R&E Threat Landscape (2026+?)

Roderick Mooi

GÉANT Association

(on behalf of Threat Landscape workshop contributors)

Top 10 Threats for R&E?

"The research and academia sector … ranked among the top targets for threat actors due to its high-value IP, decentralized infrastructure, and expansive digital footprint."

– Microsoft Digital Defense Report 2025

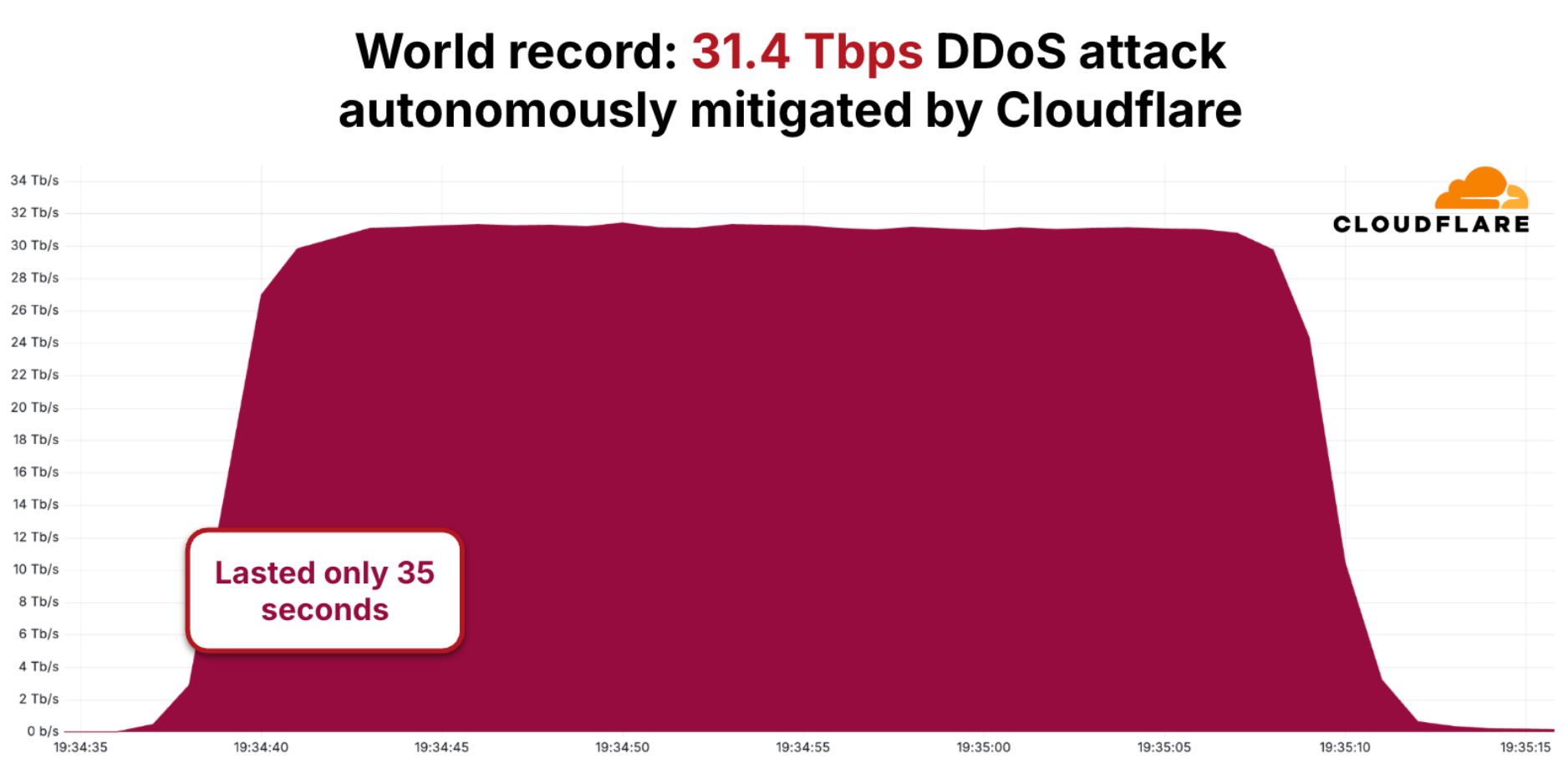
10. Lack of Contingency Plans

- Makes us more vulnerable to the rest of the threats...

→ Crisis exercises

→ Good cyber hygiene

9. DDoS Attacks

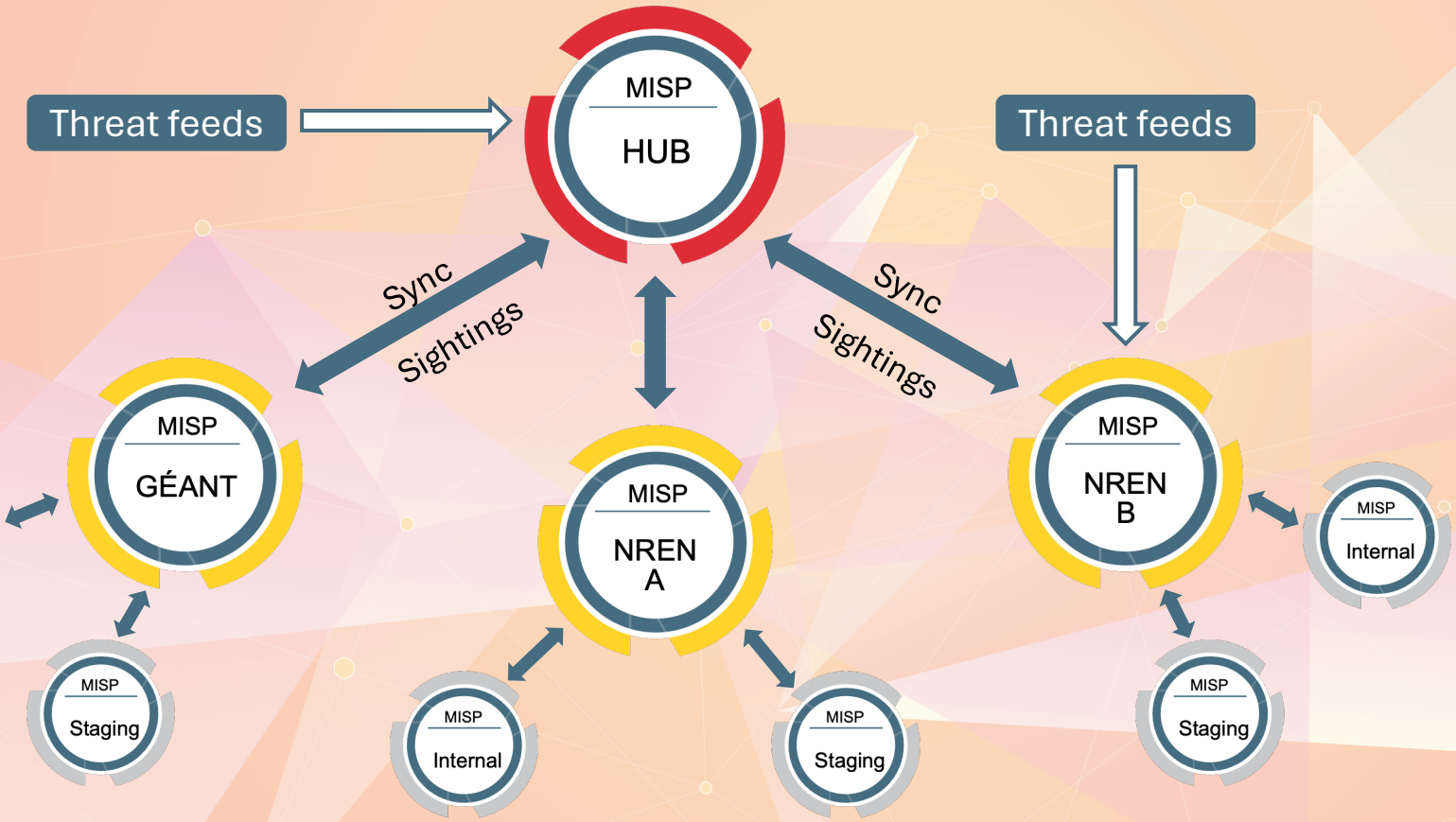


Hint: Join the GÉANT DDoS Working Group (also the workshop this afternoon in Mission 2!)

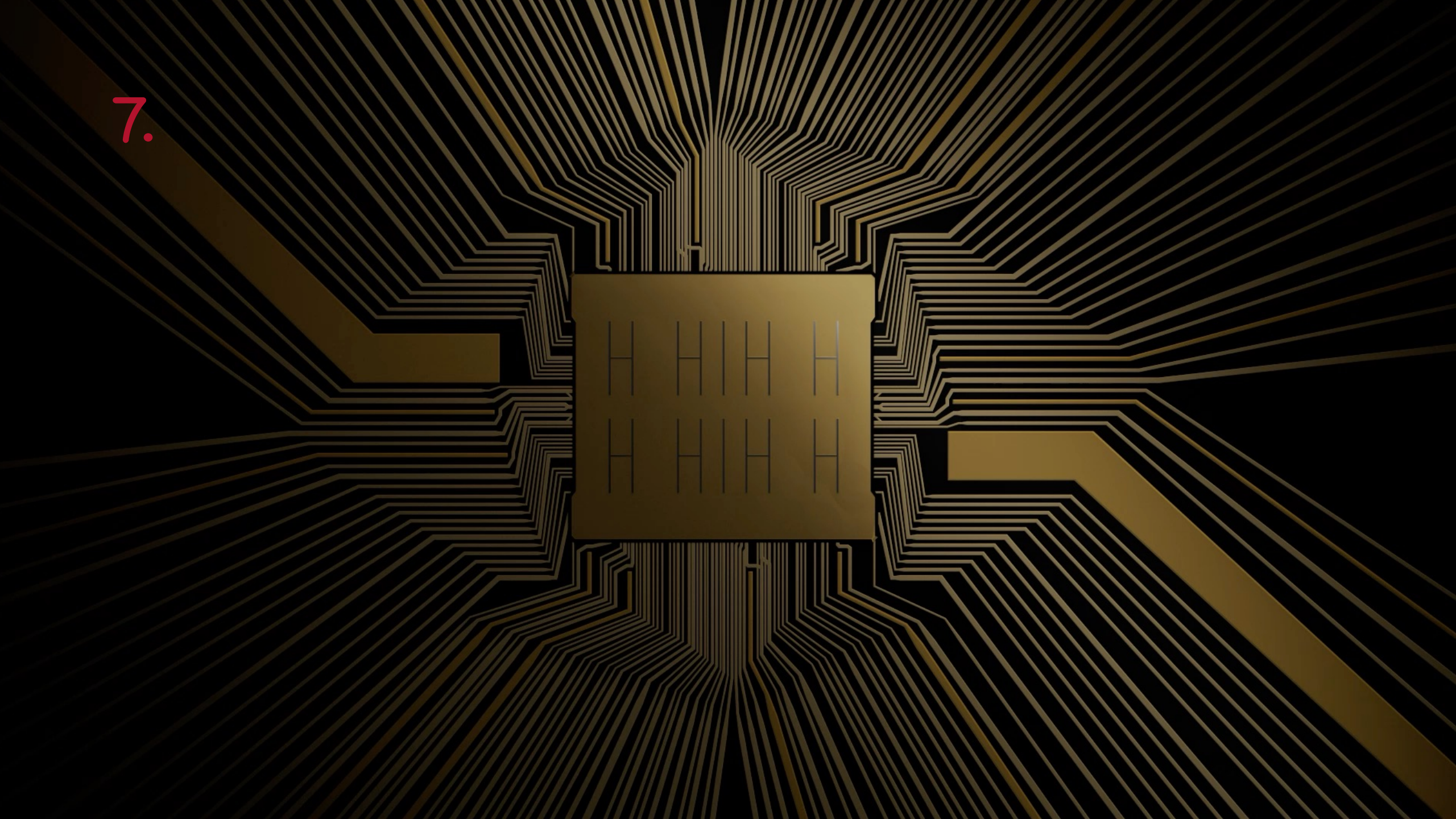
8. Not sharing

- Missing data
- Reputation
- Resources
- Too late

→ R&E Cyber Hub



7.



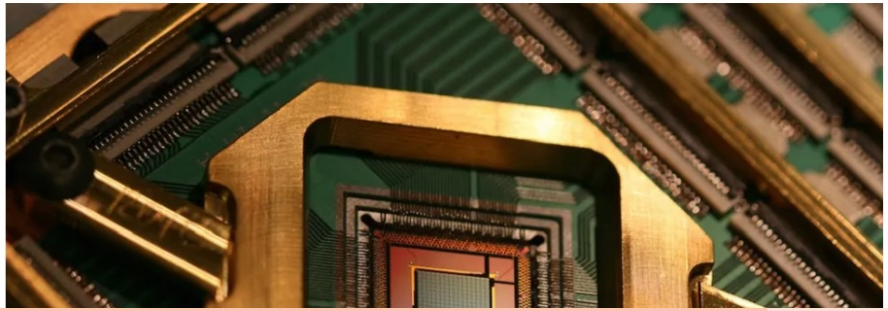
7. Quantum Computers

- Cryptographically Relevant Quantum Computers (CRQCs)
- Store now; decrypt later
- Assymetric cryptography broken (Shor); symmetric weakened (Grover)
- Lack of urgency and uncertainty about timelines

Chinese scientists use quantum computers to crack military-grade encryption — quantum attack poses a "real and substantial threat" to RSA and AES

News By Mark Tyson published October 14, 2024

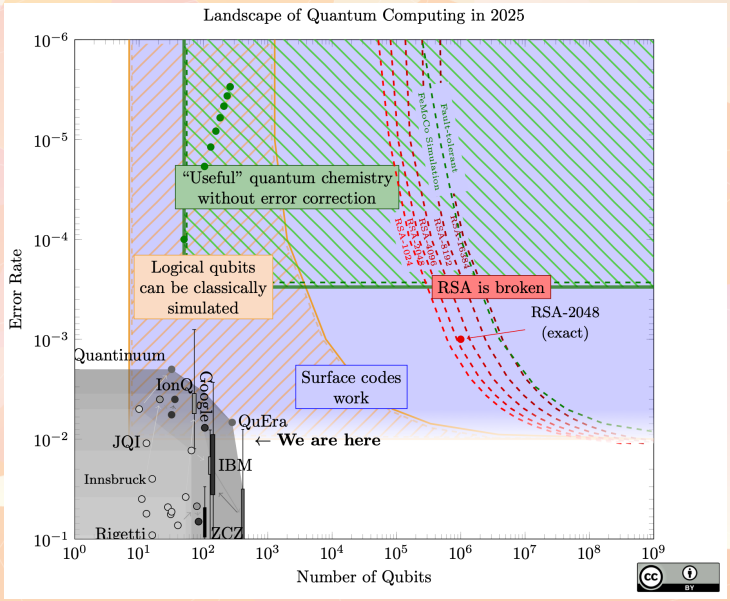
Claim an effective attack on widely used encryption algorithms.



EU Commission Roadmap Targets 2030 for Post-Quantum Cryptography Transition

Marin Ivezic · June 24, 2025 · 4 minutes read

https://postquantum.com/quantum-policy/eu-pqc-roadmap/



https://sam-jaques.appspot.com/quantum_landscape

https://www.tomshardware.com/tech-industry/quantum-computing/chinese-scientists-use-quantum-computers-to-crack-military-grade-encryption-quantum-attack-poses-a-real-and-substantial-threat-to-rsa-and-aes

arXiv > quant-ph > arXiv:2603.28627

Quantum Physics

[Submitted on 30 Mar 2026]

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain, Qian Xu, Robbie King, Lewis R. B. Picard, Harry Levine, Manuel Endres, John Preskill, Hsin-Yuan Huang, Dolev Bluvstein

• Store now; decrypt later

Caltech Team Sets Record with 6,100-Qubit Array

September 24, 2025

INTERESTING ENGINEERING

Subscribe Sign In

NEWS VIDEOS ENERGY SCIENCE MILITARY HEALTH TRANSPORTATION SPACE INNOVATION

Quantum advance cuts qubit needs from 1000 to 5, brings practical computing closer

Caltech researchers reduce qubit needs, speeding up path to fault-tolerant quantum computers

to crack military-grade encryption — quantum attack poses a "real and

POSTQUANTUM

Home / Research News / The 1,000-Qubit Ceiling That Probably Isn't

Research News

The 1,000-Qubit Ceiling That Probably Isn't

"Useful" quantum chemistry without error correction

FORBES DIGITAL ASSETS

Google Finds Quantum Computers Could Break Bitcoin Sooner Than Expected

By Javier Bastardo, Contributor. Javier Bastardo is a Venezuelan covering Bi... Follow Author

Published Mar 31, 2026, 08:53am EDT

Number of Qubits

https://www.tomshardware.com/tech-industry/quantum-computing/chinese-scientists-use-quantum-computers-to-crack-military-grade-encryption-quantum-attack-poses-a-real-and-substantial-threat-to-rsa-and-aes

7. Quantum Computers

→ Crypto inventory + migration evaluation

→ Upgrade TLS libraries with quantum-safe ciphers (min. TLS 1.3)

→ Use browsers with (hybrid-) PQC support

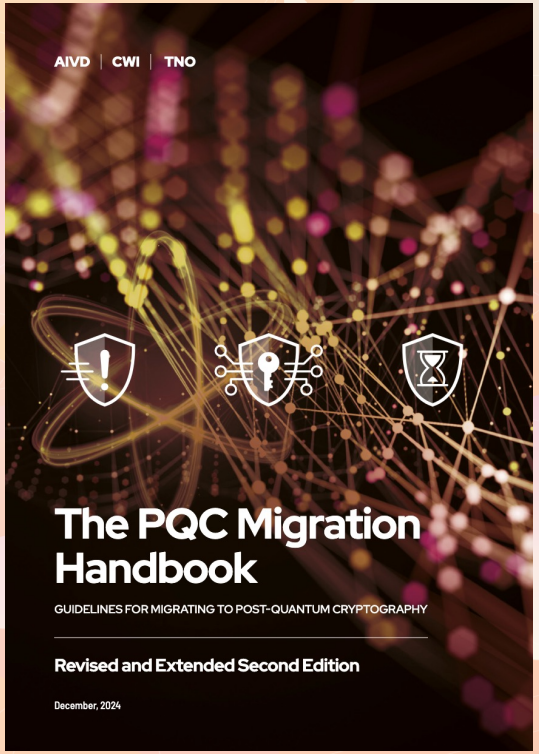
Google Security Blog

Cultivating a robust and efficient quantum-safe HTTPS

February 27, 2026

Firefox Release Notes

Future-ready encryption: Added support for ML-KEM (mlkem768x25519) in TLS 1.3 and HTTP/3, a next-generation approach built to defend against future quantum attacks.



https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook

In Focus • Network • Security

Quantum security moves closer: CESNET validates a new generation of data encryption

4 months ago

6. Insider Threat / Decision Making

- HR and hiring
- IP theft
- More pressure, less people: bad decisions. Managers want more AI, leading to less critical thinking.
- "75% of insider incidents are non-malicious, with negligence and compromised credentials accounting for the majority" – Ponemon Institute 2025 report
- "In R&E, high turnover, extensive third-party collaboration, and structural shadow IT compound these conditions considerably"

→ Secure By Design + → Support Secure Behaviour

5. Social Engineering ++

- "Rather than exploiting technical vulnerabilities, attackers target people"
- Voice cloning and deep fakes
- Targeted phishing
- No more language issues/spelling mistakes
- PhaaS kits, ClickFix, FileFix

→ GÉANT *Be Mindful. Stay Safe.* Campaign

→ https://security.geant.org/awareness/

4. Geo Politics (incl. APTs/nation states)

- IP theft
- Hybrid warfare / pre-staging; Trade wars?
- Political agendas, Hacktivists, Extremists
- Transnational Repression, Censorship
- Russia/Ukraine (e.g. NoName057(16)) → DDoS
- Middle East (e.g. Handala Hack Team)
- Chinese ATPs (e.g. Salt Typhoon)
- Linked to:
  - Quantum
  - Supply chain (e.g. SolarWinds), Wipers
  - Insider threats

https://pngimg.com/download/77545

CYBER THREAT INTELLIGENCE REPORT

Iran vs Albania: A Sustained Cyber Conflict

2021 – 2026 | Based on publicly available sources

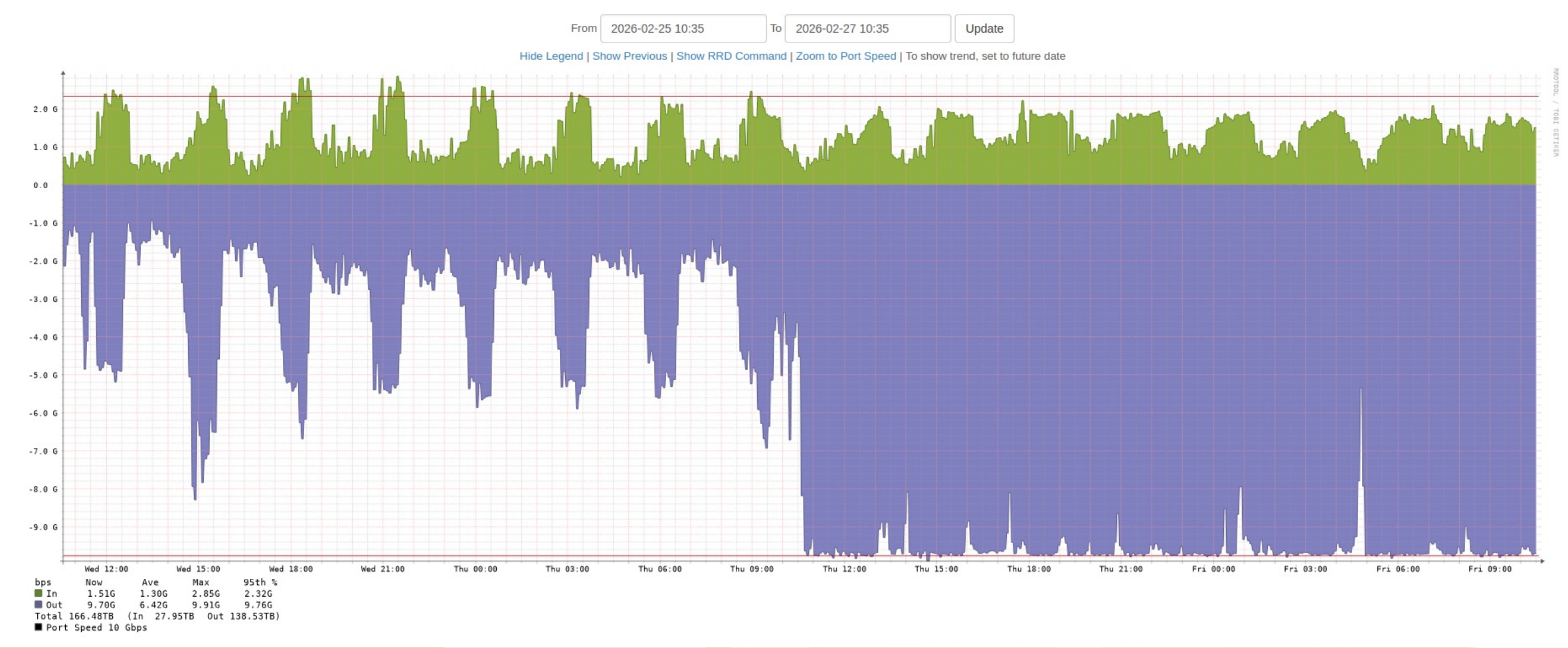
Prepared: March 26, 2026

Executive Summary

Since 2021, the Islamic Republic of Iran has conducted an escalating campaign of cyberattacks against Albanian government infrastructure. The attacks are carried out primarily by a group known as HomeLand Justice, attributed by the FBI, CISA, Mandiant, and Microsoft to Iranian state actors — specifically Iran's Ministry of Intelligence and Security (MOIS) and, in later operations, the Islamic Revolutionary Guard Corps (IRGC).

The root cause is geopolitical: Albania hosts over 3,000 members of the Mujahedin-e-Khalq (MEK), an Iranian opposition group that Tehran considers a terrorist organization. Iran views Albania's hosting of MEK as a direct threat and has used cyberspace as the primary instrument of retaliation.

NoName057(16) → DDoS



Again: Join the GÉANT DDoS Working Group (also the workshop this afternoon in Mission 2!)

3. Supply Chain

- Increasing regulatory pressure + prices
- Digital Sovereignty
- "AI" enabled
- Open-source library / ecosystem compromises (TeamPCP, Axios)
- Bottlenecks (e.g. chip shortages)
- Oil? (and other Geo-political links)

→ Good supply chain management
→ Inventory and monitor software dependencies
→ Follow advice and best practices

2. Insufficient Support for Secure Behaviours (was: Poor Cyber Hygiene)

- "Zero days" / patch cycles vs time-to-exploit
- Unnecessarily exposed/vulnerable* services
- System hardening and baselining
- Legacy/fragile systems "broken by design"
- Vibe coding
- Poorly designed systems and unrealistic security demands
- Creating: predictable attacks paths for adversaries

* "over the past 1-2 years we have seen a significant shift with the majority of our major incidents caused by a vulnerable service being the initial access" vs compromised account

→ Awareness (memorable/"exciting"/user-centred messaging)
→ GÉANT Security Baseline
→ Address fears (support rather than punish)

Users are not stupid: Six cyber security pitfalls overturned

Received (in revised form): 9th November, 2022

Julie Haney
Usable Cybersecurity Program Lead, National I

Julie Haney conducts research about the huma
and adoption of cyber security solutions, work
perceptions of privacy and cyber security. She
forums spanning industry, government and aca
research and practitioner publications. Prior to
in the U.S. Department of Defense as a cyber s
conducted vulnerability assessments, wrote wi
the adoption of cyber security mitigations. She
of Maryland, Baltimore County, an MSc in com
computer science from Loyola University Mary

National Institute of Standards and Technology, 10
E-mail: julie.haney@nist.gov

https://www.nist.gov/news-events/news/2023/03/your-cybersecurity-strategy-falling-victim-these-6-common-pitfalls

1. AI +++

- "AI isn't replacing attackers, but it is accelerating them." – Lakera
- "For the First Time, Every Threat Carries an AI Dimension" – SANS Top 5 Most Dangerous New Attack Techniques (RSAC2026)
- Automated Cyber Attacks
- AI Generated Deepfakes
- Mass Scale Social Engineering
- Mimicking human behaviour / expectations
- Disinformation & Hallucination Driven Harm
- Agentic AI (e.g. OpenClaw) without policies/awareness
- AI as a Vulnerability

AI Attack Techniques

Hyper-Personalized Phishing

Top concern—LLM-crafted emails at scale with no telltale signs

Automated Vuln Scanning

AI-enabled exploit chaining and vulnerability discovery.

Adaptive Malware

Self-modifying code that evades signature-based detection.

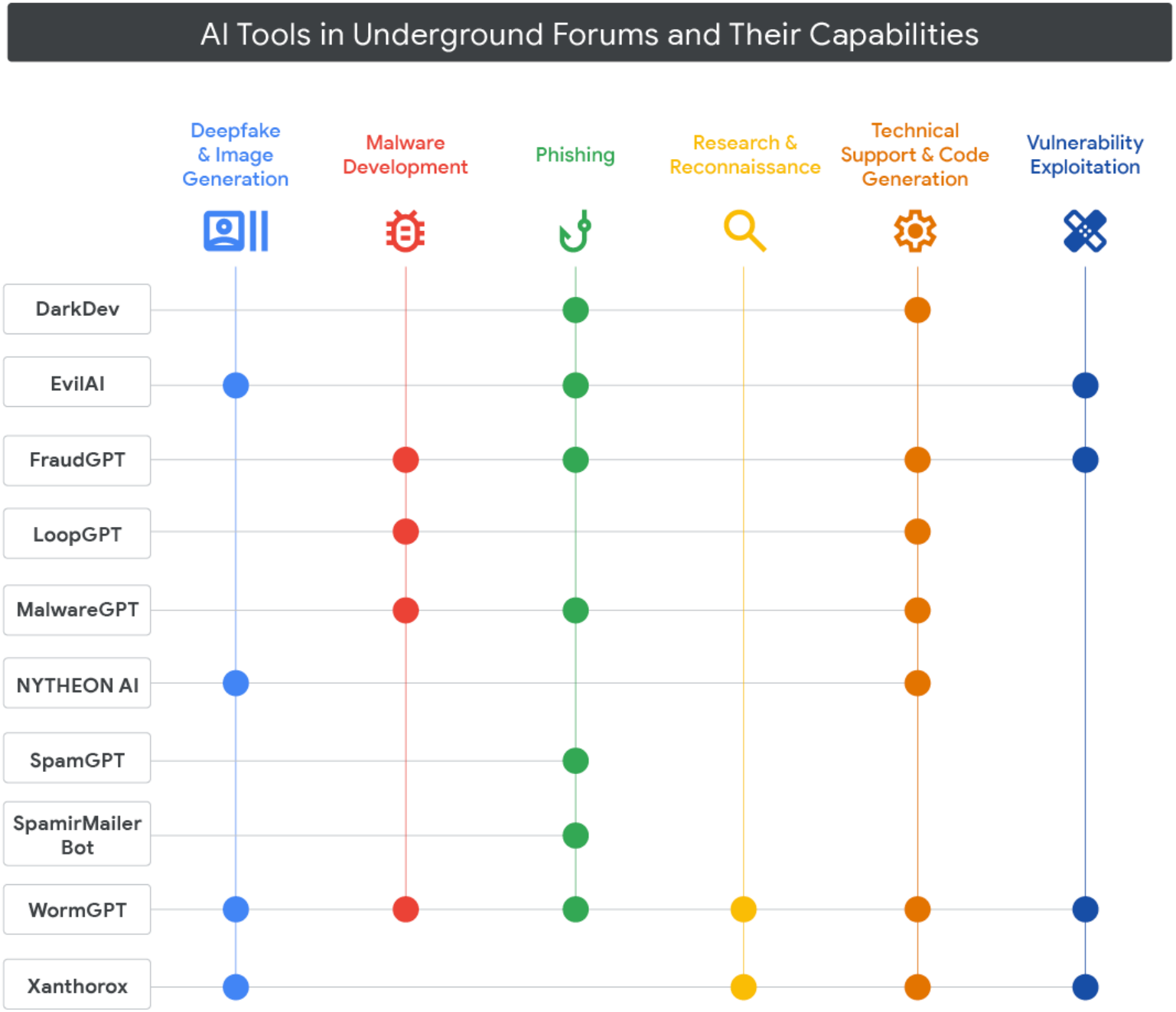
Deepfake Voice Fraud

AI-generated voice cloning for vishing attacks.

*Generated using Google Gemini AI (Nano Banana 2) with original text

Credit:

Google Threat Intelligence Group



1. AI +++

→ AI for defense
→ Policies
→ Awareness
→ All the others
→ ??

Top 10 Threats for R&E – 2026+

1. AI
2. Insufficient Support for Secure Behaviours
3. Supply Chain
4. Geo Politics
5. Social Engineering
6. Insider Threat / Decision Making
7. Quantum Computers
8. Not Sharing
9. DDoS Attacks
10. Lack of Contingency Plans

Please come talk to me
if you'd like to contribute
to the report ☺

FORESIGHT 2030 THREATS

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
20 years!

MARCH 2024

SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES

1

AI

16

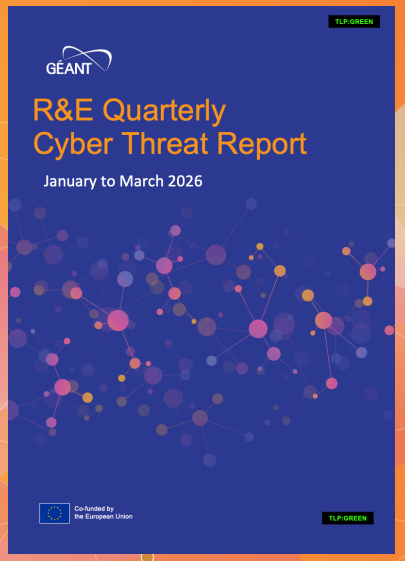
AI DISRUPTING / ENHANCING CYBER ATTACKS

Escalation as a result of AI-based tools. Attackers will use AI-based technologies to launch attacks. In order to defend against those attacks and even to launch counter measures, there must also be defensive AI-based weapons. Behaviour of the AI in these cases is difficult to test, measure and control – if speed of response is valued.

“Academic freedom and accountability are not opposites: the freedom to pursue and share knowledge openly is only sustainable if the integrity and security of that knowledge is protected.”

Thank you!

Look out for our threat landscape
+ quarterly reports ☺



https://lists.geant.org/sympa/subscribe/cti-reports

GÉANT

Security .Days