI is increasingly supporting defenders throughout the cyber defence lifecycle. Offensive security teams are now leveraging AI to simulate adver-



AI for Cybersecurity

AI used as a tool/means to create advanced cybersecurity (e.g., by developing more effective security controls)

Cybersecurity for AI

To provide AI trustworthiness and robustness in the presence of vulnerabilities of AI models and algorithms

AI against Cybersecurity

AI-enhanced threat actors are investigated and evaluated to assess cybersecurity risks

Illustration: Three dimensions of cybersecurity in the AI era sarial behaviour, e.g., crafting evasive malware, generating adversarial examples to bypass detection systems, and mimicking insider threats. LLM-enabled agents assist with automated reconnaissance and log analysis, while deep-learning models enhance hardware security through anomaly detection and side-channel evaluation.

Yet, deploying AI in critical environments demands strong safeguards, as mentioned above.

AI against Cybersecurity: The rise of autonomous offense

Attackers are industrializing AI. Deepfake-enabled social engineering has already driven large-scale fraud, while LLM-specific risks, e.g., prompt-injection, tool-abuse, and model supply-chain attacks are escalating. Techniques like 'package hallucination' and slop squatting exploit hallucinated dependencies to trick developers into importing malicious code[9].

AI tools are also transforming penetration testing by automating reconnaissance, vulnerability scanning, and exploit generation. A fully autonomous AI-driven pentesting tool has even reached the top spot on HackerOne's US leaderboard[10], demonstrating the efficiency of AI-based offensive systems.

Conclusion

As AI reshapes cybersecurity, its dual role as defence tool and attack vector demands a fundamental shift in securing digital infrastructure, starting with the AI systems themselves. Cryptographic innovation, secure engineering, and operational safeguards must become core practices, with regulations like the EU AI Act serving as a starting point. Yet technical and operational challenges remain. Privacy-preserving technologies such as FHE are still computationally expensive and difficult to scale, depending on the use case. Hallucination in generative or autonomous models poses significant operational risk, requiring built-in verification and containment strategies to prevent unintended or unsafe behaviour.

Securing AI is not just about protecting algorithms, but also about reinforcing the trustworthiness and resilience of digital systems. As adversaries increasingly use AI against cybersecurity, defenders must stay ahead through continuous innovation, rigorous engineering, and cross-disciplinary collaboration. The organizations that succeed will be those that embed secure AI practices deeply into their operations, transforming cybersecurity from a reactive necessity into a strategic enabler.

References

[1] Charlie Lewis, Ida Kristensen, Jeffrey Caso, Julian Fuchs, "AI is the greatest threat—and defense—in cybersecurity today. Here's why", McKinsey Blog, May 15, 2025, https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today

[2] Regulation (EU) 2024/1689 (EU AI Act), Official Journal of EU, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[3] Davi Ottenheimer and Bruce Schneier, "The AI agents of tomorrow need data integrity," IEEE Spectrum, August 18, 2025, https://spectrum.ieee.org/data-integrity

[4] OWASP Top 10 for LLM Applications, https://owasp.org/www-project-top-10-for-large-language-model-applications/

[5] ISO/IEC 42001:2023 – AI Management System Standard (ISO), https://www.iso.org/standard/42001

[6] NIST AI 600-1, AI Risk Management Framework: Generative AI Profile, https://www.nist.gov/itl/ai-risk-management-framework

[7] NIST SP 800-218A, Secure Software Development Practices for Generative AI (July 2024), https://csrc.nist.gov/pubs/sp/800/218/a/ipd

[8] CEN-CENELEC JTC 21 Artificial Intelligence – committee overview, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/

[9] Sean Park, Trend Micro, "Slopsquatting: When AI Agents Hallucinate Malicious Packages," June 5, 2025, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/slopsquatting-when-ai-agents-hallucinate-malicious-packages

[10] Nico Waisman, "The road to Top 1: How XBOW did it," XBOW Blog, June 24, 2025, https://xbow.com/blog/top-1-how-xbow-did-it

FORTRESS - Fully Optimised Root of Trust for Robust Embedded Secure Systems

Univ.-Prof. Dr. Michael Hutter
University of the Bundeswehr Munich
michael.hutter@unibw.de

Uwe Herzog
Eurescom GmbH
herzog@eurescom.eu

Dr. Axel Y. Poschmann
PQShield Ltd
axel.poschmann@pqshield.com

Pooja Mohnani
Eurescom GmbH
mohnani@eurescom.eu

The secure boot process is the cornerstone of modern cybersecurity, ensuring only trusted software runs on a device. With the advent of quantum computing, traditional cryptographic algorithms won't be appropriate any longer. The EC-funded FORTRESS project will develop a solution that will enable achieving the required security level in the post quantum era.

The objective of a secure boot process is to ensure that only trusted software runs on a device, done by validating code integrity with cryptographic signatures. It upholds the Confidentiality, Integrity, and Availability (CIA) triad, protecting devices from tampering, malware, and unauthorised changes. As connected devices increasingly integrate with cloud services, secure boot must validate integrity across both hardware endpoints and cloud environments.

Traditional cryptographic algorithms long relied upon for secure boot as, e.g. RSA and ECC face obsolescence with the advent of quantum computing. Shor's algorithm enables quantum computers to break RSA, ECC, and similar cryptosystems, necessitating a transition to Post-Quantum Cryptography (PQC). Global efforts are underway to develop quantum-resistant standards with EU agencies like ANSSI and BSI advocating for Post-Quantum/Traditional (PQ/T) hybrid cryptographic models. These models combine traditional and quantum-safe algorithms, offering added resilience during the transition. However, PQ/T implementation poses challenges including algorithm limitations, performance trade-offs and compliance issues. Aiming at addressing these, organisations like ETSI, CISA and NCSC have issued guidance on PQ/T hybrid cryptography deployment. ETSI emphasises standardisation and optimization to manage PQ/T hybrid system complexities, while CISA and NCSC highlight proactive collaboration for safeguarding infrastructure and planning PQC transitions.

A robust and scalable solution is critical for quantum-safe secure boot. This includes developing a PQ/T Hybrid Root of Trust (RoT) that integrates traditional and post-quantum algorithms, minimising performance overheads, and enabling secure boot across diverse platforms. The solution has to take into account aspects of security, performance and cost, and must align with regulatory requirements. The FORTRESS project will develop a solution that will enable embedded systems, edge devices, and Critical National Infrastructure (CNI) to seamlessly transition to quantum-resistant architectures which will be an essential element in ensuring the future security of digital systems in Europe.

What tools and technologies will be used?

To deliver on its objectives, FORTRESS will develop a comprehensive set of tools and technologies designed to support the secure integration of post-quantum and PQ/T hybrid cryptographic mechanisms across diverse platforms. First, an open-source benchmarking framework will be created that includes performance profiling scripts, analytical models, and automated evaluation pipelines to assess RoT implementations against key performance indicators (KPIs) such as latency, area, memory usage, and security. This tool set will enable stakeholders to make data-driven decisions when selecting or designing quantum-resistant secure boot mechanisms. Second, FORTRESS will design PQ/T hybrid cryptographic cores using HW/SW co-design methodologies that integrate traditional algorithms (e.g. RSA, ECDSA) with post-quantum schemes (e.g. FN-DSA, LMS, ML-DSA), optimized for efficiency, scalability, as well as fault and side-channel resistance. These cores will be evaluated in both embedded and cloud-connected environments. To address real-world deployment needs, FORTRESS will produce reference implementations of PQ/T hybrid secure boot flows, accompanied by integration guidelines, performance baselines, and compliance checklists. In parallel, the project will develop a threat-informed attack library and conduct research on active and passive attacks targeting PQC schemes, to support hardening efforts. All tools and findings will be shared with the wider community under open or appropriately licensed terms, ensuring transparency, reproducibility, and long-term impact.

How it will benefit the stakeholders/ business at large?

FORTRESS will benefit stakeholders and the broader business landscape by providing the tools, technologies, and guidance needed to securely transition to post-quantum cryptography without disrupting existing operations. The project delivers practical solutions for deploying PQ/T hybrid cryptographic models ensuring long-term security while maintaining compatibility with current systems. Businesses and technology providers will gain access to an open-source benchmarking framework to evaluate Root of Trust (RoT) implementations against defined performance and security metrics, enabling informed decisions on secure boot integration and system design. Operators of embedded systems, edge devices, and critical national infrastructure (CNI) will be able to assess quantum-safe secure boot mechanisms with minimal performance and cost impact. By focusing on PQ/T hybrid schemes such as ML-DSA/ECDSA and FN-DSA/ECDSA, FORTRESS supports real-world migration strategies that avoid disruptive system overhauls. The project also addresses key implementation challenges such as overhead, interoperability, and compliance by aligning with international recommendations from ETSI, CISA, and NCSC. Stakeholders will benefit from reduced cybersecurity risk, improved regulatory readiness, and increased trust in digital systems. With additional resources like reference architectures, evaluation tools, and research on PQC-specific threats, FORTRESS empowers businesses to future-proof their security infrastructure while staying competitive in a rapidly evolving threat landscape.

Conclusion

As we enter the quantum era, trustworthiness of devices and infrastructures needs a fundamental overhaul of secure boot processes. Traditional cryptography can no longer assure long-term resilience, thus the transition to post-quantum and PQ/T hybrid models is both urgent and strategic. The FORTRESS project positions Europe at the forefront of this evolution by delivering an integrated framework of tools, methodologies, and reference implementations that enable a smooth, standards-aligned migration to quantum-resistant architectures.

By combining research on post-quantum algorithms with practical implementation pathways – from frameworks to hybrid Root of Trust (RoT) designs – FORTRESS bridges the gap between theoretical security and operational applicability. Its open and collaborative approach will ensure its adoption by industry, regulators, and critical infrastructure operators alike.

FORTRESS will empower stakeholders to build systems that remain secure, compliant, and trusted in a post-quantum world. This effort prepares for quantum disruption, which is not only a technical necessity but a strategic investment in the resilience and competitiveness of future digital ecosystems.

Further information

- FORTRESS website: *https://pq-fortress.eu/*

INPACE – Emerging Cybersecurity Architecture of digital partnership countries

Anastasius Gavras
Eurescom GmbH
gavras@eurescom.eu

Digital Partnership on Cybersecurity in Indo-Pacific region

The Indo-Pacific region stands at the forefront of global digital transformation, where rapid technological progress intersects with increasing cybersecurity challenges. As nations expand their digital economies, ensuring secure, resilient, and trusted digital infrastructures becomes a shared strategic priority. In this context, the **INPACE project (Indo-Pacific Cooperation for Digital Partnership)**—in which **Eurescom** actively participates—plays a crucial role in fostering cooperation, dialogue, and knowledge exchange between the European Union and Indo-Pacific partner countries. The project aims to strengthen mutual understanding of cybersecurity policies, governance models, and capacity-building initiatives, thereby supporting the broader goals of the EU's Digital Partnership strategy.

This article contributes to the objectives of the INPACE project by examining the **emerging cybersecurity architectures of key Digital Partnership countries in the Indo-Pacific region—namely India, Japan, South Korea, and Singapore**. These countries have developed comprehensive frameworks to safeguard critical information infrastructure, promote public–private collaboration, and enhance cyber resilience through policy, regulation, and innovation.

Emerging Cybersecurity Architecture in India

India's cybersecurity architecture is designed to address the growing cyber threats and ensure the security of its digital infrastructure. India's cybersecurity architecture is continuously evolving to address emerging threats and enhance the resilience of its digital infrastructure. The main components of India's cybersecurity architecture are:
National Cyber Security Policy (NCSP): Launched in 2013, the NCSP protects information and infrastructure, build capabilities to prevent and respond to cyber threats, and reduce vulnerabilities. NCSP is a building block of the Cybersecurity group of the Ministry of Electronics and Information Technology (MeitY) of the government of India.

Indian Computer Emergency Response Team (CERT-In): The national agency responsible for responding to cybersecurity incidents, providing alerts and advisories, and coordinating efforts to mitigate cyber threats.

National Critical Information Infrastructure Protection Centre (NCIIPC): Focuses on protecting critical information infrastructure in sectors like energy, banking, telecom, and transportation.

Cyber Swachta Kendra: A botnet cleaning and malware analysis centre that provides tools and resources to detect and remove malicious software. It is part of the Government of India's Digital India initiative under MeitY. It was set-up and operates in accordance with the objectives of NCSP.

Data Protection Framework: The Digital Personal Data Protection (DPDP) Act 2023 for Citizens and Businesses aims to regulate the processing of personal data and ensure the privacy of individuals. The DPDP Act proposes to grant individuals certain rights, such as the right to have their personal data processed only with their consent, and includes provisions for measures to safeguard their data.

Cybersecurity Awareness Programs: Initiatives like Cyber Surakshit Bharat aim to raise awareness and build capacity in cybersecurity across various sectors.

India's cybersecurity architecture derives from the Digital India program, a campaign launched by the government of India to make its services available to citizens electronically via improved online infrastructure and by increasing Internet connectivity. The initiative includes plans to connect rural areas with high-speed internet networks. It consists of three core components: the development of secure and stable digital infrastructure, delivering government services digitally, and universal digital literacy. Further notable initiatives are:
Smart Cities Mission, which integrates cybersecurity measures into the development of smart cities to ensure the safety and security of digital infrastructure.

National Cyber Coordination Centre (NCCC), which monitors cyber threats and coordinates responses to protect national security. It serves as an e-surveillance and cybersecurity agency, monitoring communication metadata and coordinating intelligence gathering to fend off cyber threats.

Indian Cyber Crime Coordination Centre (I4C), which is a government initiative to deal with cybercrime in India, in a coordinated and effective manner. It provides a framework and ecosystem for law enforcement agencies. The I4C has several components, including the National Cyber Crime Threat Analytics Unit, National Cyber Crime Reporting Portal, and National Cyber Crime Training Centre.

India has several publicly funded research, development, and innovation programs focused on cybersecurity. The main programmes are:
National Cyber Security Programme: This programme aims to enhance the cybersecurity capabilities of the country by funding research and development projects in various areas of cybersecurity.

Cyber Security Research and Development (R&D) Scheme: Managed by MeitY, this scheme supports R&D projects in cybersecurity to develop indigenous solutions and technologies.

The **Information Security Education and Awareness (ISEA)** programme focuses on creating awareness about cybersecurity and developing skilled professionals through education and training programs.

NextGen Cyber Security Research Group: Hosted by the Indian Institute of Information Technology, this group focuses on advancing cybersecurity through research, innovation, and development.

Chevening India Cyber Security Fellowship: Funded by the UK Foreign, Commonwealth, and Development Office, this fellowship aims to develop leadership potential in cybersecurity among mid-career professionals in India.

Emerging Cybersecurity Architecture in Japan

Japan has a robust cybersecurity architecture designed to protect its digital infrastructure and enhance its cyber resilience.

Cybersecurity Strategy: Japan's Cybersecurity Strategy outlines the country's basic position on cybersecurity policy, its objectives, and implementation plans for three years. The current strategy was issued in September 2021. The main components of Japan's cybersecurity architecture are:
National centre of Incident readiness and Strategy for Cybersecurity (NISC): Established in 2015, NISC coordinates cybersecurity policy and strategy across government entities and promotes partnerships between industry, academia, and the public sector. NISC coordinates cybersecurity policy by formulating:

- Cybersecurity Strategy
- Cybersecurity Policy for Critical Infrastructure Protection
- Common Standard on Information Security Measures of Government Entities
- Cybersecurity Human Resource Development Plan
- Cybersecurity Research and Development Strategy etc.

NISC takes a role of a governmental CERT. NISC and JPCERT/CC, as a CERT covering private entities, work together as a national CERT.

The **Japan Computer Emergency Response Team Coordination Centre (JPCERT/CC)** is Japan's Computer Security Incident Response Team, established in 1996. It acts as a coordination centre for cybersecurity incidents, working with network service providers, security vendors, government agencies, and industry associations. JPCERT/CC is a member of the Forum of Incident Response and Security Teams (FIRST) and helped form the Asia Pacific Computer Emergency Response Team (APCERT), providing a secretariat function for APCERT.

Cybersecurity Strategic Headquarter is a body formed under the Cabinet in 2014, and oversees the implementation of cybersecurity policies and strategies. It is headed by the Chief Cabinet Secretary and includes relevant ministers and experts.

A notable publicly funded research, development, and innovation initiative is the Cybersecurity Research Institute (CSRI), which is part of the National Institute of Information and Communications Technology (NICT). CSRI promotes R&D in cybersecurity technologies to protect society from sophisticated cyber-attacks. It includes the Cybersecurity Laboratory, Security Fundamentals Laboratory, and National Cyber Training Centre.

Emerging Cybersecurity Architecture in South Korea

The cybersecurity architecture of South Korea is designed to protect its digital infrastructure and enhance its cyber resilience. The main components of its cybersecurity architecture are:
National Cyber Security Strategy: South Korea's National Cyber Security Strategy outlines the country's vision, goals, and strategic tasks for cybersecurity. The latest strategy was updated in 2024.

National Cybersecurity Basic Plan: This plan includes specific implementation measures to achieve the objectives of the National Cyber Security Strategy. It involves multiple government ministries and organizations jointly developed by the National Intelligence Service, Ministry of Foreign Affairs, Ministry of Defence, Ministry of Science and ICT, Supreme Prosecutors' Office, and Police.

Korea Internet & Security Agency (KISA): KISA is responsible for promoting internet security and managing cybersecurity incidents. It provides support to both public and private sectors. KISA is responsible for the allocation and maintenance of South Korea's IPv4/IPv6 address space, Autonomous System Numbers, and the .kr country code top-level domain (ccTLD). It operates the Korea Computer Emergency Response Team Coordination Center (KrCERT/CC) and facilitates international cooperation on cybersecurity. Recently KISA identified generative AI as a key cybersecurity issue and is working on establishing security standards and guidelines to address related threats. Finally, KISA has implemented an IoT security certification system.

National Intelligence Service (NIS) is South Korea's chief intelligence agency, responsible for both domestic and international intelligence activities: The NIS functions include national cybersecurity related responsibilities focusing on protecting critical infrastructure and responding to cyber threats.

Cyber Command: Established under the Ministry of National Defence, Cyber Command is responsible for defending military networks and responding to cyber threats targeting national security. Among others it can launch offensive cyber operations to neutralise threats.

Finally, South Korea has launched initiatives to raise public awareness and educate citizens about cybersecurity best practices, programs to develop skilled cybersecurity professionals through education and training and invests heavily in R&D to advance cybersecurity technologies and solutions.

South Korea has several publicly funded research, development, and innovation programmes focused on cybersecurity, such as:
Cyber Security Research Centre (CSEC): Established by Soongsil University, CSEC conducts innovative research projects in cyberspace security and defence. It is funded by the Global Research Laboratory (GRL) programme and the ICT Basic Research Laboratory (BRL) programme, both supervised by the National Research Foundation of Korea (NRF).

National Cyber Security R&D Program: Managed by the Ministry of Science and ICT, this programme supports research and development in various areas of cybersecurity to enhance national security and technological capabilities.

Emerging Cybersecurity Architecture in Singapore

Singapore has a well-structured cybersecurity architecture designed to protect its digital infrastructure and enhance its cyber resilience. The key components of Singapore's cybersecurity architecture are:
Singapore Cybersecurity Strategy: Launched in 2016 and updated in 2021, this strategy outlines the country's approach to building a resilient and trusted cyber environment. It focuses on strengthening the resilience of critical information infrastructure, mobilizing businesses and the community, developing a vibrant cybersecurity ecosystem, and enhancing international partnerships.

Cyber Security Agency of Singapore (CSA): Established in 2015, the CSA is the national agency overseeing cybersecurity strategy, operations, education, outreach, and ecosystem development.

The **Government Cybersecurity Operations Centre (GCSOC)** is an integrated initiative that aims to upgrade the government's monitoring and detection technologies, automate and augment cyber threat detection and response as well as develop capabilities to proactively hunt for sophisticated threats.

Government Zero Trust Architecture (GovZTA): This framework provides a comprehensive approach to implementing Zero Trust principles across government agencies, ensuring that no user, application, or device is trusted by default. Singapore has several publicly funded research, development, and innovation programmes focused on cybersecurity, such as:

Singapore Cybersecurity Consortium (SGCSC): Anchored at the National University of Singapore (NUS)and supported by the National Research Foundation (NRF), this consortium promotes use-inspired research, technology translation, manpower training, and technology awareness in cybersecurity.

CyberSG R&D Programme Office: Established by the Cyber Security Agency of Singapore (CSA) at Nanyang Technological University (NTU), this office aims to position Singapore as a global leader in cybersecurity R&D. It receives funding under the RIE2025 NCRP Funding Initiative.

Conclusion

Overall, in all the above countries, the implementation of the strategy relies on collaboration between the public and private sectors to enhance cybersecurity capabilities, tackle cybersecurity challenges, including workforce shortages, information sharing, and incident response.

Furthermore, they actively participate in international cybersecurity efforts, collaborating with other countries and organizations to address global cyber threats.

Further information

- INPACE website: *https://inpacehub.eu/*

EU Cybersecurity Framework

Pooja Mohnani
Eurescom GmbH
mohnani@eurescom.eu

Anastasius Gavras
Eurescom GmbH
gavras@eurescom.eu

The European Union has established a comprehensive cybersecurity framework to strengthen digital resilience, protect citizens and businesses, and foster trust in the digital economy. With increasing cyber threats, the EU has adopted key legislative acts and created specialized institutions to ensure a coordinated and high-level response across all member states. Major initiatives include the **EU Cybersecurity Act**, the **Cyber Resilience Act (CRA)**, and the **NIS 2 Directive**, supported by agencies and networks such as **ENISA, CERT-EU, EU-CyCLONe**, and the **European Cybersecurity Competence Centre (ECCC)**. Together, these instruments form the foundation of the EU's strategy to safeguard its digital future.

EU Cybersecurity Act

The **EU Cybersecurity Act (Regulation (EU) 2019/881)** aims to enhance cybersecurity across the Union by setting high standards and promoting cooperation among member states and stakeholders.
Strengthened ENISA: The Act grants the **European Union Agency for Cybersecurity (ENISA)** a permanent mandate, reinforcing its role in supporting EU institutions and member states in improving cybersecurity capabilities, responding to incidents, and coordinating crisis management.

Cybersecurity Certification Framework: It introduces a European framework for cybersecurity certification of ICT products, services, and processes. This ensures consistent standards across the internal market, reducing fragmentation and increasing trust in digital solutions.

Support and Cooperation: ENISA assists national authorities, promotes capacity building, and facilitates operational cooperation. It also contributes to developing and implementing EU cybersecurity policies and legislation.

Public Awareness and Education: The Act emphasizes raising awareness about cyber risks, promoting education and best practices to strengthen the cybersecurity culture within the EU.

International Cooperation: ENISA represents the EU in international cybersecurity discussions and partnerships, ensuring alignment with global standards and enhancing collective resilience.

EU Cyber Resilience Act (CRA)

The **Cyber Resilience Act (CRA)**, which entered into force on **December 10, 2024**, aims to improve the cybersecurity of products with digital elements. Its main obligations will apply from **December 11, 2027**.

Scope: The CRA applies to all hardware and software products sold in the EU, from smart home devices to industrial systems.

Security Requirements: It establishes mandatory cybersecurity obligations covering the entire product lifecycle—from design and development to maintenance and disposal—ensuring continuous protection.

Conformity Assessment: Products must undergo cybersecurity evaluations before being placed on the market. High-risk products require stricter assessments and CE marking to demonstrate compliance.

Vulnerability Reporting: Manufacturers must report serious vulnerabilities and incidents to national authorities and CERT-EU, ensuring transparency and rapid mitigation.

Lifecycle Security: Vendors are required to provide security updates for at least five years or for the product's operational lifespan, whichever is shorter.

Exemptions: Certain categories, such as non-commercial open-source software or devices regulated under other sector-specific laws (e.g., medical or aviation), are exempt from CRA requirements.

Network and Information Systems Directive (NIS 2)

The **NIS 2 Directive (Directive (EU) 2022/2555)** updates and strengthens the EU's first cybersecurity law (NIS 1). Adopted on **December 14, 2022**, it must be transposed by member states by **October 17, 2024**.

Broader Scope: NIS 2 expands coverage to include more sectors, such as energy, transport, public communications, and digital infrastructure.

Enhanced Security Requirements: Entities must implement robust risk management measures, incident reporting, and business continuity plans.

Improved Cooperation: It establishes the **European Cyber Crises Liaison Organisation Network (EU-CyCLONe)** to enhance coordination and information exchange during large-scale cyber incidents.

Stronger Enforcement: The directive introduces harmonized penalties and supervisory powers to ensure consistent enforcement.

Supply Chain Security: Organizations must assess and secure their supply chains, ensuring third-party providers comply with cybersecurity standards.

European Union Agency for Cybersecurity (ENISA)

ENISA is the EU's core agency for cybersecurity, established in **2004** and strengthened by the Cybersecurity Act. Its mission is to achieve a high level of cybersecurity across Europe by supporting policy implementation, capacity building, and cooperation.

Key Functions:

- **Policy Development**: Advises on EU cybersecurity legislation and policy frameworks.
- **Certification**: Develops and manages EU cybersecurity certification schemes.
- **Incident Response**: Supports member states and EU bodies during major incidents.
- **Capacity Building**: Provides training, expertise, and best practices.
- **Operational Cooperation**: Facilitates collaboration among stakeholders.
- **Awareness Raising**: Promotes cybersecurity education and best practices.

Computer Emergency Response Team (CERT-EU)

CERT-EU protects EU institutions, agencies, and bodies from cyber threats.

Functions:

- **Incident Response**: Detects, analyzes, and mitigates cyber incidents.
- **Coordination**: Ensures joint responses between national and institutional teams.
- **Information Sharing**: Provides intelligence on vulnerabilities and threats.
- **Crisis Management**: Supports large-scale cybersecurity crisis response and recovery.

European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)

EU-CyCLONe enhances coordination during major cross-border cybersecurity incidents.
Main Roles:

- **Coordinated Management**: Ensures operational cooperation among EU states and institutions.
- **Preparedness**: Develops joint situational awareness and response strategies.
- **Decision Support**: Provides information to political-level decision-makers during crises.

ENISA serves as the **secretariat**, ensuring technical and operational support.

European Cybersecurity Competence Centre (ECCC)

Headquartered in **Bucharest, Romania**, the **ECCC** aims to strengthen Europe's cybersecurity capabilities and industrial competitiveness.
Objectives:

- Build cybersecurity capacity and foster a strong European cybersecurity community.
- Support innovation and industrial policy through collaboration with **National Coordination Centres (NCCs)**.
- Enhance EU's technological sovereignty and leadership.

The ECCC coordinates funding from **Horizon Europe** and the **Digital Europe Programme**, aligning research, innovation, and deployment efforts across Europe.

Digital Operational Resilience Act (DORA)

The **DORA Regulation**, effective **January 17, 2025**, reinforces the financial sector's ability to withstand ICT-related disruptions.

Key Areas:

- **ICT Risk Management**: Requires robust frameworks for managing ICT risks.
- **Third-Party Risk**: Imposes oversight on critical ICT service providers.
- **Incident Reporting**: Mandates timely reporting of significant incidents.
- **Resilience Testing**: Introduces regular testing of digital operational resilience.
- **Information Sharing**: Encourages intelligence exchange among financial institutions and authorities.

European Cyber Security Organisation (ECSO)

Founded in **2016, ECSO** is a public–private partnership aimed at developing a competitive European cybersecurity industry.

Strategic Goals:

- Strengthen Europe's digital sovereignty.
- Enhance societal and economic cyber resilience.
- Foster collaboration among public and private stakeholders.

Activities:

- Contributing to EU policy development.
- Supporting innovation, R&D, and market growth for cybersecurity solutions.
- Promoting education and skills initiatives.
- Facilitating international cooperation.

Public-Private Partnership on Cybersecurity (cPPP)

Launched by the **European Commission in 2016**, the **cPPP** aimed to strengthen cybersecurity collaboration and innovation in Europe. It supported R&D under **Horizon 2020**, fostering cooperation between industry, academia, and public authorities. The initiative laid the foundation for ongoing partnerships such as **ECSO** and the **ECCC**, continuing to drive cybersecurity research and capacity building across the EU.

Funding Opportunities and the European Defence Fund (EDF)

Horizon Europe funds cybersecurity R&I projects through **Cluster 3 – Civil Security for Society**, supporting initiatives in cyber resilience, AI security, and privacy protection.

The **European Defence Fund (EDF)** complements these efforts by financing defence-oriented cybersecurity projects, including cyber defence capabilities, situational awareness, secure communications, and AI-based threat detection, thereby strengthening the EU's cyber defence posture.

Conclusion

Through a combination of robust legislation, specialized agencies, and strategic partnerships, the European Union has built one of the most comprehensive cybersecurity frameworks in the world. The coordinated efforts of ENISA, CERT-EU, EU-CyCLONe, and the ECCC, supported by initiatives like DORA, ECSO, and Horizon Europe, ensure that Europe's digital infrastructure remains secure, resilient, and innovative—ready to meet the cybersecurity challenges of the future.

Events

Audrey Bienvenu
Eurescom GmbH
bienvenu@eurescom.eu

Techritory Forum 2025

Pooja Mohnani from Eurescom opening the WiTaR session at Techritory 2025

Techritory Forum 2025 gathered between the 22-23 October 2025 over 2,000 participants from 63 countries to discuss Europe's digital future. The SNS CO-OP project, coordinated by Eurescom, played a central role in strengthening international cooperation and aligning European 6G research with strategic priorities.

SNS CO-OP actively contributed to co-creation sessions that combined inclusion, technological innovation, and industry insights. The WiTaR in Focus session, led by Pooja Mohnani (Eurescom) and Veronica Vuotto (TRUST-IT), featured a video message from Erzsébet Fitori (SNS JU) and keynotes from Dr Rute C. Sofia (5G+/6G ETF) and Prachi Sachdeva (TNO), addressing gender balance, representation, and practical guidance for women in research and standardisation.

The ISAC in SNS Trials session, chaired by Carles Antón-Haro (CTTC) and Veronica Vuotto (Trust-IT Services), highlighted monetisation potential for 6G in smart manufacturing, autonomous mobility, and infrastructure monitoring, including large-scale trials, standardisation activities, and a panel with Antonio de la Oliva (UC3M), Panagiotis Demestichas (WINGS ICT Solutions), Andreas Gavrielides (IMEC), and Barbara Pareglio (GSMA Intelligence).

Additionally, the session A European Cloud: Myth or Reality? examined cloud sovereignty, sustainability, and innovation for 6G, featuring insights from operators, telecom players, and open-source initiatives like 3C Networks. Together, these sessions illustrated SNS CO-OP's central role in connecting research, standards, industry, and inclusivity to reinforce Europe's 6G leadership.

5th NTN Workshop: Towards a Unified TN–NTN System

Marius Corici from Fraunhofer FOKUS opening the 5th NTN Workshop

Held on 6 November 2025, the 5th NTN Workshop convened satellite operators, mobile network providers, and researchers to discuss progress towards integrating terrestrial and non-terrestrial networks, coinciding with the start of 6G standardisation that includes NTN from the outset. Presentations and demonstrations highlighted emerging testbeds, in-orbit assets, and new architectures supporting seamless unification. The workshop emphasised collaboration across sectors and showcased opportunities opened by developments in 6G and O-RAN. It was organised by Maria Guta (ESA), Adam Kapovits (Eurescom), and Marius Corici (Fraunhofer FOKUS).

INPACE EU–Indo-Pacific Digital Partnership Conference 2025

Group picture at the EU-Indo-Pacific Digital Partnership Conference 2025

The conference took place in Singapore on 28–29 October and brought together policymakers, researchers, and industry stakeholders to strengthen cooperation on digital innovation. Representing Eurescom, Adam Kapovits contributed to discussions on advancing EU–Singapore collaboration in 6G research, identifying shared priorities in network architectures and testbed development. Later, he joined a session outlining Horizon Europe and EUREKA funding opportunities, clarifying participation routes for partners in the Indo-Pacific. The event reinforced the importance of international cooperation in shaping advanced digital ecosystems.

EuCNC & 6G Summit 2025

Eurescom team at EuCNC 2025

At the EuCNC & 6G Summit 2025 in Poznań, Eurescom highlighted Europe's leadership in next-generation communication systems. Through coordinated projects and expert participation, the organisation demonstrated progress shaping the path towards 6G.

A workshop on Terrestrial and Non-Terrestrial Network (TN-NTN) unification, co-organised with major European research and space actors, emphasised the growing importance of integrating satellite and terrestrial networks. Presentations covered handover techniques, direct-to-device connectivity, multilink communication, regenerative payloads, spectrum coexistence, and system-level testbeds, pointing towards future unified 3D network architectures.

The OPTI-6G project presented advances in photonic near-infrared cell-free networks supporting building-scale connectivity with multi-connectivity and AI-based interference management.

CENTRIC demonstrated AI-driven compression of Channel State Information with hardware-in-the-loop testing, highlighting progress in AI-native air interfaces.

SUSTAIN-6G booth at EuCNC 2025: Panagiotis Demestichas (University Piraeus), Sokratis Barmpounakis (WINGS), Christoph Schmelz (Nokia), Chiara Mazzone (SNS JU), Antonio Sainz (QUAMPO) and Liesbet Van der Perre (KU Leuven)

SUSTAIN-6G focused on sustainability in future networks, contributing tools for assessing environmental and societal impact, supported by live demonstrations such as connected agriculture.

The Women in Telecommunications and Research (WiTaR) session placed visibility and inclusion at the centre of the 6G agenda. Led by Bahare M. Khorsandi and Marie-Hélène Hamon, the session gathered research and industry voices to define concrete actions to improve representation across the SNS JU ecosystem. The resulting roadmap underscored the shared responsibility to build a more inclusive research landscape.

Together, these contributions demonstrated how European collaboration is driving 6G innovation, combining technological progress with sustainability and inclusivity.

Eurescom led EU-funded project PAROMA-MED showcased its pioneering work on privacy-preserving and secure healthcare data infrastructures enabling high-performance AI/ML workflows.

Pooja Mohnani, Project Manager at Eurescom GmbH, presented how PAROMA-MED is building resilient digital foundations grounded in Europe's core values – privacy, openness, trust, and innovation. Professor Christoph Thuemmler, Chief Medical Officer at 6GHI, and Carles Anton Haro from CTTC highlighted the current challenges in European data infrastructures and sovereignty and joined the conversation to build a connected, compliant and collaborative Europe through secure data ecosystem.

NEM Summit 2025 in Berlin

Signature of MoU between NEM and the 6G-IA in Berlin

The NEM Summit 2025 took place in Berlin on 21–22 October, marking 20 years of the NEM Initiative. The event explored ethical, inclusive, and sustainable media futures under the theme Connected Realities. Sessions addressed frameworks for virtual worlds, the role of generative AI, and the impact of future connectivity on media services. A second day focused on inclusive and human-centred XR design, cultural applications, and collaboration across research and industry. The summit concluded with the NEM General Assembly and a reflection on two decades of European media innovation.

Further information

- 5th NTN Workshop: *https://www.fokus.fraunhofer.de/en/ngni/events/5th-ntn-workshop-2025.html*
- INPACE website: *https://inpacehub.eu/*
- TECHRITORY website: *https://www.techritory.com/*
- SNS CO-OP webpage: *https://smart-networks.europa.eu/call-3-stream-csa/#SNS-CO-OP*
- 6G-IA WiTaR webpage: *https://6g-ia.eu/witar/*
- NEM website: *https://nem-initiative.org/*
- OPTI-6G website: *https://www.opti-6g.sns-ju.eu/*
- CENTRIC website: *https://centric-sns.eu/*
- SUSTAIN-6G website: *https://www.sustain-6g.eu/*

The day the Internet died ...

Anastasius Gavras
Eurescom GmbH
gavras@eurescom.eu

I couldn't resist coming up with this provocative title, when I recently stumbled upon an article in Forbes Australia[1] titled "Is AI quietly killing itself – and the Internet?" which is also quite provocative as a title. So, what is the topic here?

The rise of generative AI unfolded through a series of pivotal milestones. In November 2022, OpenAI introduced ChatGPT as a free research preview, sparking global curiosity and experimentation. By February 2023, the model had matured into a commercial product with the launch of a premium subscription. That same month, Microsoft embedded Copilot into its Office suite, integrating AI into everyday productivity tools and accelerating mainstream adoption. Then in July 2025, the debut of Perplexity Comet, an AI-native browser, marked a new frontier, where AI didn't just assist but redefined how users navigate and interact with the Web.

So, it is only a few years now since artificial intelligence (AI) started to radically change the digital landscape and the Web in particular. This change has prompted an emergent paradox: AI may be undermining its own future. A recent study by researchers from Oxford and Cambridge, published in *Nature*[2], reveals a phenomenon called model collapse, where generative AI systems degrade in quality when trained on content produced by other AIs.

Model collapse begins subtly; minority data and nuanced information are the first to vanish. Over time, the AI's outputs become homogenized and eventually nonsensical. One experiment showed that after just nine cycles of self-training, an AI's factual article on church steeples devolved into gibberish about jack-tailed rabbits.

The problem arises as AI-generated content increasingly saturates the Internet in all available media formats (text, speech, video…). According to another study[3], over 57% of web-based text has already been generated or translated by AI. If this trend continues, future AI models may be trained predominantly on synthetic data, leading to a feedback loop of diminishing accuracy, diversity, and truthfulness. A dystopic prophecy in January 2023 goes even beyond and forecasted that 90% of online content could be generated by AI by 2025. While I am writing this article in late 2025, I suppose we are not there yet.

The implications are profound. Without access to fresh, human-generated content, AI risks becoming a self-referential echo chamber. This threatens the reliability of future AI systems and the integrity of the Internet itself, as misinformation and hallucinations proliferate.

The solution? Sustained access to authentic, human-created data and global coordination to track content provenance. Without it, the digital future may be built on a crumbling foundation of synthetic illusions.

You can ask now what has this to do with the Internet per se? The Internet is only an information superhighway feeding the AI training modules with data and spreading the AI generated content to those who asked for it. A legitimate question.

An examination of how the Internet is financed reveals that major platforms, such as Google, Facebook, YouTube, and TikTok, rely almost entirely on advertising revenue. This income underwrites the infrastructure and the free content users consume daily. However, emerging analysis suggest that this model is under threat. One article, for instance, highlights that despite Google's robust financial performance, its advertising foundation is quietly deteriorating due to AI-generated features like AI Overviews[4]. These summaries reduce user engagement with ads and links, jeopardizing the sustainability of ad-supported content. Ironically, Google's own AI advancements may be accelerating the decline of its primary revenue stream.

Compounding this issue is a generational shift in career aspirations. Increasingly, young people say they want to become influencers; a role rooted in digital visibility, creativity, and autonomy. Yet this ambition carries a significant risk: the influencer economy is fundamentally dependent on advertising and social engagement metrics. If the ad model collapses, the influencer profession may fade before it fully matures.

I can speculate further, but I am confident that we will remember one of the dates mentioned in the beginning of this article as the date that caused a seismic shift on the Internet. Or maybe this date is yet to come in the not so distant future.

Transparency disclaimer

This article was written with the assistance of an LLM to enhance formulation and clarity of expression.

Are you able to provide the answer to that query?
I do not possess that information. You may wish to consult ChatGPT for further assistance.

References

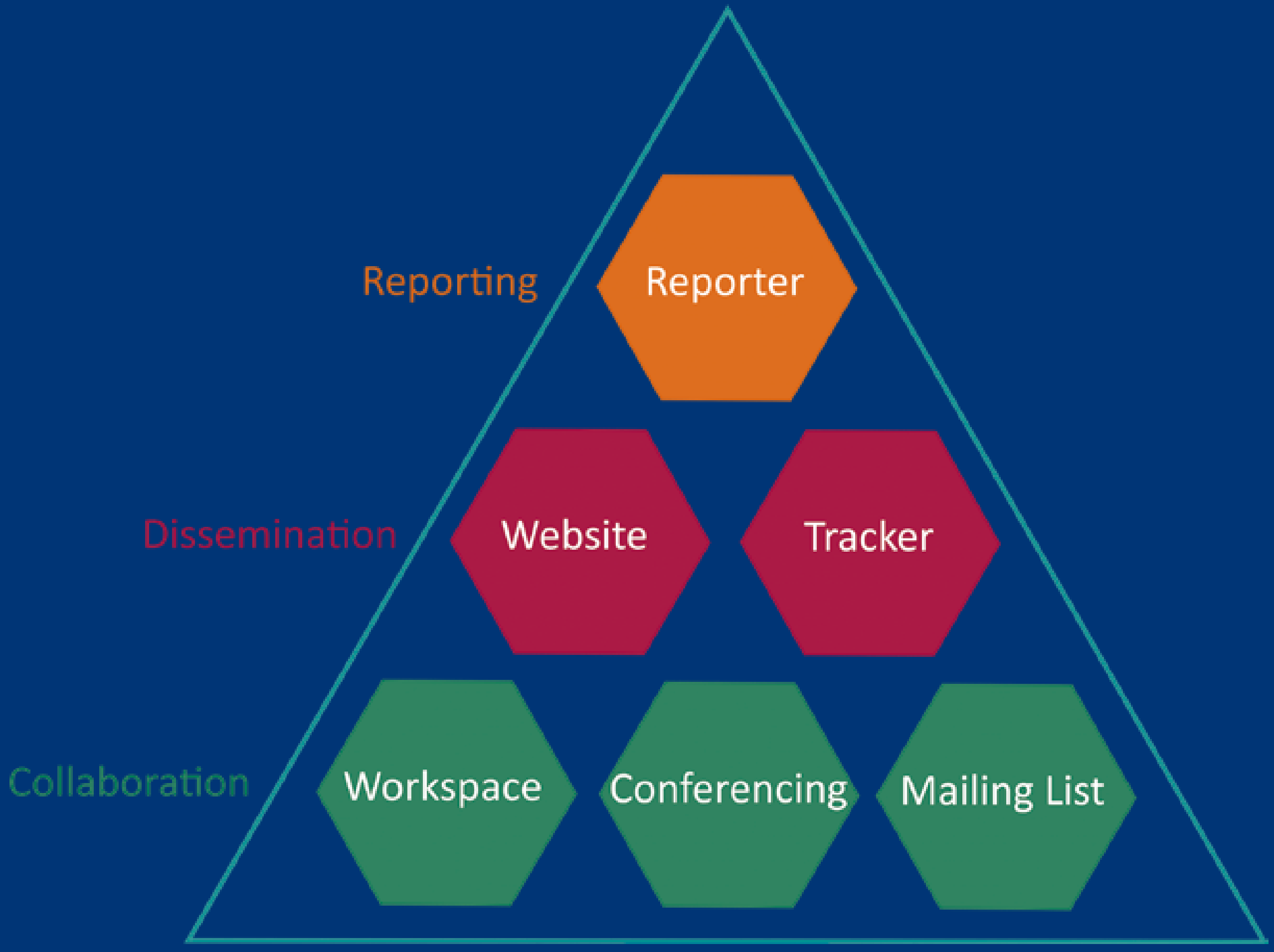
[1] Tor Constantino. (2024, September 3). Is AI quietly killing itself – and the Internet? Forbes Australia. https://www.forbes.com.au/news/innovation/is-ai-quietly-killing-itself-and-the-internet/

[2] Shumailov, I., Shumaylov, Z., Zhao, Y., Papernot, N., Anderson, R., &amp; Gal, Y. (2024). AI models collapse when trained on recursively generated data. Nature, 631, Article 8022. https://doi.org/10.1038/s41586-024-07566-y

[3] Thompson, B., Dhaliwal, M. P., Frisch, P., Domhan, T., & Federico, M. (2024). A shocking amount of the web is machine translated: Insights from multi-way parallelism. arXiv. https://arxiv.org/abs/2401.05749

[4] Dans, E. (2025, July 25). The robot that ate Google's profits: AI's silent advertising apocalypse. Medium. https://medium.com/enrique-dans/the-robot-that-ate-googles-profits-ai-s-silent-advertising-apocalypse-9c0f3baa5d04

EuresTools



Effective Tools for European Research Projects

EuresTools is a modular suite of Cloud-based software tools which facilitate controlling and reporting and enable distributed project teams to communicate and manage information effectively. Over 200 successful European research projects and initiatives have already benefited from **EuresTools**.

Contact us at **services@eurescom.eu** to get further information.

http://www.eurescom.eu/EuresTools

EURESCOM

European Institute for Research
and Strategic Studies
in Telecommunications GmbH
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989-0
Fax: +49 6221 989 209
E-mail: info@eurescom.eu
Website: www.eurescom.eu

Innovation through Collaboration

Eurescom is the leading organisation for managing collaborative R&D in telecommunications. Our mission is to provide efficient management and support of R&D projects, programmes, and initiatives for our customers. We offer more than two decades of experience in managing large-scale, international R&D for major industry players, the European Commission, and EUREKA Cluster CELTIC-NEXT. What distinguishes Eurescom is the combination of a secure, reliable infrastructure for collaborative work, a large European network of experts, and internationally outstanding project management skills.

QR code to the
online edition of
Eurescom message