

Cybersecurity

Authors

Anna Gerasymenko (Leiden University), Martine Groen (Hogeschool Utrecht),
Mick Deben (MBO Digitaal), Rob Gerritsen (formerly Graafschap college),
Nicole van der Meulen (SURF)



1. Emerging dual-use of AI in cybersecurity

2. More accessible privacy-enhancing technologies to share data

3. Rising pressure to prepare for post-quantum cryptography

4. Emergence of measures for secure Internet of Things

5. The growing need for security protocols to work in the cloud

Introduction

The field of cybersecurity has advanced significantly since computer programmer Bob Thomas created the Creeper virus in 1971. Although this virus, which targeted the Advanced Research Projects Agency Network (ARPANET), was not a malicious virus, it marked an important moment in cybersecurity history. Over 50 years later, cyber attacks have grown increasingly malicious and become a significant threat to society.

Technologies, such as Artificial Intelligence (AI) and Internet of Things (IoT), bring new challenges and risks that must be addressed to maintain robust cybersecurity. For example, although AI can help improve defences against cyber attacks, it can also increase the threat by enabling automated malware.

While these digital technologies expose organisations to new threats, they are

also becoming increasingly essential for organisations to manage and protect themselves. For instance, quantum computing will enable the implementation of complex and potentially very secure cybersecurity protocols. Such technologies offer significant opportunities for both individuals and organisations.

Despite these technological advancements, it remains crucial to stay vigilant about potential threats. Understanding the tools and techniques used by cybercriminals and knowing how to secure yourself and your organisation is essential for maintaining (cyber)resilience. In recent years, incidents within the education sector have highlighted the significant damage that can result from a seemingly harmless click by a so-called patient zero.

An understanding of how technologies can and could potentially shape the future of cybersecurity is essential. Therefore, this chapter has been included in the SURF Tech Trends to explain how new threats are emerging and to highlight the opportunities arising from technologies that have become integral to daily life. As society grows increasingly reliant on digital systems, cybersecurity and cyber resilience have become vital components of organisational strategy and operations. Organisations must focus on protecting (sensitive) data, complying with evolving policies and regulations (such as the EU Cyber Resilience Act), addressing the vulnerability of IoT devices to malicious attacks or unauthorised control, and mitigating emerging threats.

Contributors

Zeki Erkin (TU Delft), **Jeroen van der Ham - de Vos** (University of Twente)

TREND #1

Emerging dual-use of AI in cybersecurity

Public Values

	Autonomy	Privacy
	Justice	Integrity Accountability Transparency
	Humanity	Safety

Maturity

- WATCH
- PLAN
- ACT

Drivers

Automation & AI; Cybersecurity & trust; Engineering advances & computation; Value of knowledge & skills; Weaponisation of knowledge; Digital transformation

AI is transforming cybersecurity by improving real-time threat detection and efficient responses against these threats. AI models can analyse large datasets and data streams, identify anomalies, and predict attacks, making them a critical tool for security operations.

However, cybercriminals are also exploiting AI to improve their attacks. Techniques like AI-driven phishing, deepfakes, and automated vulnerability scanning are making cyberattacks more convincing and scalable. Rising concerns are developments on the deployment of GenAI to generate malware with minimal input and adversarial machine learning. Attackers are manipulating data to deceive AI models – such as those used for cyber defence – causing the models to overlook threats.



SIGNALS

Rise of offensive AI capabilities

Cybercriminals are leveraging large language models to craft context-specific phishing content and social engineering scripts

- **Phishing and social engineering in the age of LLMs** (link.springer.com) [🔗](#)
- **Back to the hype: an update on how cybercriminals are using GenAI** (ibm.com) [🔗](#)
- **With generative AI, social engineering gets more dangerous—and harder to spot** (ibm.com) [🔗](#)
- **Could cyberattacks ‘turn the lights off’ in Europe?** (knowbe4.com) [🔗](#)

AI-generated deepfakes are increasingly used in identity fraud and disinformation campaigns

- **How deepfakes, disinformation and AI amplify insurance fraud** (swissre.com) [🔗](#)
- **A pro-Russia disinformation campaign is using free AI tools to fuel a ‘content explosion’** (wired.com) [🔗](#)
- **The dark side of AI: how deepfakes and disinformation are becoming a billion-dollar business risk** (forbes.com) [🔗](#)

“You can see that AI can help both attackers and defenders in cybersecurity. But the main focus remains on getting the basics right, with AI as a tool.”

- Jeroen van der Ham - de Vos, University of Twente

Open source generative models are enabling low-resource actors to create evasive malware and automate attacks

- **Prediction for open source security in 2025: AI, state actors and supply chains** (openssf.org) [🔗](#)
- **OpenAI confirms threat actors use ChatGPT to write malware** (bleepingcomputer.com) [🔗](#)
- **How generative AI is changing how cybercrime gangs work** (bugcrowd.com) [🔗](#)

SIGNALS

Defensive AI integration in cybersecurity operations

AI-powered Security Operations Centres (SOCs) use machine learning to automate threat detection, reduce alert fatigue, and speed up incident response

- **IBM Security, cost of a data breach report** (cloudfront.net) [↗](#)
- **Microsoft Security Copilot insights** (microsoft.com) [↗](#)

Behavioural analytics and predictive AI models identify anomalies and pre-empt threats before they escalate into attacks (of any scale)

- **Transforming SOCs with AI: From Reactive to Proactive Security** (cloudsecurityalliance.org) [↗](#)

Network & Extended Detection and Response (NXR/XDR) platforms integrate AI to provide real-time attack correlation, autonomous triage, and adaptive defence

- **Microsoft - What is extended detection and response (XDR)?** (microsoft.com) [↗](#)
- **Vectra.ai** (vectra.ai) [↗](#)

Mitigating adversarial AI risks

Cyber defenders use adversarial training and robust model tuning to harden AI systems against manipulation and input poisoning.

- **NIST AI risk management framework** (nist.gov) [↗](#)
- **MITRE ATLAS Framework** (atlas.mitre.org) [↗](#)

AI red teaming and model auditing are increasingly adopted to identify vulnerabilities in machine learning pipelines before attackers exploit them.

- **Anthropic: challenges in red teaming** (anthropic.com) [↗](#)
- **Microsoft Red Team** (learn.microsoft.com) [↗](#)

Threat intelligence platforms now incorporate adversarial AI detection modules to flag synthetic media, spoofed behaviour, and tampered datasets

- **Recorded Future** (recordedfuture.com) [↗](#)
- **Darktrace** (darktrace.com) [↗](#)
- **TNO and Jungle AI collaborate to detect cyberattack on wind turbine and improve detection capabilities** (tno.nl) [↗](#)



IMPACT



Education

AI tools offer the potential to secure online learning environments through anomaly detection and behavioural analytics. However, the misuse of AI can undermine educational integrity through automated cheating, deepfakes, or phishing. Securing AI in education requires balancing innovation with ethical and regulatory safeguards.



Research

Research institutions benefit from AI for advanced threat modelling, data protection, and network monitoring. However, open access policies and collaborative research environments also increase exposure to AI-driven threats. Robust model governance and adversarial resilience are key to maintaining research integrity.



Operations




As institutions digitalise, integrating AI into cybersecurity infrastructure enhances real-time response and reduces reliance on manual oversight. Yet, AI systems themselves are then becoming high-value targets. Institutions must build secure AI pipelines and invest in threat-informed AI deployment strategies to ensure long-term operational security.



TREND #2

More accessible privacy-enhancing technologies to share data

Public Values

	Autonomy	Privacy
	Justice	Integrity Equity Transparency Accountability
	Humanity	

Maturity

- WATCH
- PLAN
- ACT

Drivers

Compliance & regulation: Cybersecurity & trust;
Automation & AI; Individualisation & empowerment;
Digital transformation; Value of knowledge & skills

Privacy-enhancing technologies (PETs) protect sensitive information while enabling secure data processing and sharing. The adoption of PETs – such as differential privacy, synthetic data sets to resemble real sensitive data, federated learning, and homomorphic encryption – is being driven by growing data demands in education and research due to the sensitivity of data.

The recent availability of sector-specific solutions has made PETs more accessible, promising to unlock privacy-focused multi-party data sharing and analytics through research initiatives and private/public collaborations.

Embedding PETs into IT architectures will complement traditional security-by-design approaches with data-centric controls, reducing organisational vulnerability exposure, and defending against unauthorised access.



SIGNALS

Growth of synthetic data solutions

Information systems audit and control association (ISACA) (isaca.org) [↗](#)

Researchers at Erasmus University are being encouraged to use AI-driven synthetic data generated by Syntho Engine (2023) (syntho.ai) [↗](#)

Utrecht University has developed the MetaSyn platform for anonymised and FAIR data publishing (uu.nl) [↗](#)

Dienst Uitvoering Onderwijs (DUO) has shared synthetic datasets with Dutch researchers to train research models and help improve the education system (duo.nl) [↗](#)

TNO PET Lab aims to facilitate and spread the use of PETs in innovation (tno.nl) [↗](#)

Federated and secure data analytics piloting

SPATIAL (TU Delft) set to integrate PETS to achieve trustworthy, transparent, and explainable AI solutions for cybersecurity (spatial-h2020.eu) [↗](#)

Amsterdam University Medical Centre applies Federated Analytics to collaboratively develop predictive models for ICU outcomes (amc.nl) [↗](#)

In the Netherlands, the Social Insurance Bank (SVB) and the Employee Insurance Agency (UWV) successfully explore Multi-Party Computation (MPC) at the National Innovation Centre for Privacy-Enhancing Technologies (NICPET) (tno.nl) [↗](#)

PETs in cross-border data sharing

Calls for Federated Infrastructure for intensive care units data across Europe (doi.org) [↗](#)

EU Safe-DEED consortium project set to offer PETs for data marketplaces

- eurecat.org [↗](#)
 - tudelft.nl [↗](#)
-

Dutch HERACLES project lays foundation for secure private-public data sharing in healthcare sector (tno.nl) [↗](#)

IMPACT



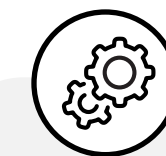
Education

As education digitises, PETs will be crucial for securing student and staff data in online learning environments. Using cryptographic techniques and federated learning, PETs address privacy and security concerns in learning analytics, mitigating risks, and fostering trust amongst students and teachers in adaptive, data-driven, or personalised education systems.



Research

PETs empower researchers with secure access to sensitive or distributed datasets, mitigating privacy, reputation, and strategic risks associated with data sharing. While these technologies promise greater confidence in innovative research, they also increase pressure on institutions to facilitate them with supporting IT infrastructure.



Operations




As educational institutions adopt emerging (AI, edge computing) and maturing (cloud computing) technologies, the need for robust digital trust and data-centric security is intensifying. PETs will become essential towards achieving reliable and transparent security solutions, determining future IT security and regulatory compliance. PETs maturity and interoperability will support sector-wide implementation.



TREND #3

Rising pressure to prepare for post-quantum cryptography

Public Values

	Autonomy	Privacy
	Justice	Integrity Accountability Sustainability
	Humanity	Safety

Maturity

WATCH

PLAN

ACT

Drivers
Engineering advances & computation; Cybersecurity & trust; Automation & AI; Compliance & regulation; Critical infrastructure; Digital transformation

Once quantum computers reach sufficient scale, traditional cryptographic systems, which are used in digital signatures and secure communications, will be extremely vulnerable to attack.

Many of our current infrastructures lack crypto-agility, which slows transitions to robust cryptographic systems and leaves them exposed to Store Now-Decrypt Later (SNDL) threats. Most organisations are or will be exposed to these decryption threats, and their data (communication) protection readiness hinges on adopting Post-Quantum Cryptography (PQC).

Currently, the US agency NIST has released standards for PQC encryption and is encouraging system administrators to begin transitioning as soon as possible. In addition, European initiatives such as the European Quantum Communication Infrastructure (EuroQCI) seek to build secure communication networks using quantum key distribution (QKD), enabling and accelerating the distribution of cryptographic keys.



SIGNALS

Post-quantum cryptography standardisation

NIST releases first 3 finalised post-quantum encryption standards (nist.gov) [↗](#)

NIST standardises quantum-safe cryptography methods (cwi.nl) [↗](#)

“Store now, decrypt later” strategy

State actors are already collecting encrypted data for future decryption with quantum computers, as part of the “store now, decrypt later” approach (enisa.europa.eu) [↗](#)

National government’s quantum security initiatives

The Dutch National Cybersecurity Centre (NCSC) and AIVD are leading efforts to prepare organisations for quantum threats, advising on mapping encryption use and transitioning to quantum-safe technologies (ncsc.nl) [↗](#)

Next steps National Cyber Security Centre (UK): Preparing for Post-Quantum Cryptography (ncsc.gov.uk) [↗](#)

Support for crypto-agility

PQC Handbook - Evaluate and plan for a seamless migration to post-quantum cryptographic systems (aivd.nl) [↗](#)

EuroQCI project: building quantum-secure communications

The European Quantum Communication Infrastructure (EuroQCI) project aims to establish a secure communication network across Europe using quantum key distribution (QKD), ensuring long-term protection against quantum threats (digital-strategy.ec.europa.eu) [↗](#)

IMPACT



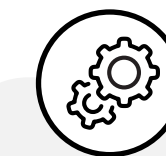
Education

- Post-quantum security breaches are possible due to open IT environments, dependence on third-party cloud providers, and the long retention of confidential data.
- Identities could be compromised, with the exposure of gradebooks, assessments, or personal info.
- Archived teaching content, communications, or certification records could be forged or altered.



Research

- “Store now, decrypt later” is a significant threat to research confidentiality. Data such as genetic records and AI models intercepted today could be decrypted years later, exposing proprietary or sensitive findings.
- Research partners may hesitate to share data or collaborate if quantum-insecure systems are in use, leading to a breakdown in trust-based collaboration.
- Universities involved in patentable or commercially relevant research could lose a competitive advantage in the event of intellectual property theft.
- Failure to secure data may lead to funding body restrictions or non-compliance with ethical and legal requirements.






Operations

The emerging risk of quantum computers eventually breaking today’s encryption algorithms is already prompting “store now, decrypt later” tactics by state-affiliated actors, targeting data with long-term sensitivity. Therefore, key PQC infrastructure must be established. Without early PQC action in terms of policy and infrastructure funding, institutions risk long-term data exposure and eroded trust.

TREND #4

Emergence of measures for secure Internet of Things

Public Values

	Autonomy	Privacy
	Justice	Accountability Integrity
	Humanity	Safety

Maturity

- WATCH
- PLAN
- ACT

Drivers

Connectivity & interaction; Cybersecurity & trust; Digital transformation; Compliance & regulation; Critical infrastructure; Individualisation & empowerment

The Internet of Things (IoT) is here to stay, and it is revolutionising industries by improving efficiency and providing more insights. Yet, it faces significant security challenges and risks related to, for example, identification, authentication, and ownership of ‘smart’ devices, such as autonomous drones.


Over the last decade, IoT developers and vendors have neglected their responsibility for security updates throughout the product lifetime, creating cybersecurity gaps within organisations.

To mitigate such risks, security solutions, such as endpoint protection, are being developed. In addition, new legislation, like the Cyber Resilience Act, will force IoT developers and vendors to include security updates for any product’s lifetime.




SIGNALS

IoT devices are being integrated into day-to-day practices


IoT devices can be found and are increasing across all verticals and supply chains, in their integration in day-to-day practices, be it in the hospital, the factory, or at home
(demandsage.com) 

The EU Cyber Resilience Act (CRA), effective 2024
(digital-strategy.ec.europa.eu) 

IoT security has its own specific security

A review of multi-factor authentication in the Internet of Healthcare Things (doi.org) 

UTwente opened an IoT Cyberlab (utwente.nl) 

Edge AI: connecting cloud and devices for safe, sustainable AI (doiotfieldlab.tudelftcampus.nl) 

Practical actions and guidelines

Tips from the Dutch National Cybersecurity Centre (ncsc.nl) 

Guidelines for Securing the Internet of Things
(enisa.europa.eu) 

IMPACT



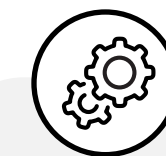
Education

Professional degrees like system engineering integrate IoT and its security aspects into the curriculum. However, the application of IoT in educational methods focuses less on digital technology, such as providing instant feedback. Enabling personalised learning remains limited.



Research

- The secure implementation of IoT can also contribute to the collection of data for scientific research (e.g. via devices and wearables).
- IoT and the security of IoT is being investigated in a wide variety of applications with higher education research institutions. This includes, for example, privacy-preserving and secure protocols for healthcare wearables (IoMedicalT), smart traffic management systems, and developing models that detect and classify IoT attacks.



Operations




IoT is often overlooked by IT security operations, despite the significant increase of its attack surface area. It is therefore important that IT security operations regain control of their hidden IoT assets, facilitate the use of secure IoT, as well as educate their employees and students about the security risks associated with IoT interactions (awareness). Institutions are advised to isolate IoT networks, use dedicated servers, and implement governance frameworks to ensure secure IoT adoption.



TREND #5

The growing need for security protocols to work in the cloud

Public Values

	Autonomy	Privacy
	Justice	Integrity Accountability Transparency
	Humanity	Safety

Maturity

- WATCH
- PLAN
- ACT

Drivers

Automation & AI; Engineering advances & computation; Cybersecurity & trust; Digital transformation; Service-oriented & value-based economies; Value of knowledge & skills


Cloud computing offers unprecedented scalability, flexibility, and cost efficiency; however, the widespread adoption of cloud services introduces significant cybersecurity challenges. These challenges stem from shared provider-user responsibilities, an expanded attack surface, reliance on third-party vendors, and a lack of transparency in software and hardware.

Additionally, AI integration complicates security and privacy concerns. Hybrid cloud setups require robust security practices, like zero-trust architectures, continuous monitoring, and strong encryption.



SIGNALS


European and national alternatives for cloud services

Start Next Cloud pilot: seventy researchers across five Dutch universities (communities.surf.nl) 

Rotterdam, Utrecht University, and Tilburg University will collaborate (voxweb.nl) 

Dutch government committed to Dutch sovereign cloud for sensitive information

- security.nl 
- open.overheid.nl) 

EU FED Cloud which complies with relevant EU regulations such as the Data Act, AI Act, GDPR, eIDAS, DORA, and EUCS (eufedcloud.eu) 

EOSC EU Node (open-science-cloud.ec.europa.eu) 

European legal developments

NIS2 directive into force, including in the higher education sector (business.gov.nl) 

EU regulation Cyber Resilience Act (CRA) (eur-lex.europa.eu) 

IMPACT



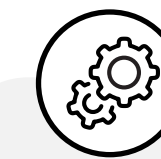
Education

- Other ways of working with cloud computing technology evolve, such as switching between cloud providers and/or solutions, including addressing cybersecurity aspects. It is expected that the importance of data sovereignty and sovereignty in general will become more integrated into curricula.
- Revisions in IT education curricula could help to address the critical skills of cybersecurity professionals.



Research

- Due to a shortage of cybersecurity professionals, a lack of skilled personnel can leave research environments exposed to cyber threats, potentially affecting the integrity of research workflows and outcomes. To mitigate this, cybersecurity awareness training for researchers could be investigated.
- Shared responsibilities can lead to data breaches or loss, particularly if researchers are unaware of security protocols.
- Researchers must navigate various regulations regarding data protection and privacy, which can be complicated by cloud environment.



Operations

- As cloud adoption continues to rise, careful planning and enhanced security measures are essential for institutions to protect sensitive data, ensure compliance, and maintain resilience in an evolving threat landscape. There will also be a large impact due to (data) migrations and the associated steps, such as preparation, awareness, and costs. The adoption of open-source software (OSS) is also expected to increase.
- While hybrid clouds offer flexibility, they necessitate advanced security practices, which may be challenging for some research institutions to implement effectively.

SURF Utrecht

Hoog Overborch Office Building (Hoog Catharijne)
Moreelsepark 48
3511 EP Utrecht
+31 88 787 30 00

SURF Amsterdam

Science Park 140
1098 XG Amsterdam
+31 88 787 30 00

futuring@surf.nl
www.surf.nl/en