CYBERVEILIG NEDERLAND



Cybersecurity, AI en digitale autonomie: wat de geschiedenis ons kan leren?

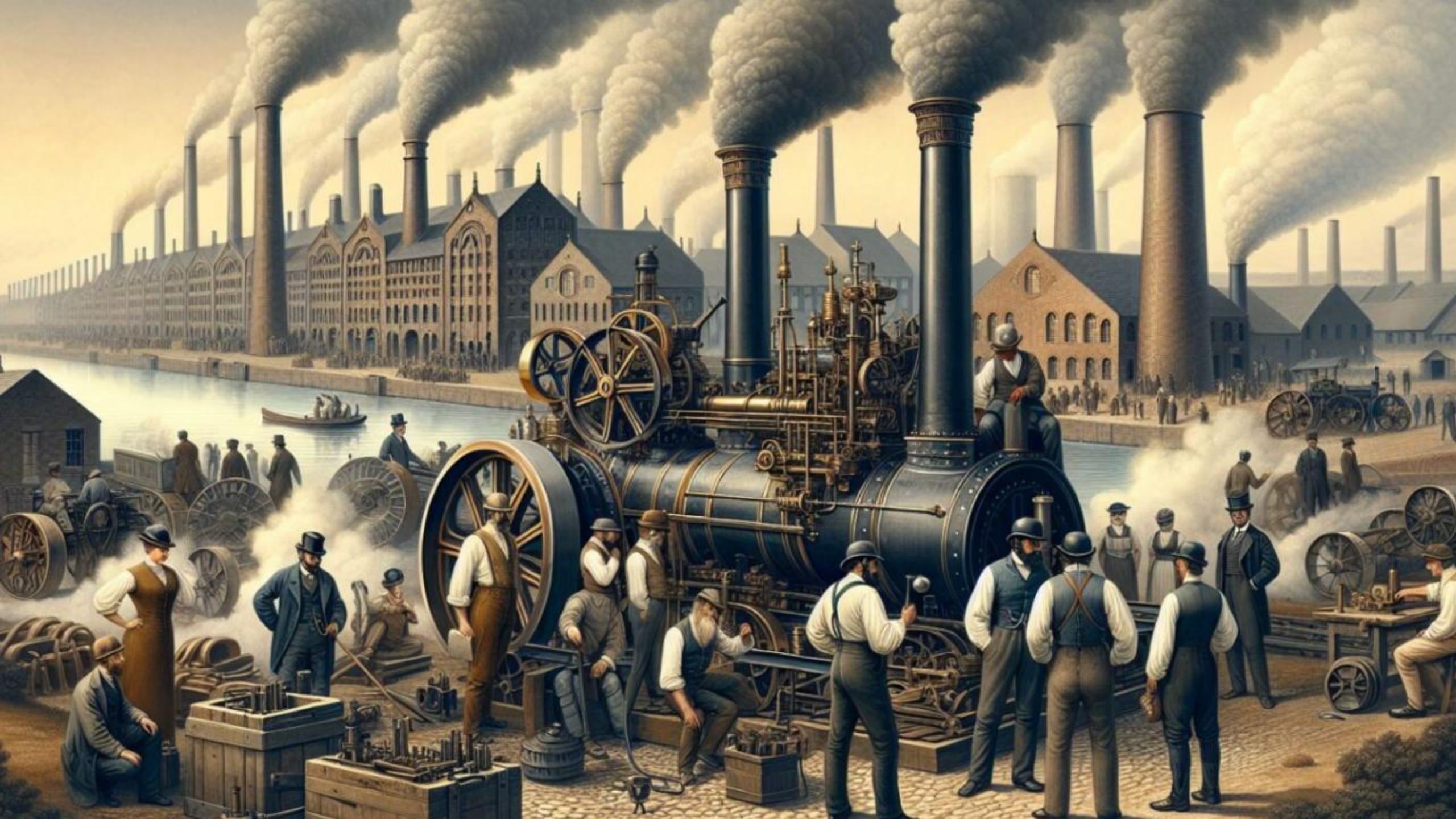
NFIR relatiedag



Holterman heeft een vrij ongebruikelijk profiel. Ze is begonnen als historicus, werd vervolgens inlichtingenofficier bij de AIVD, maakte daarna de overstap naar bedrijfsleven en brancheorganisaties en is uiteindelijk een prominente stem geworden op het gebied van cybersecurity en nationale veiligheid. Tegelijkertijd houdt ze via haar commissariaat bij Cogas toezicht op een organisatie die zelf met vitale infrastructuur te maken heeft.


JOHANNES
GUTENBERG







VROUW EN COMPUTER

Afl. 4: Automatisering op het werk




CRA
Cyber Resilience Act
Veiligere producten
Eisen aan fabrikanten
Minder kwetsbaarheden
NIS2
Network and Information Security Directive 2
Betere cyberbeveiliging
Voor essentiële sectoren
Meldplicht bij incidenten
EU
WET- EN REGELGEVING


YAHOO!
DIGG
WIKIA
WIKIPEDIA
CNN
IMDB
BBC
AOL
AMAZO
ASK
ABOUT
WEBMD
BABYLON
OCEAN
OF
INFORMATION
DATAFLOW
SEA
BRITANNICA
CA
TECHNOLOGIES
BMC
EMC
CISCO
IBM
ORACLE
HP
GOOGLE
DRIVE
CHROME
WEBMASTER
SEA
INTERNET
EXPLORER
NORTH DATASTREAM
SOUTH DATASTREAM
FAR SOUTH DATASTREAM
THE CAPITOL
MICROSOFT
RAPID
SHARE
DROPBOX
CLOUD
MOZILLA
OPERA
MS DOS SEA
DEVELOPER SEA
GNU
UBUNTU
CONDUIT
APPSTORE
INNOVATION
SEA
MEGA
MEGA
UPLOAD
SEA OF
ARCHIVES
FLICKR
PHOTO
BUCKET
SEA OF
COPYRIGHT
APP SEA
PROGRAMM


Project
Glasswing
Securing critical software
for the AI era

1. AI voor cyberaanvallen

2. Aanvallen op AI

3. AI voor cybersecurity

4. Cybersecurity van AI

Announcements

Statement on the US government directive to suspend access to Fable 5 and Mythos 5

12 jun 2026

The US government, citing national security authorities, has issued an export control directive to suspend all access to Fable 5 and Mythos 5 by any foreign national, whether inside or outside the United States, including foreign national Anthropic employees. The net effect of this order is that we must abruptly disable Fable 5 and Mythos 5 for **all** our customers to ensure compliance. **Access to all other Anthropic models will not be affected.**

We received the directive from the government today at 5:21pm (ET). The letter did not provide specific details of its national security concern. Our understanding is that the government believes it has become aware of a method of bypassing, or "jailbreaking" Fable 5. We reviewed a demonstration of this specific technique being used to identify a small number of previously known, minor vulnerabilities. These vulnerabilities all appear relatively simple, and we have found that other publicly-available models are able to discover them as well

OPENBAAR DREIGINGSBEELD · AIVD · MIVD · NCTV · MEDIA

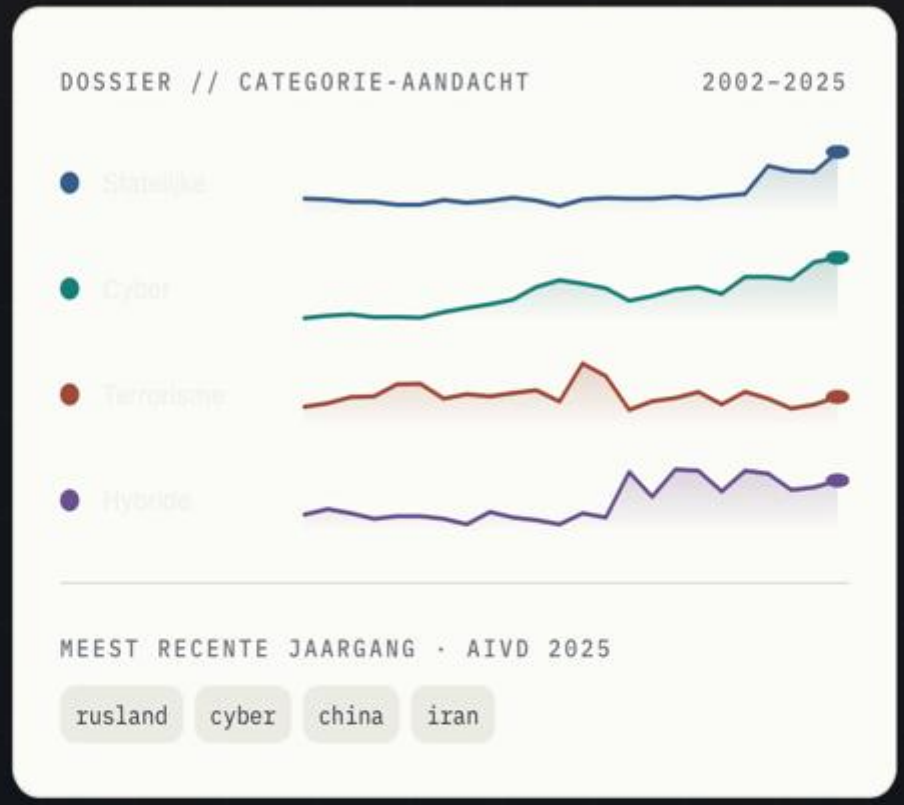
Maak dreiging bestuurlijk en operationeel bespreekbaar.

De Dreigingsmonitor vertaalt openbare bronnen van AIVD, MIVD, NCTV en media naar inzicht, scenario's en oefenvragen — voor crisismanagers, analisten en besluitvormers. Van 24 jaar dreigingsbeeld naar betere voorbereiding.

Start bij uw rol →

Plan een scenario-oefening

Bekijk het dashboard →



AANDACHT ≠ DREIGING

Deze tellingen meten aandacht in de jaarverslagen, geen dreigingsniveau. Het officiële NCTV-niveau (verderop) is wél een dreigingsbeoordeling.

48	24	4	4
JAARVERSLAGEN	JAAR IN BEELD	OPENBARE BRONNEN	CATEGORIEËN



Het Cybersecuritybeeld Nederland (CSBN) 2026 laat zien dat de capaciteiten en activiteiten van statelijke actoren en cybercriminelen toenemen. Hoewel er verschillende maatregelen worden genomen om Nederland tegen deze veranderende cyberdreiging te verdedigen, groeit de digitale weerbaarheid van Nederlandse organisaties en bedrijven niet in hetzelfde tempo mee. Hierdoor ontstaat verdere scheefgroei tussen de cyberdreiging en de digitale weerbaarheid. Dit vormt een ernstig risico voor de nationale veiligheid. Deze scheefgroei vergroot de kans dat Nederland slachtoffer wordt van maatschappij ontwrichtende spionage, datadiefstal, sabotage en uitval van digitale processen. De komende jaren zal AI het cyberlandschap ingrijpend veranderen en de dreiging verder versterken. Zoals het jaarbeeld, met daarin een selectie van publiekelijk bekende incidenten in deze rapportageperiode laat zien, heeft Nederland nu al te maken met veel cyberincidenten. Een deel van de cyberaanvallen waarvan Nederlandse organisaties en bedrijven slachtoffer zijn, is bovendien (nog) onzichtbaar. Het is dan ook niet de vraag óf, maar wanneer Nederland te maken krijgt met een maatschappij ontwrichtend cyberincident.

Van security naar weerbaarheid

“Kunnen we aanvallen voorkomen?”

“Kunnen we blijven opereren als preventie faalt?”

Inzicht in:



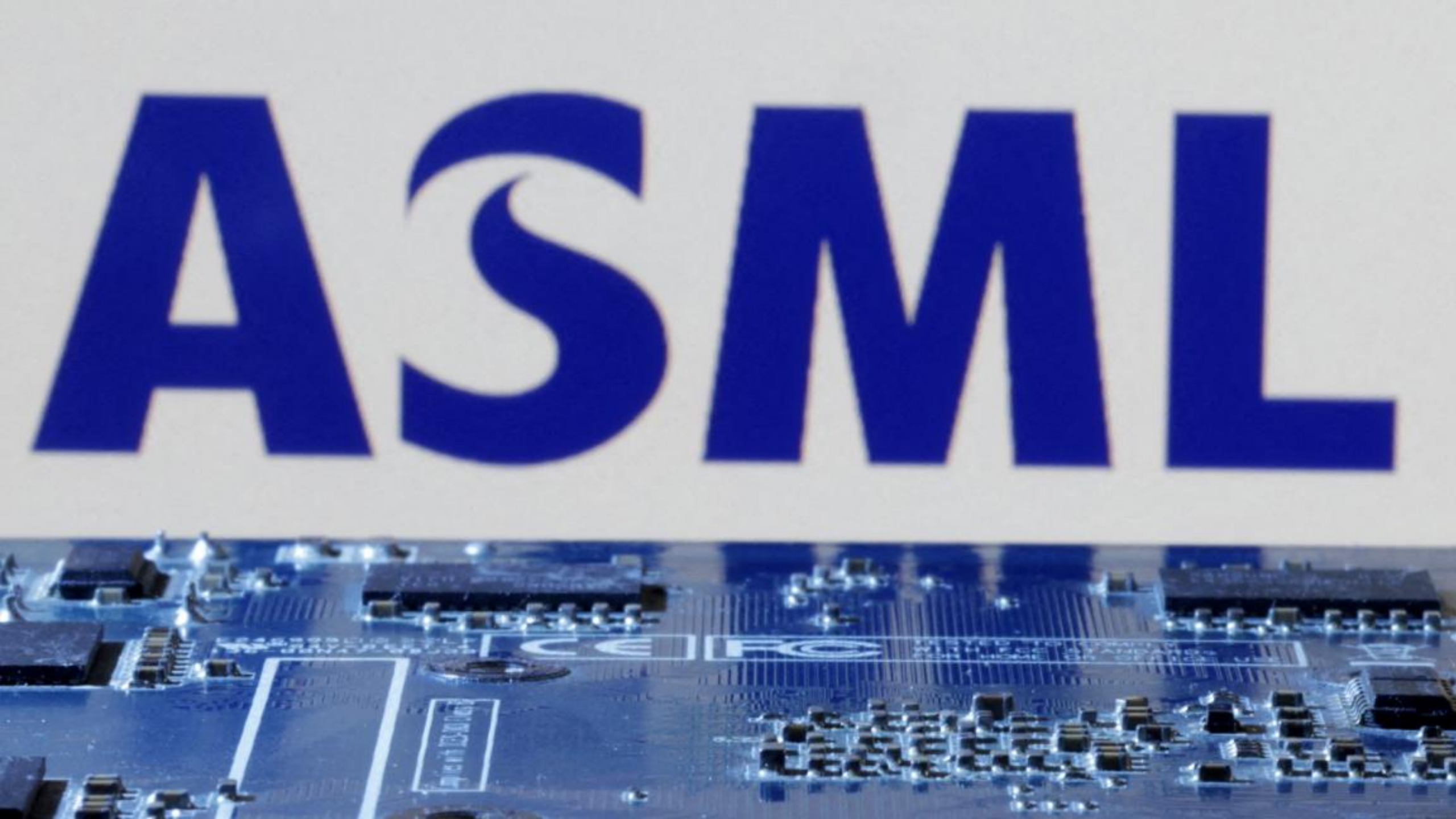
Kritische processen



Gevoelige data



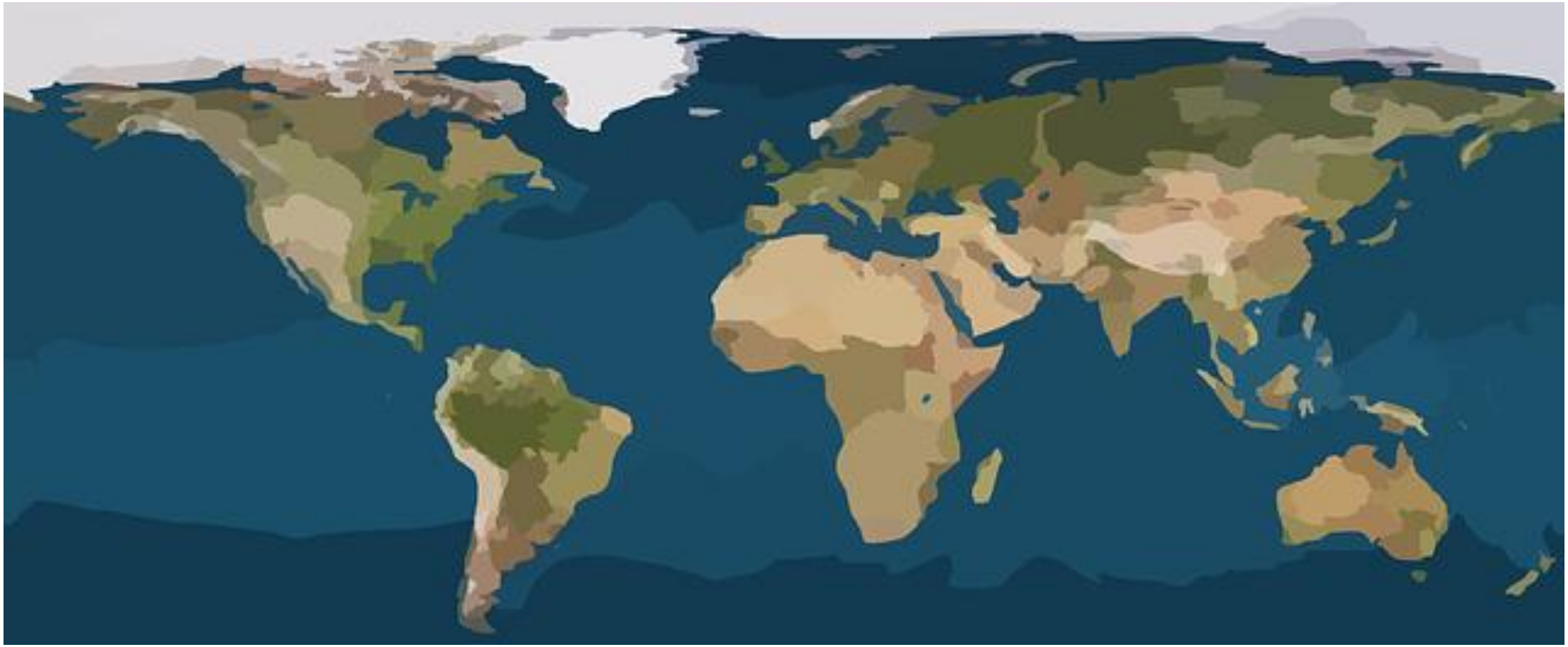
Strategische afhankelijkheden


ASML

Inkoopstrategie



Geografische distributie



S/HBOM: Inzicht in wat er in je systemen zit — van code tot chip

SBOM — Software Bill of Materials

Een gestructureerde lijst van alle softwarecomponenten, bibliotheken en afhankelijkheden waaruit een applicatie of systeem is opgebouwd.

- 📦 Open-source bibliotheken & versienummers
- 🔗 Transitieve afhankelijkheden (libs in libs)
- ⚠️ Bekende kwetsbaarheden (CVE-koppeling)
- 📜 Licenties van alle componenten

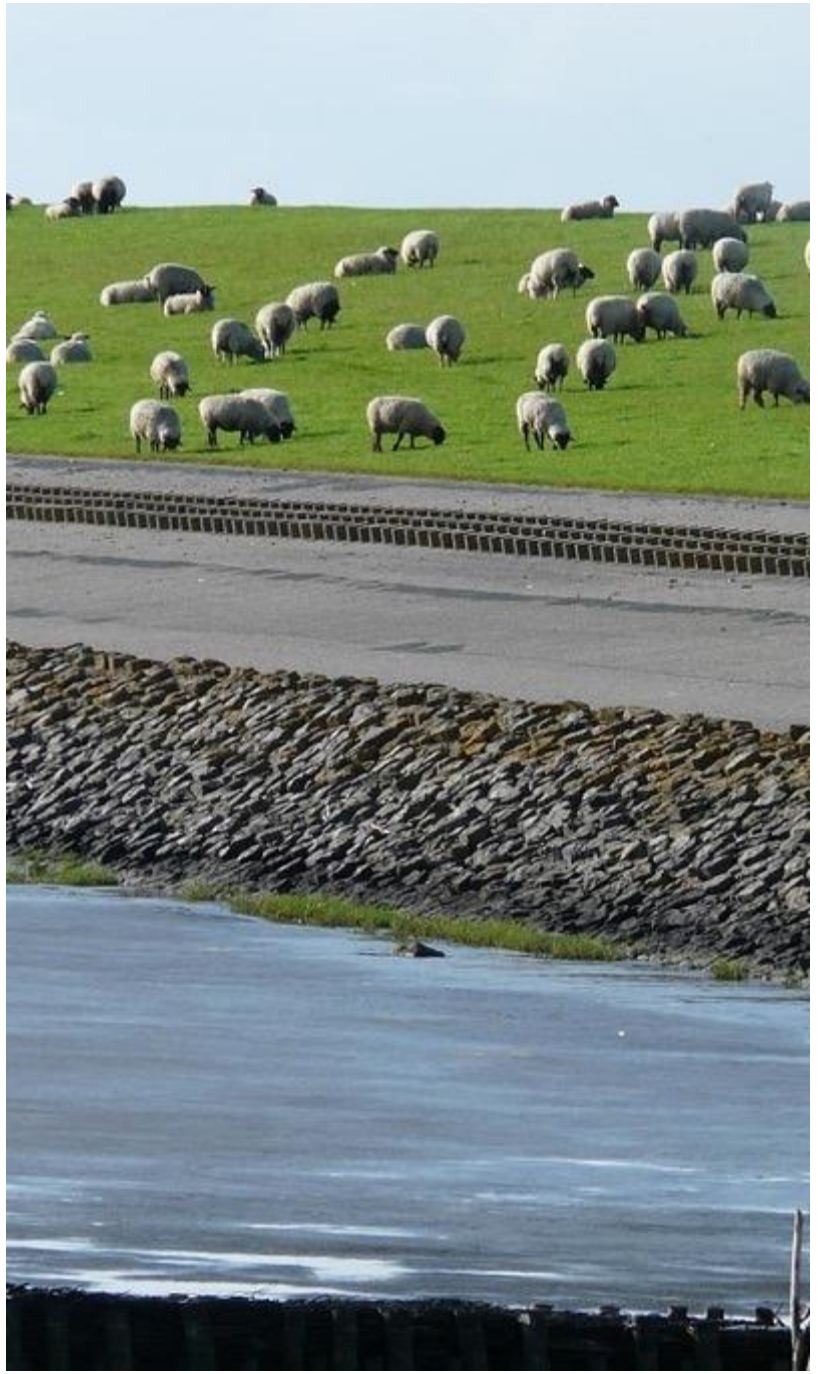
HBOM — Hardware Bill of Materials

Een gestructureerde inventarisatie van alle fysieke hardwarecomponenten in een apparaat of systeem, inclusief herkomst en fabrikant.

- 🖥️ Processoren, chips & microcontrollers
- 🌍 Herkomst & productieland van componenten
- 🏭 Leveranciers en toeleveringsketens
- 🔌 Firmware op hardwarecomponenten

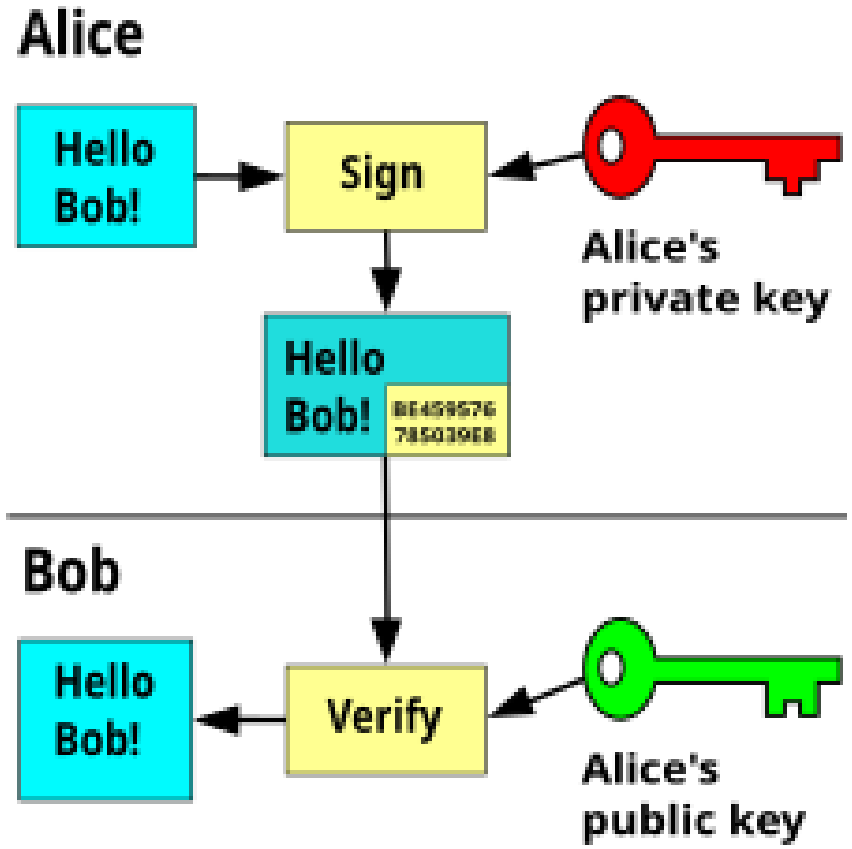
🔍


5¢
25¢
$1





Betere bescherming van gevoelige data





Versterking human capital



Digitale Autonomie = eigen regie

Controle

Keuzevrijheid

Weerbaarheid

Vraaggesprek security professional - bestuurder



- Waar accepteren we afhankelijkheid en waar niet?
- Welke OT-assets zijn *crown jewels*?
- Welke leveranciers zijn single points of failure?
- Hoeveel autonomie is economisch verantwoord?



Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties



Weerbaar tegen dreigingen van binnenuit

Herkennen en voorkomen

En anders kunnen we BINGO spelen…

B	I	N	G	O
Windows 365	Data diode	24/7	Sandworm	Wwke
Legacy	SBOM / HBOM	Stuxnet	Patchen	NIS2 / Cbw
Soevereine cloud	Data diefstal	Analoog alternatief	Incident respons	Cyber Resilience Act
Kill Switch	AI Agent	Statelijke actor	Kritieke infrastructuur	ISO 27001
Awareness	Vendor lock-in	Keten-afhankelijkheid	Zero trust	Risico analyse



www.cyberveilignederland.nl



www.cyberveilignederland.nl



liesbeth@cyberveilignederland.nl

www.cyberveilignederland.nl