

HTTPS is gebroken

Zo herstellen wij het met Post-Quantum Cryptografie

Daan Acohen

Inhoud

- Wie ben ik?
- Wie zijn jullie
- Publieksvraag
- Geschiedenis Versleuteling
- Huidige status versleuteling
- Publieksantwoord
- Hoe we u kunnen helpen

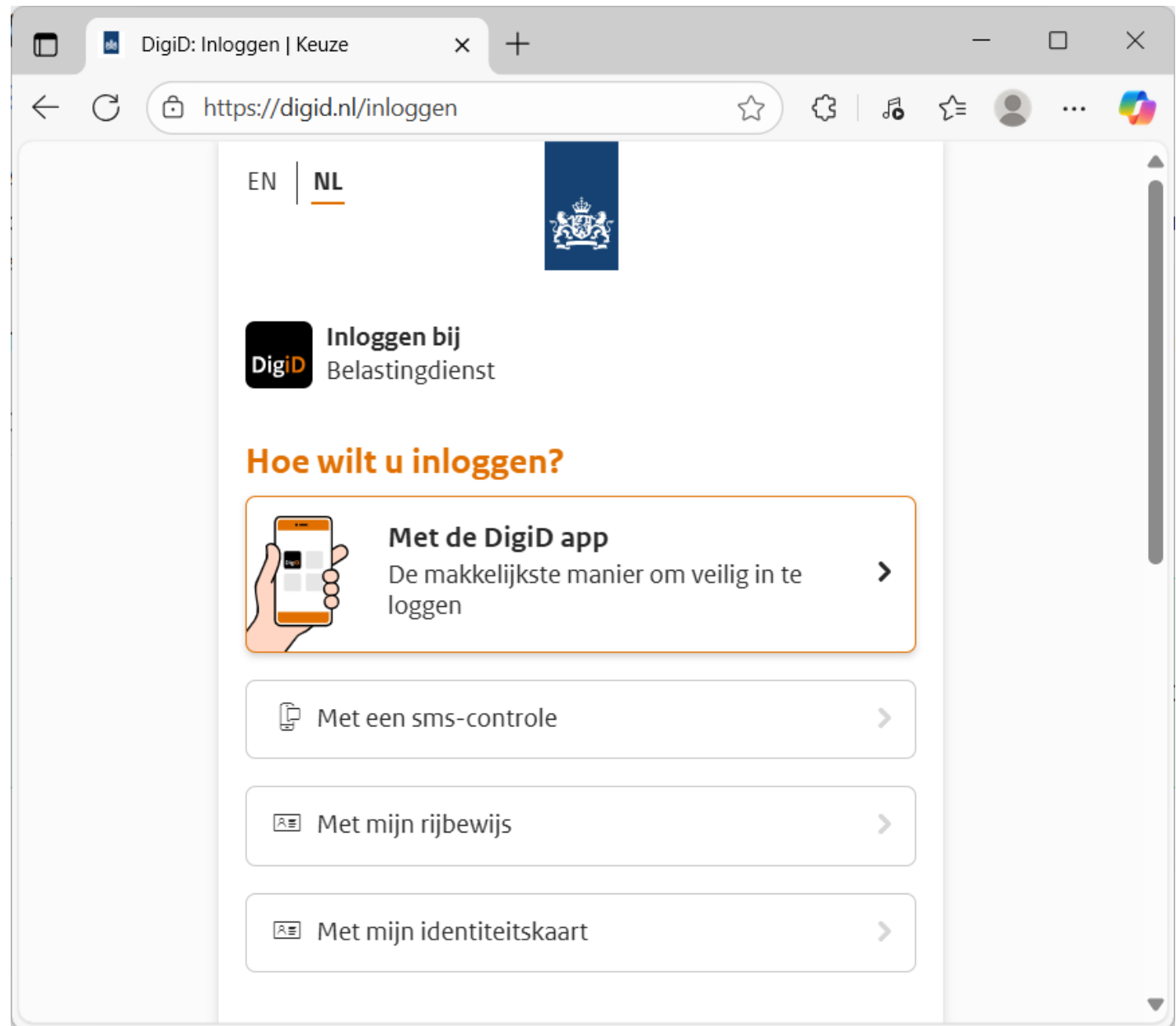
Wie ben ik?

- Daan Acohen
- Zelfstandig .NET ontwikkelaar en PQC-specialist
- Publicaties op CodeProject
- NuGet packages
- Klanten in Nederland en België
- Getrouwd
- Woon in Den Haag

Wie zijn jullie?

- Ontwikkelaar
- Historicus
- Security Engineer
- CISO
- Natuurkundige
- Cryptograaf or Cypto-analist
- Wiskunde overig
- En verder?

Publieksvraag



Geschiedenis, oud

- Egyptenaren
- Romeinen
- Grieken

Vervanging van letters/hiërogliefen



Veilig?

Niet meer.....

Middeleeuwen

- Al-kindi, frequentie-analyse, 9e eeuw
- Nieuwe coderingstechnieken



Veilig?

Niet meer.....

Geschiedenis, rond 1900

- Automatisering
- Enigma-machine



Veilig?

Niet meer.....

Moderne Geschiedenis

- Diffie-Helman, public key encryption
- RSA, ontbinden priemgetallen



Veilig?

Niet meer.....

Waarom niet ?

- Shor (1994)
- Leek puur theoretisch

Puur
theoretisch?

Browser window showing a news article from heise online:

URL: <https://www.heise.de/en/news/Cryptocalypse-EU-dem...>

heise online


heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissenschaft Digital He

IONOS Domain • Website • Cloud

"Cryptocalypse": EU demands quantum-safe encryption – partly by 2030

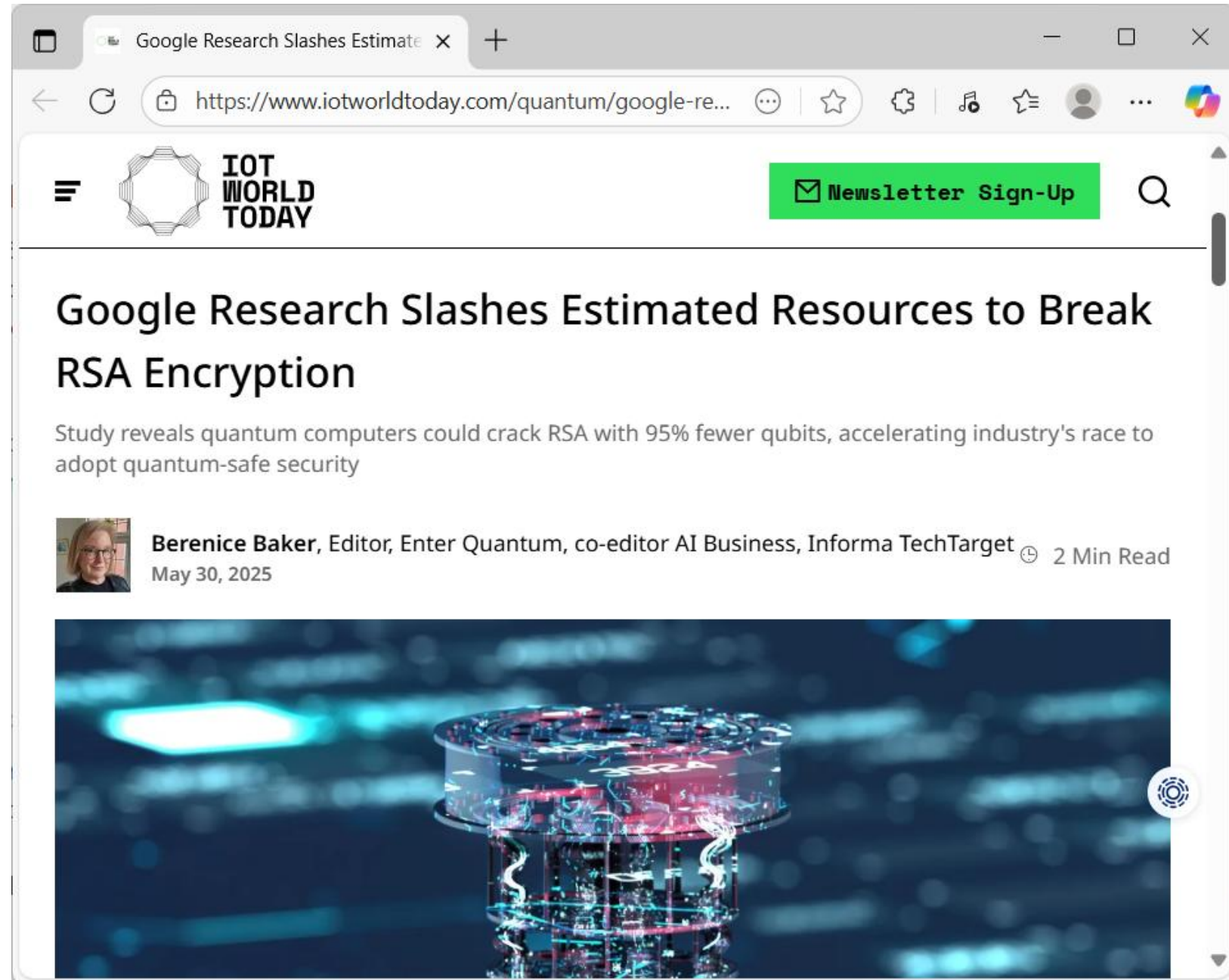
All member states should start switching to post-quantum cryptography by 2026, EU bodies demand. Critical infrastructures are in a hurry.

Germany icon | Speaker icon

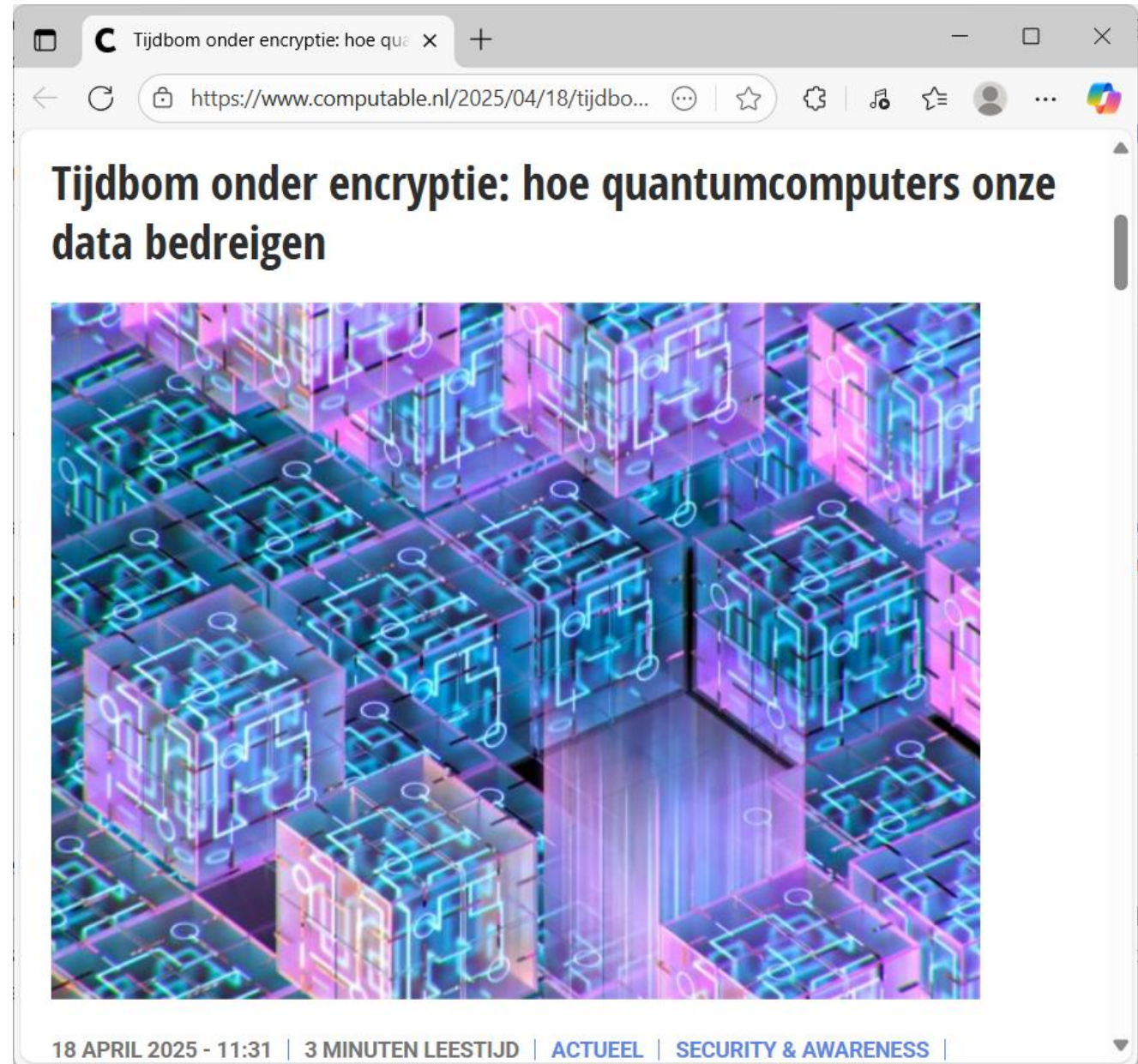


Video player controls: play/pause, volume, progress bar.

Puur
theoretisch?



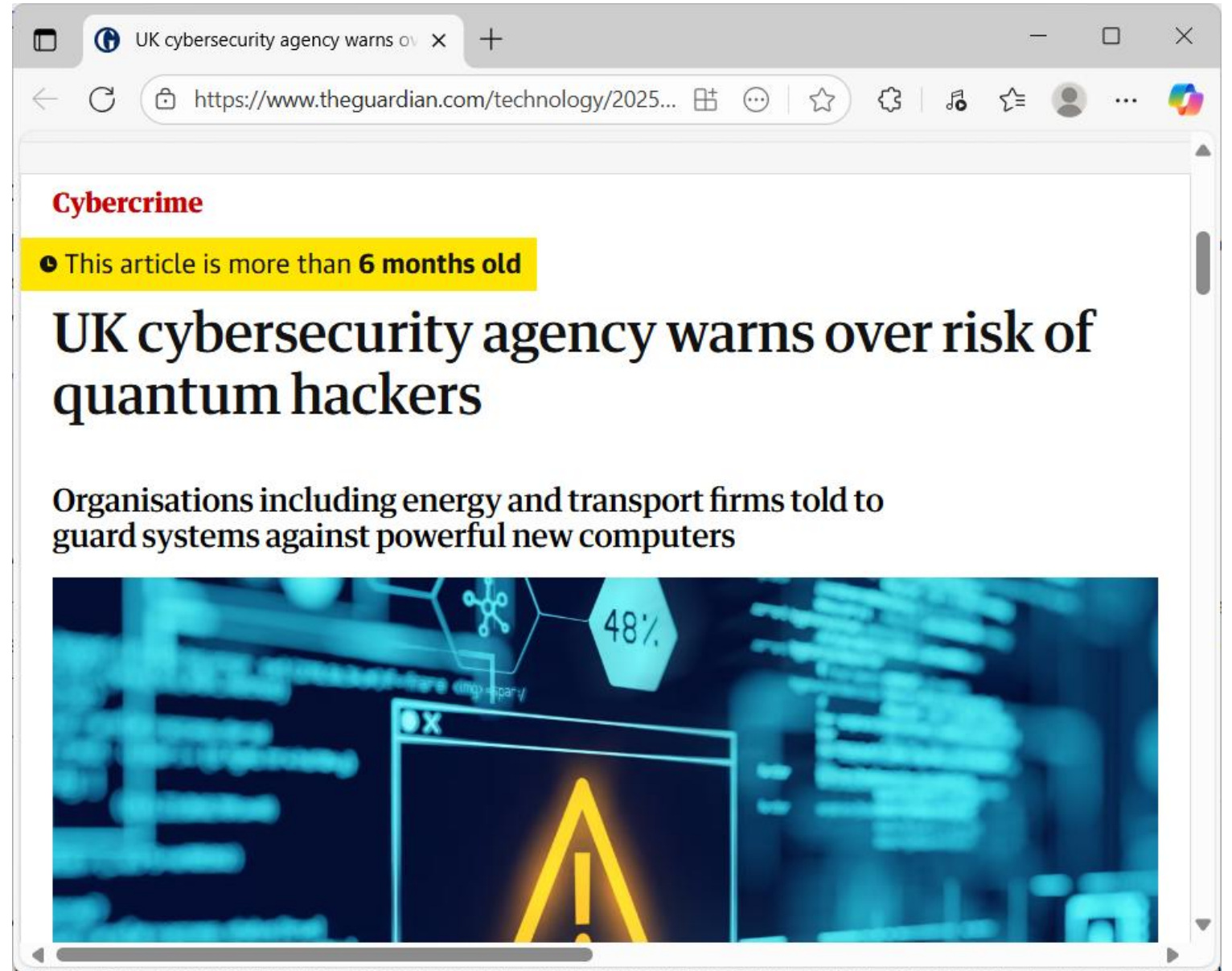
Puur
theoretisch?



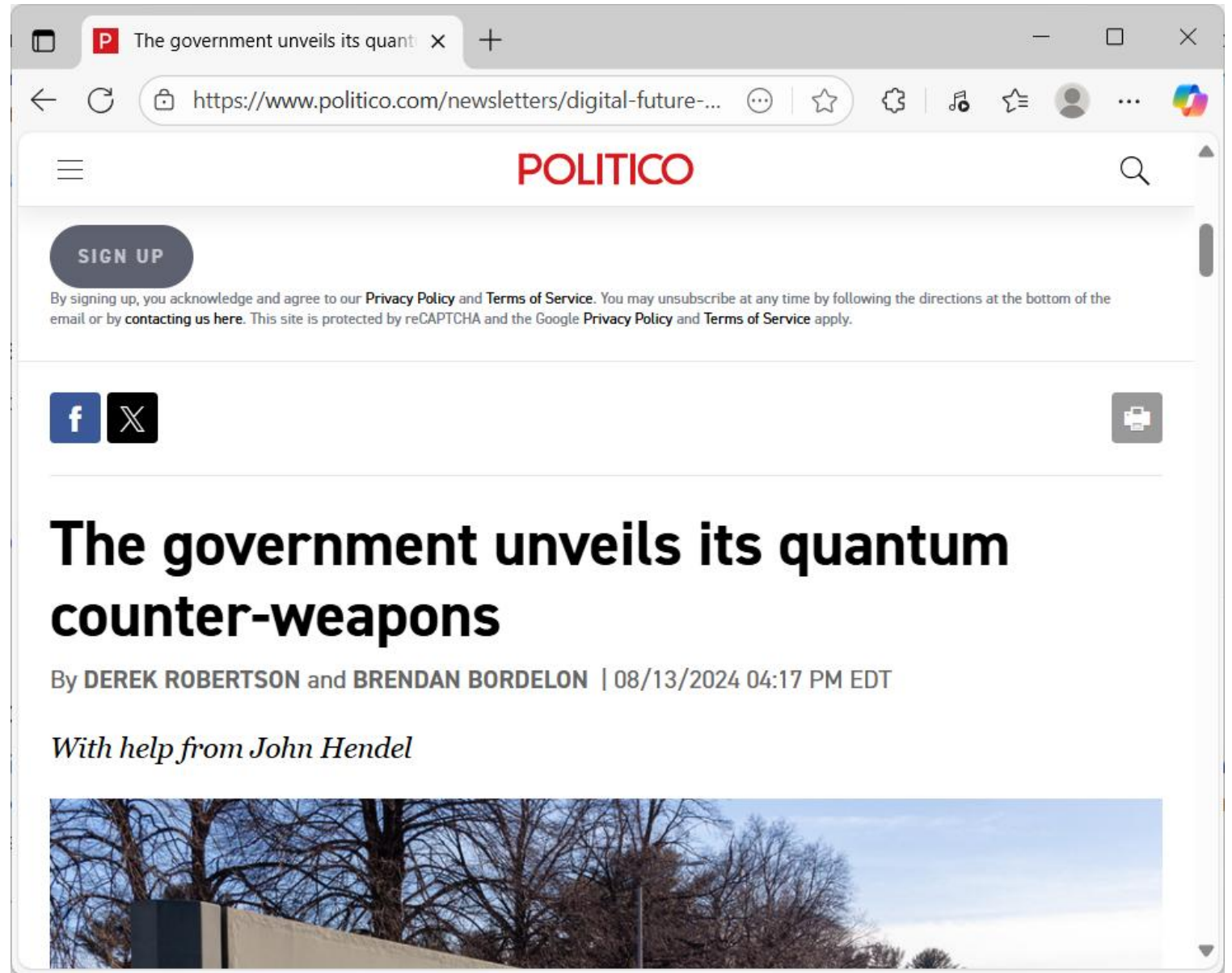
Puur
theoretisch?



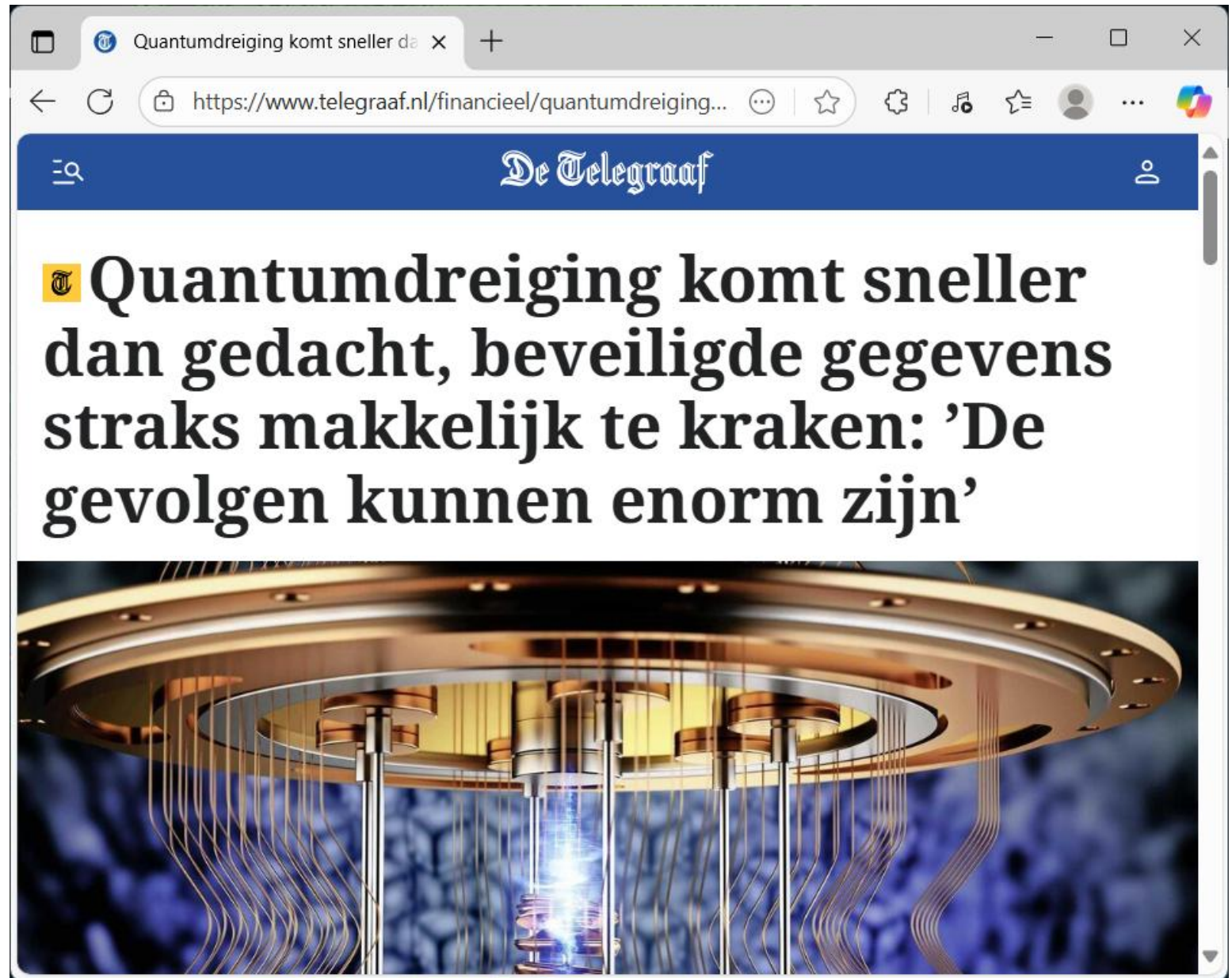
Puur
theoretisch?



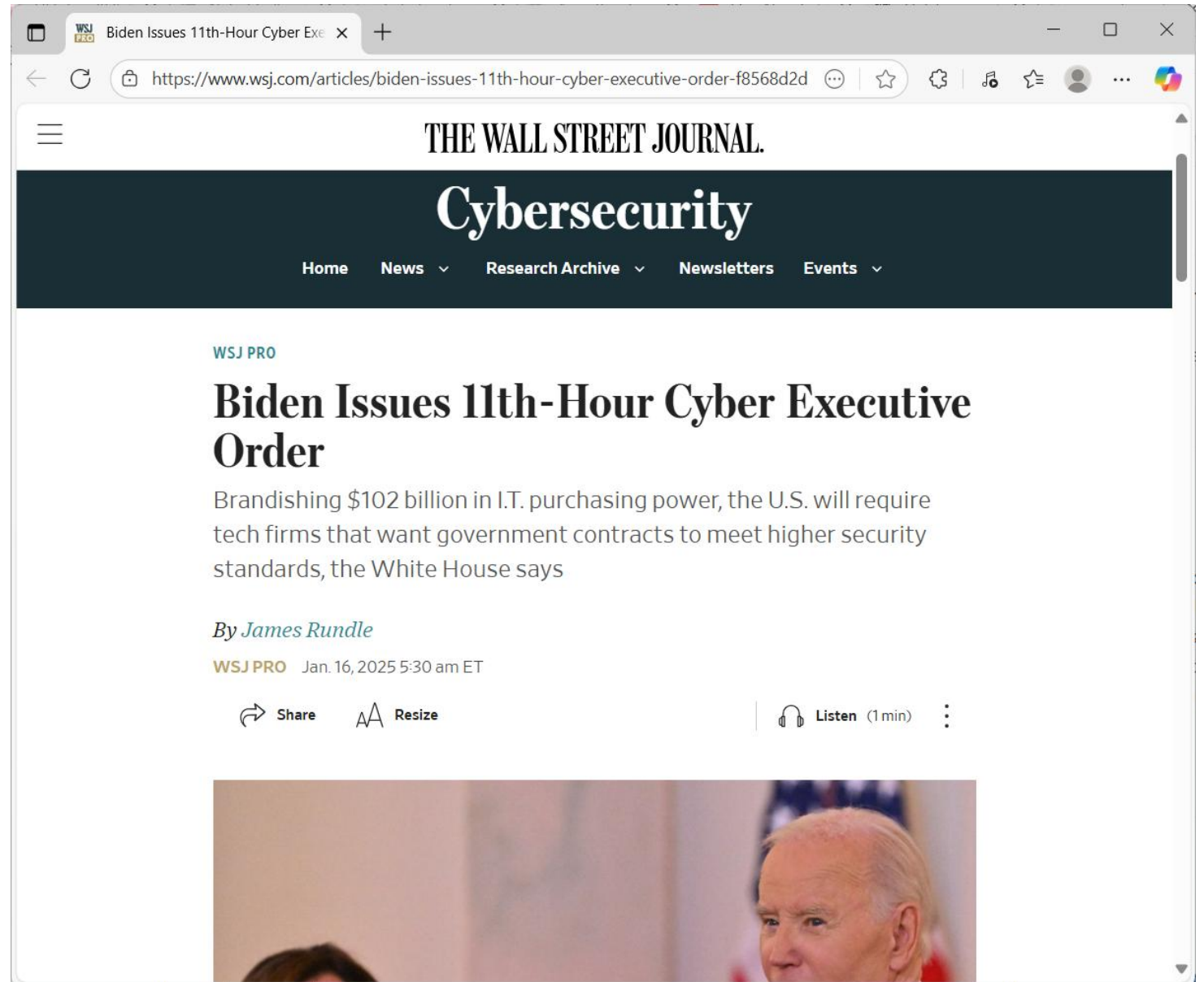
Puur
theoretisch?



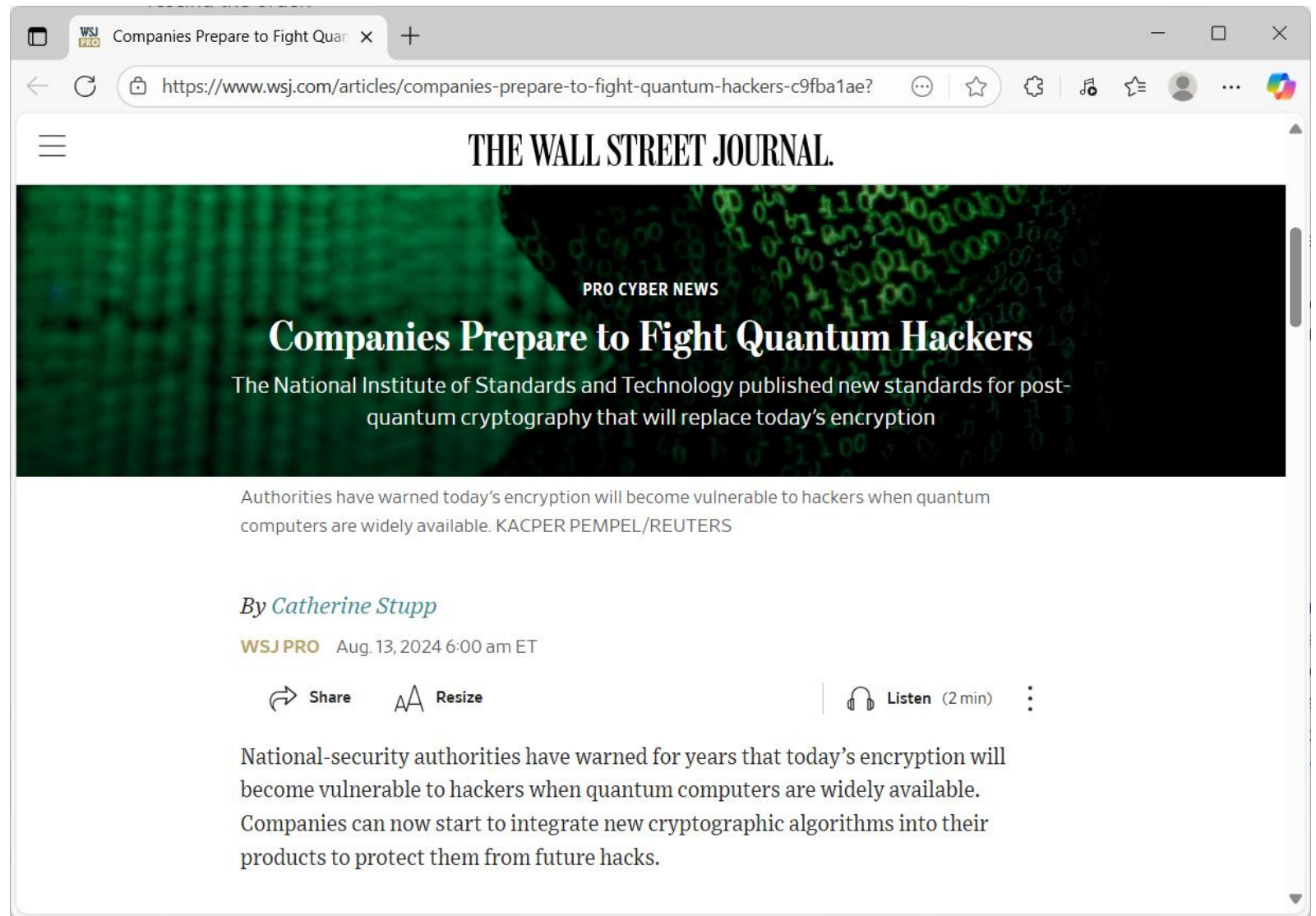
Puur
theoretisch?



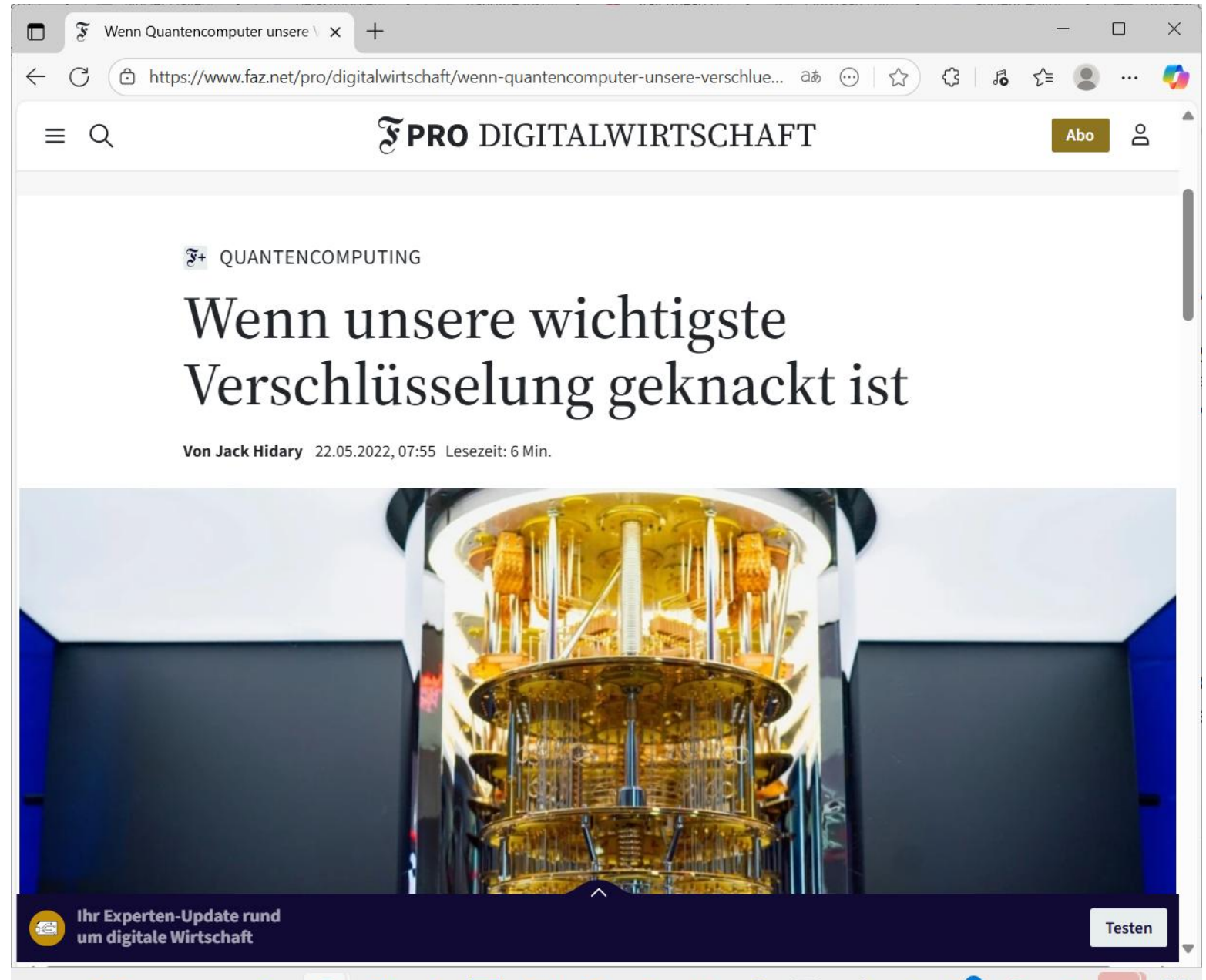
Puur
theoretisch?



Puur
theoretisch?



Puur
theoretisch?



Puur theoretisch?



The screenshot shows a web browser window with the address bar displaying "https://www.orange cyberdefense.com/nl/blog/cybersecurit...". The article title is "Quantum computing: een reële dreiging voor encryptie". The text discusses the threat of quantum computers to cryptography between 2030 and 2035, the impact on data security, and the European Commission's advice for a transition to post-quantum cryptography (PQC) by 2030. A button for downloading a quantum whitepaper is visible. The bottom of the page includes a section titled "Wat is post-quantum cryptografie (PQC)?" and a footer with "Incident Response Hotline".

Quantum computing: een reële dreiging voor encryptie

De komst van grootschalige quantumcomputers tussen 2030 en 2035 vormt een directe bedreiging voor de cryptografie die onze digitale communicatie vandaag beveiligt. Wat nu nog veilig is, kan straks eenvoudig worden gekraakt.

Deze verschuiving verandert het cybersecuritylandschap fundamenteel. De impact? Vertrouwelijkheid, integriteit en authenticatie van gevoelige data en transacties komen in gevaar. En cybercriminelen zijn al bezig middels hun 'harvest now, decore later' strategie: ze verzamelen nu versleutelde data met de intentie om die later te ontsleutelen zodra quantumtechnologie volwassen is.

Voor organisaties met complexe, multiregionale infrastructuren is vroege voorbereiding cruciaal voor een soepele en tijdige migratie. De Europese Commissie adviseert lidstaten om uiterlijk eind 2026 te starten met de overgang naar post-quantum cryptografie (PQC), en kritieke infrastructuur moet uiterlijk in 2030 zijn gemigreerd.

Download ook ons quantum whitepaper

Wat is post-quantum cryptografie (PQC)?

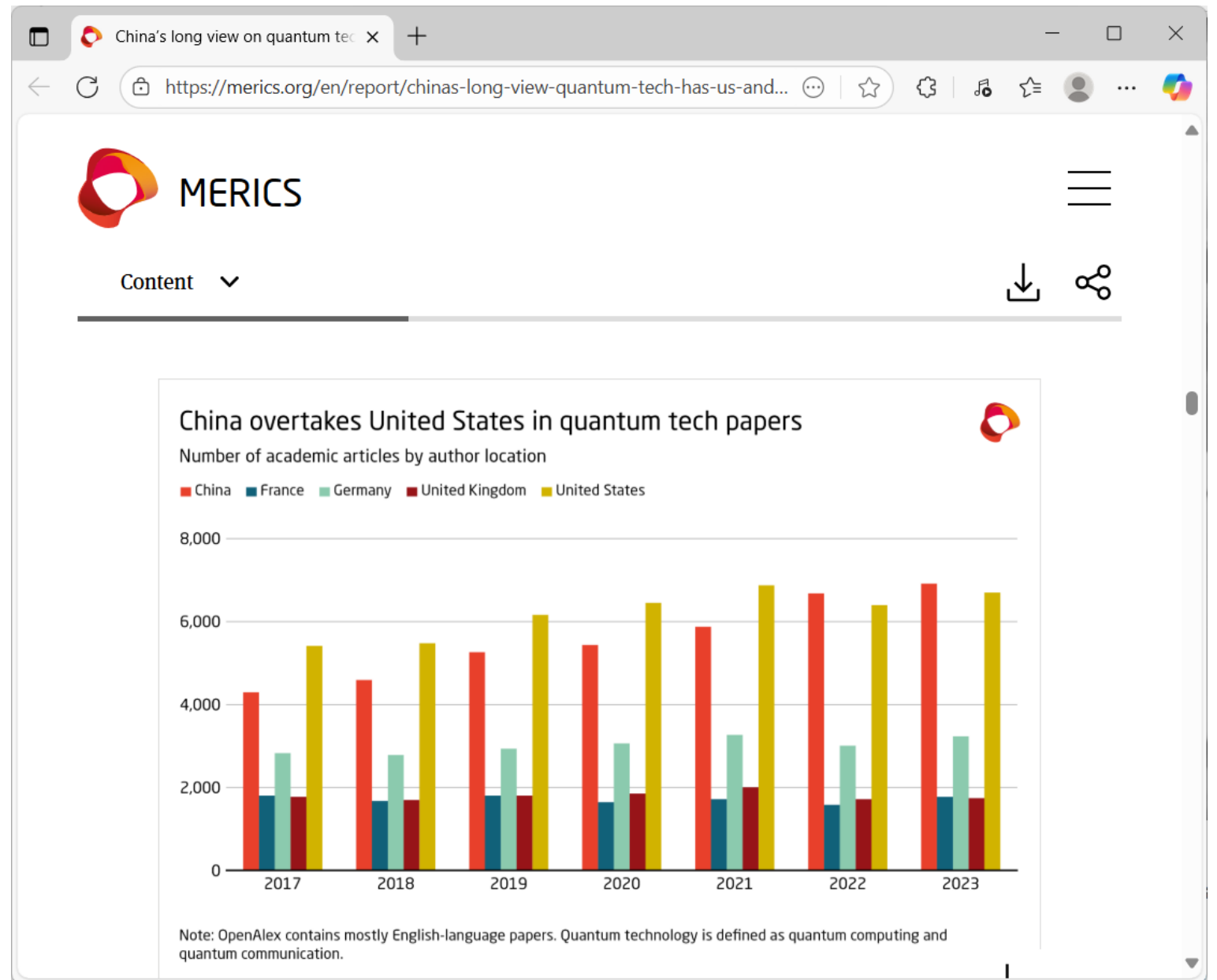
Post-Quantum Cryptografie verwijst naar cryptografische algoritmen die specifiek zijn ontworpen om bestand te zijn tegen aanvallen van quantumcomputers. Verschillende van deze algoritmen zijn al

Incident Response Hotline

Nieuwe bedreigingen

- Kwantumcomputer
- Kwantumalgoritmen
- Statelijke actoren
- Store Now Decrypt Later

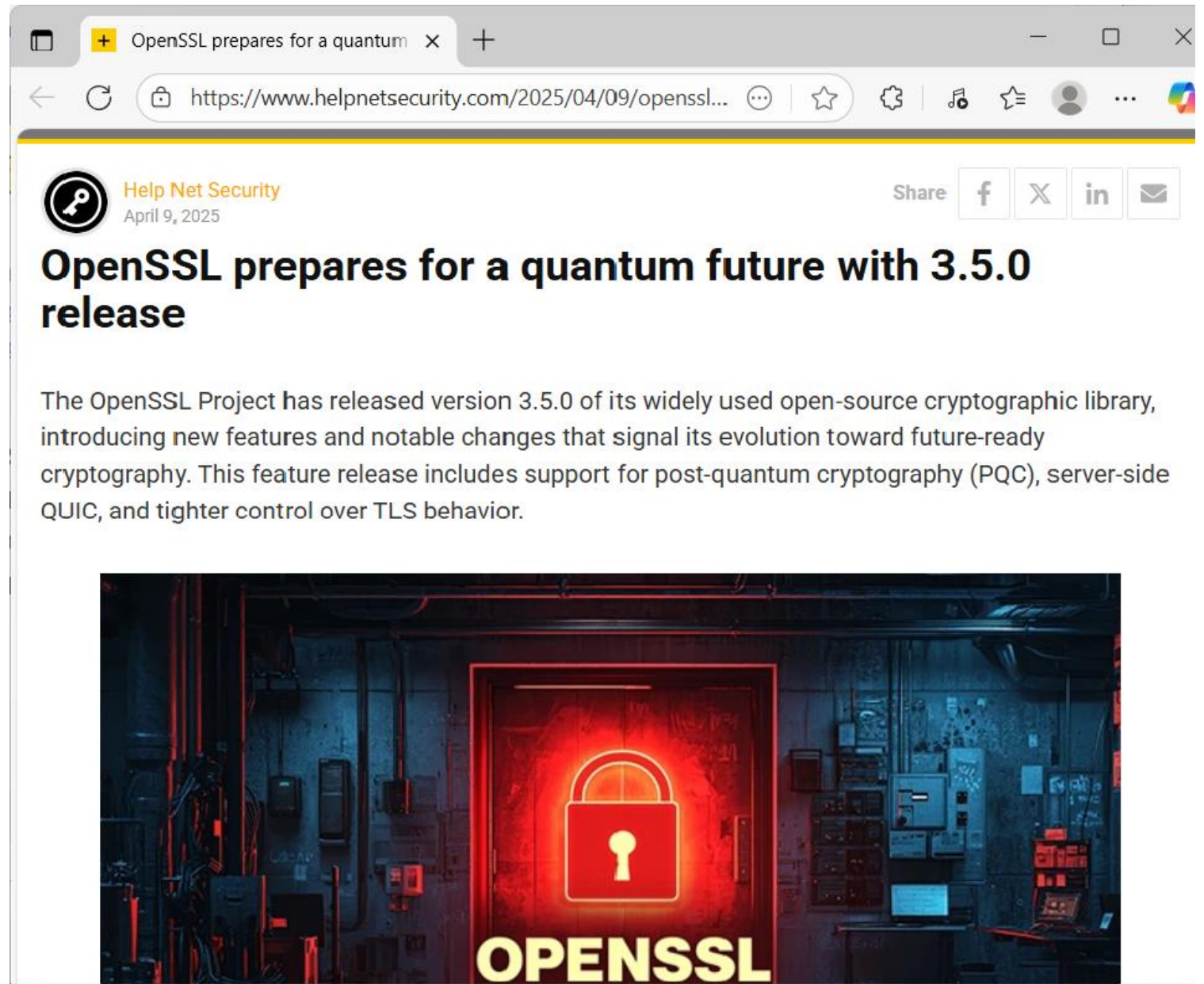
Statelijke Actoren



Store Now Decrypt Later

- Van toepassing op gegevens die lang geheim moeten blijven
- Bedrijfs grootte nauwelijks relevant
- Vertrouwelijkheid ook nauwelijks relevant
- BSN, Risico
- Creditcardnummers, geen risico

Oplossingen



Stay Ahead of Quantum Threats

https://www.quantumsafeaudit.com

Quantum Website Scanner

Stay Ahead of Quantum Threats

Attackers can copy your encrypted data today and break it tomorrow with quantum computers – the store-now, decrypt-later threat. In a short time we reveal which certificates, protocols and key stores keep that door open. We turn the results into a step-by-step action plan and—if you choose—our own specialists apply every fix, so you don't need extra engineers. The outcome: future-proof encryption and demonstrable compliance with NIS 2 and DORA.

Test your website for Post-Quantum Cryptography readiness. Enter your domain below to start a scan.

Domain Name

example.com

Quantum Scan

Saved info

Please fill out this field.

securitydelta.nl

The i

your

learn

ah.nl

accounts.nintendo.com

www.grantthornton.com

www.ibm.com

jumbo.com

1768, which demonstrates that

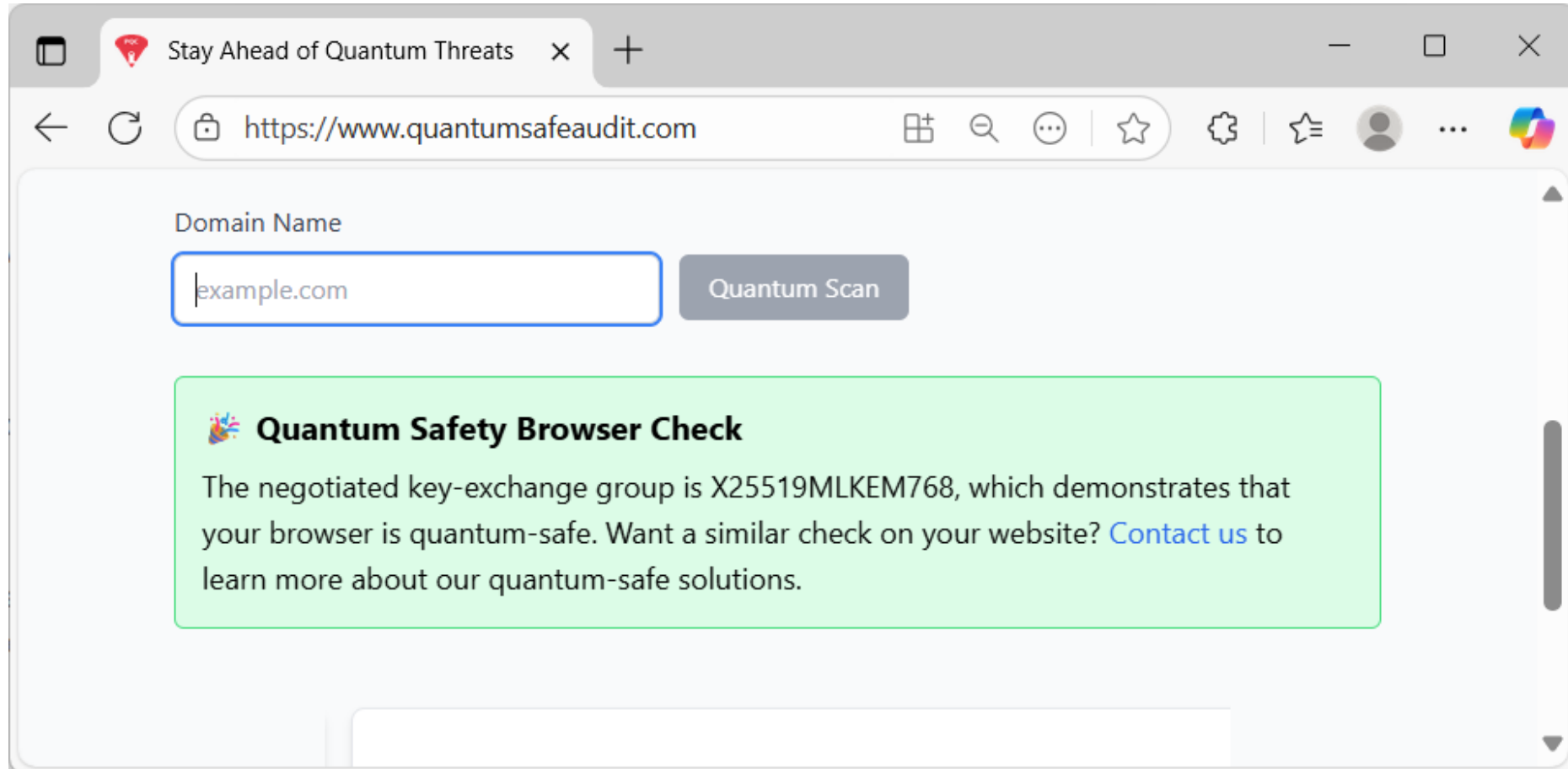
n your website? [Contact us](#) to

imated

Resources to Break RSA Encryption

IoT World Today (May 2025)

Client Screening



The screenshot shows a web browser window with the address bar displaying `https://www.quantumsafeaudit.com`. The browser's tab is titled "Stay Ahead of Quantum Threats". The main content area features a "Domain Name" label above a text input field containing "example.com". To the right of the input field is a grey button labeled "Quantum Scan". Below this, a green-bordered box contains the heading "Quantum Safety Browser Check" with a small icon. The text inside the box states: "The negotiated key-exchange group is X25519MLKEM768, which demonstrates that your browser is quantum-safe. Want a similar check on your website? [Contact us](#) to learn more about our quantum-safe solutions."


Stay Ahead of Quantum Threats

`https://www.quantumsafeaudit.com`

Domain Name

example.com

Quantum Scan

 **Quantum Safety Browser Check**

The negotiated key-exchange group is X25519MLKEM768, which demonstrates that your browser is quantum-safe. Want a similar check on your website? [Contact us](#) to learn more about our quantum-safe solutions.

Client Screening

```
Command Prompt
Microsoft Windows [Version 10.0.26100.6725]
(c) Microsoft Corporation. All rights reserved.

C:\Users\daan_>curl -I https://www.quantumsafeaudit.com/
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Expose-Headers: date,content-type,content-length,server,connection
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: public, max-age=0
Content-Length: 686
Content-Type: text/html; charset=utf-8
Date: Tue, 14 Oct 2025 14:56:38 GMT
Etag: W/"2ae-197ac778b08"
Last-Modified: Thu, 26 Jun 2025 13:40:05 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Vary: Origin
X-Key-Exchange-Group: X25519

C:\Users\daan_>|
```

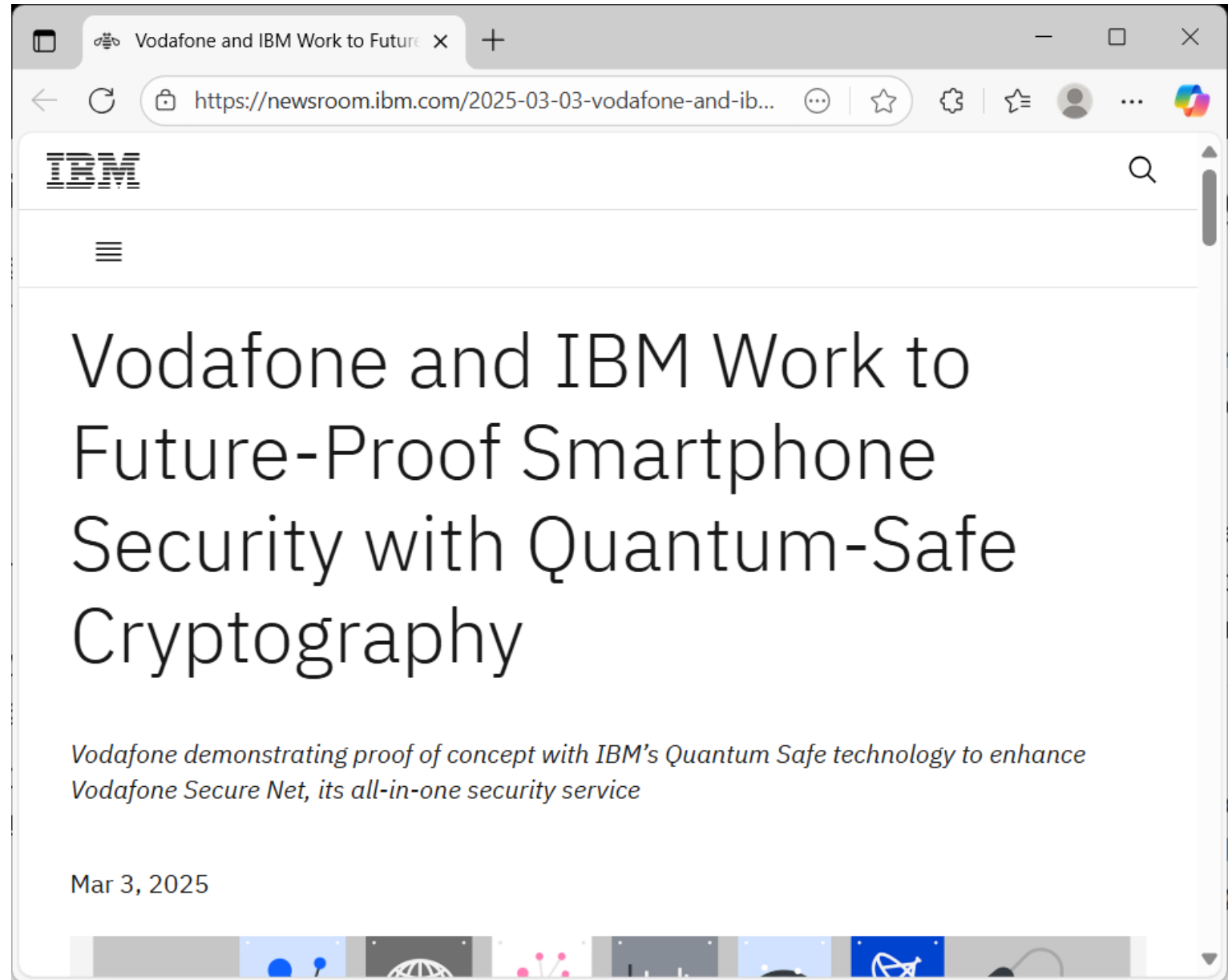

Inlezen?



Hulp nodig?

- In kaart brengen
- Compliance DORA en NIS2
- Implementatie
- QuantumSafeAudit.com werkend op uw eigen bedrijfsnetwerk

Duurder kan
ook.....



Vragen?