Het is oorlog

Maar niemand die het ziet … *(Huib Modderkolk 2020)*

In Audit

Ede, 2 juli 2025

Huib Modderkolk

Huib Modderkolk (1982) is onderzoeksjournalist bij de Volkskrant. Hij won de prestigieuze journalistieke prijzen De Tegel (2016) en De Loep (2018 en 2020). Zijn vorige boek, Het is oorlog maar niemand die het ziet, werd een instant bestseller (100.000 keer verkocht), vertaald in het Duits en Engels en stond op de shortlist voor de Brussprijs, de prijs voor het beste journalistieke boek.

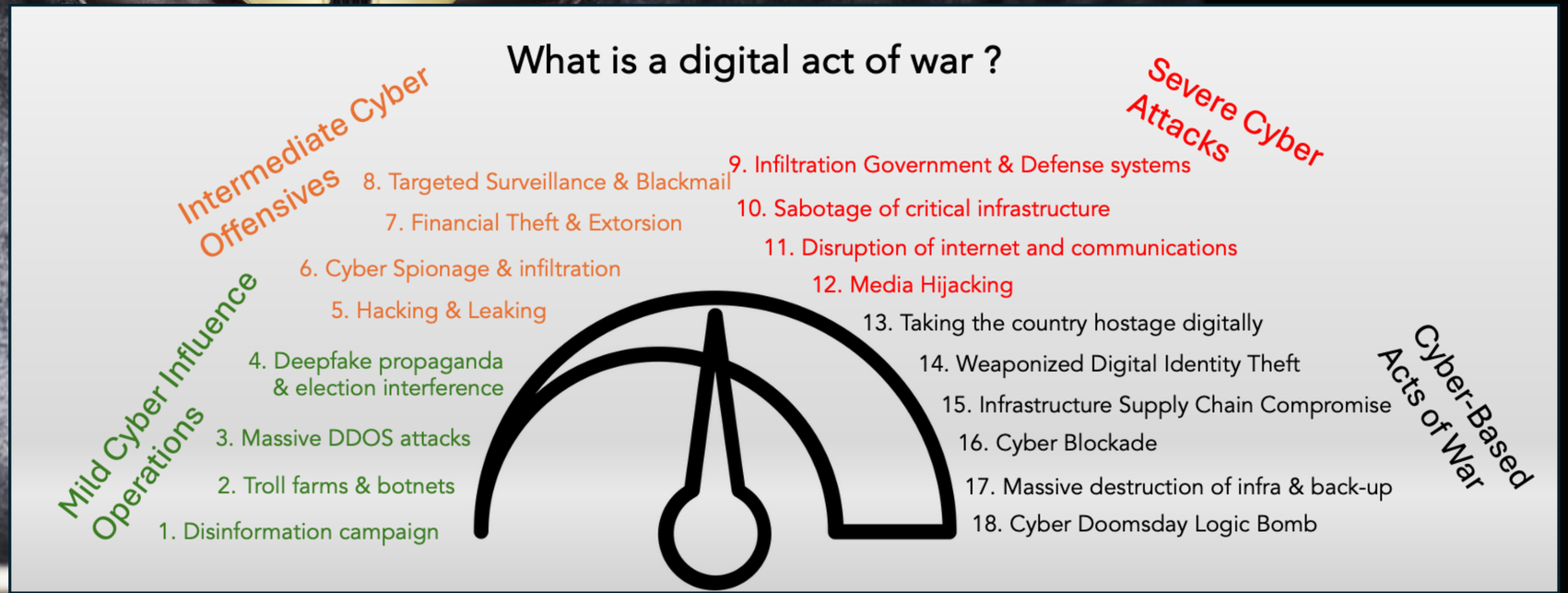
Toon meer

Samenvatting

Onderzoeksjournalist Huib Modderkolk deed jarenlang onderzoek naar de digitale wereld. Hij begon als leek, maar won steeds meer het vertrouwen van bronnen, die hem de schaduwkant van de moderne wereld toonden. Modderkolk beschrijft stapsgewijs hoe groot de afhankelijkheid van technologie is en welke risico's daarmee gepaard gaan. Vijandige regimes dringen ongezien Nederlandse organisaties binnen en overheden en bedrijven slurpen data. Iedere ontdekking roept nieuwe vragen op. Wie leest mee met onze appjes? Hoe ver reiken de tentakels van de Nederlandse veiligheidsdiensten? En hoe kunnen we onszelf beschermen?

Aan de succesvolle eerste editie, die tienmaal herdrukt moest worden, voegde Modderkolk een actueel voorwoord en hoofdstuk toe. Daarin laat hij een nieuw onderdeel van de online strijd zien: het beïnvloeden van het maatschappelijk sentiment. Twee Spanjaarden foppen sociale media, maar verliezen de controle over hun uitvinding. Als het middel vervolgens in Russische handen valt, is de geest uit de fles.

HET IS OORLOG
MAAR NIEMAND DIE HET ZIET
HERZIENE EDITIE
AL 75.000 VERKOCHT!
PODIUM
HUIB MODDERKOLK


What is a digital act of war ?
Severe Cyber Attacks
9. Infiltration Government & Defense systems
10. Sabotage of critical infrastructure
11. Disruption of internet and communications
12. Media Hijacking
13. Taking the country hostage digitally
14. Weaponized Digital Identity Theft
15. Infrastructure Supply Chain Compromise
16. Cyber Blockade
17. Massive destruction of infra & back-up
18. Cyber Doomsday Logic Bomb
Cyber-Based Acts of War
Intermediate Cyber Offensives
8. Targeted Surveillance & Blackmail
7. Financial Theft & Extorsion
6. Cyber Spionage & infiltration
5. Hacking & Leaking
Mild Cyber Influence Operations
4. Deepfake propaganda & election interference
3. Massive DDOS attacks
2. Troll farms & botnets
1. Disinformation campaign

2017 – Maersk - NotPetya
MAERSK
MAERSK
MAERSK
alamy
B B C
2025 – Bybit - Lazarus
Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live
BYBIT
Ben on ETH Wallet Incident
LIVE
BYBIT
Ben | Bybit
EXPLORE MORE
Cyber criminals contact BBC to claim hack on Co-op, M&S
23 May 2025 | World of Business
Chip maker TSMC expands US reach with new Arizona factory
22 May 2025 | World of Business
Week in Markets - 16 May 2025
16 May 2025 | World of Business
India's electric car future
15 May 2025 |
How the largest heist in crypto history happened
Hackers thought to be working for the North Korean regime have successfully converted at least $300m (£232m) of their record-breaking

AEX -0,38% 917,10 | MIDKAP +0,25% 886,00 | EUROSTOXX 50 -0,41% 5.266,91 | BRENT OLIE +0,33% 76,70 | €/$ NEW YORK -0,0522% 1,1484 | RENTE NL 10JR -0,017 2,759%

fd. het financieele dagblad

Donderdag 19 juni 2025 • Nummer 140 • 32 pagina's
'Al het geene tot het financieele eenige betrekking heeft' – sinds 1796

Gavin Newsom
Gouverneur van Californië staat vooraan in de strijd tegen Donald Trump
PAGINA 16

Monetair
Fed houdt de rente nog zeker een maand op huidig niveau van 4,5%
PAGINA 5

Overzicht

PRIVACY EN CYBERSECURITY

Nederland zet zich schrap voor cyberaanvallen tijdens Navo-top

Digitale beveiliging rond het evenement is enorm verhoogd, zeggen cyberexperts

Bert van Dijk en Jasper Houtman
Amsterdam

De bijeenkomst van de Navo volgende week in Nederland betekent een hoger risico op cyberaanvallen, zeggen cyberexperts. Het ministerie van Defensie springt bij om de risico's rond de top van de militaire alliantie in te dammen.

Grote evenementen wekken vaak de interesse van hackers, en een Navo-bijeenkomst vormt daarop geen uitzondering. In de Litouwse hoofdstad Vilnius kwamen er bij de Navo-top in 2023 vanuit Rusland bommeldingen en aanvallen van hackers. Straatlantaarns en verkeerslichten vielen ineens uit. Experts uit Litouwen hebben Nederland geadviseerd, zegt het Nationaal Cyber Security Centrum (NCSC).

De digitale dijkbewaking is enorm verhoogd, zo blijkt uit een rondgang van het FD langs cyberexperts. Het NCSC, dat de digitale weerbaarheid in Nederland moet vergroten, heeft de activiteiten opgeschaald. Cybersecuritybedrijven en netbeheerder Tennet deden hetzelfde. De Rotterdamse haven zegt 'extra maatregelen' te hebben genomen. Er is veel overleg tussen bedrijven en de overheid over dreigingen.

Volgens ceo Dave Maasland van cybersecuritybedrijf Eset Nederland zijn al bewegingen van aanvallers te zien in aanloop naar de top. 'We zien deze maand een verdubbeling van inbraakpogingen op thuiswerksystemen. Maar ook een toename van 75% van phishingaanvallen (oplichting met valse helpdeskberichten en e-mails, red.) op Microsoft-systemen.'

Waar komt het vandaan? Dat is volgens hem moeilijk te zeggen. 'Het is de eerste fase van een aanval, ze zijn nog bezig met scannen wat er openstaat en hoe binnen te komen. Als de aanval wordt uitgevoerd, kun je er meer over zeggen.'

Het NCSC kan het beeld van alvast rondsnuffelende hackers niet bevestigen. 'We zien meer gebeuren. Maar is dat omdat we nu met zijn allen alerter zijn of omdat er daadwerkelijk een toename is? Dat valt nog moeilijk te zeggen', zegt Michiel Kemp, die bij het centrum de coördinatie heeft over cyberweerbaarheid tijdens de top. 'Ook is het de vraag of die activiteiten aan de Navo-top zijn te relateren.'

Voor het eerst springt Defensie bij om een evenement in Nederland te beveiligen tegen cyberaanvallen, zegt Kemp. Reservisten zijn aanwezig bij het 'commandocentrum' waar de cyberdreigingen in de gaten worden gehouden en waar bekeken wordt hoe erop te reageren. Hetzelfde geldt voor cyberexperts van verschillende bedrijfstakken.

'We hebben altijd al overleg met deze bedrijven, maar voor het eerst is iedereen ook fysiek bij elkaar', zegt Kemp. 'We kunnen dan sneller schakelen. Als er iets verstoord raakt, is er tenminste nog iemand om mee af te stemmen. Het is ook prettig om bij onrust elkaar even in het gezicht te kunnen kijken.' De Navo-top is de grootste cyberoperatie die het NCSC heeft meegemaakt. Welke kosten ermee gemoeid zijn, kon Kemp niet zeggen.

Tennet laat weten dat het onderhoudswerkzaamheden eerder heeft uitgevoerd om de kans op verstoringen te verkleinen. De netbeheerder zette een projectgroep op die het bedrijf moet helpen bij cyberacties tijdens de Navo-top. 'Er zijn extra maatregelen getroffen in de storings- en wachtdiensten in de regio zodat monteurs toch snel ter plaatse kunnen zijn in geval van storingen.'

Voor 'cruciale partijen in de Rotterdamse haven' is er onlangs een bijeenkomst geweest waarin met hulp van het NCSC uitleg en adviezen zijn gegeven over mogelijke dreigingen. Welke stappen er al zijn gezet, wil Havenbedrijf Rotterdam niet zeggen. Ook andere partijen houden zich op de vlakte.

Bij het Haagse cybersecuritybedrijf Eye Security is de drukte toegenomen in aanloop naar de top, zegt ceo Job Kuijpers. 'We krijgen veel verzoeken van klanten voor extra ondersteuning en waakzaamheid.'

Vervolg op pagina 3

75%
CYBERSECURITYBEDRIJF ESET NEDERLAND ZIET EEN TOENAME VAN 75% VAN PHISHINGAANVALLEN OP MICROSOFT-SYSTEMEN

Het ministerie van Defensie springt om de risico's rond de Navo-top in te dammen

ILLUSTRATIE: ISTOCK/FD STUDIO

Prijs €4,60

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

› Nieuws ›

DDoS-aanvallen op Nederlandse organisaties rondom NAVO-top

Nieuwsbericht | 23-06-2025 | 16:59

Vandaag is een tiental Nederlandse organisaties, waaronder verschillende gemeenten, het doelwit van DDoS-aanvallen. Diverse media hebben hier vandaag over bericht. Bij dit soort aanvallen vindt geen systeeminbraak of datadiefstal plaats. DDoS-aanvallen passen in de verwachting die het NCSC al eerder schetste in aanloop naar de NAVO-top. De aanvallen zijn voornamelijk gericht op publieke organisaties die zich bezighouden met of een rol hebben rondom de NAVO-top.

Wat is een DDoS-aanval?

Een Distributed Denial-of-Service-aanval (DDoS-aanval) is gericht op het overbelasten van online diensten, servers of netwerkapparatuur. Hierdoor kunnen websites en andere digitale systemen tijdelijk traag of onbereikbaar worden voor gebruikers. Dit kan problemen veroorzaken, zoals het niet kunnen inloggen, of geen toegang hebben tot informatie of

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

› Nieuws ›

Kabinet werkt aan verhogen weerbaarheid tegen militaire en hybride dreigingen

Nieuwsbericht | 06-12-2024 | 15:45

De internationale veiligheidssituatie is de afgelopen jaren in hoog tempo verslechterd. We zien nu al dat Nederland doelwit is van hybride aanvallen, zoals cyberoperaties, spionage en sabotage. Bijvoorbeeld als gevolg van de nietsontziende en grootschalige Russische agressieoorlog tegen Oekraïne is iets wat lange tijd ondenkbaar was mogelijk: dat ons land direct betrokken raakt bij een grootschalig gewapend conflict. Dat conflict hoeft zich niet in Nederland af te spelen maar als we als land betrokken zijn of het zich in de nabijheid van Nederland afspeelt, dan maakt ons dat ook een mogelijk doelwit. We moeten ons dus voorbereiden op onzekere tijden.

Beeld: ©ANP

Daarom heeft het kabinet in kaart gebracht wat er nodig is om weerbaar te zijn tegen militaire of hybride dreigingen. Want hoewel er al een solide basis ligt om de weerbaarheid te versterken, is het niet genoeg. De dreiging vraagt om meer. Een weerbare samenleving helpt bovendien niet alleen tijdens een conflict, maar ook bij het bestrijden van andere crises, zoals grootschalige overstromingen, een pandemie of langdurige uitval van vitale processen. Met een brief die het kabinet vandaag aan de Tweede Kamer verzonden heeft, is een belangrijke eerste stap gezet door inzichtelijk te maken wat er aanvullend nodig is, oftewel de weerbaarheidsopgave.

https://www.nctv.nl/actueel/nieuws/2024/12/06/kabinet-werkt-aan-verhogen-weerbaarheid-tegen-militaire-en-hybride-dreigingen

https://www.nctv.nl/documenten/publicaties/2024/12/06/dreigingsbeeld-hybride-en-militaire-dreigingen

CYBER THREAT ACTORS	FOCUS	DRIJFVEREN
Nation States	*Andere landen, infrastructuur*	Economische of militaire doelen
Criminal groups	*Financiële organisaties, overheden bedrijven & particulieren*	Geld
Terrorist groups	*Overheden, infrastructuur, media en het 'publiek'*	Aandacht en steun
Hacktivists	*Overheden en (grote) organisaties*	Publiciteit (en rechtvaardiging)
Thrill seekers	*Alles en iedereen (wat maar mogelijk is)*	De 'kick' (vaak doorlopend naar criminele betrokkenheid)
Insider threats	*De eigen organisatie (liefst door middel van de 'kroonjuwelen')*	Ontevredenheid, wraak of financieel gewin *(of afpersing/druk door criminelen)*

Cyber Hygiene

Cyber Resilience

#	Group Name	First Known Activity	Origin / Affiliation	Primary Focus
1	**Equation Group**	~2001	U.S. (NSA - suspected)	Espionage (Stuxnet, Duqu, Flame)
2	**APT1 (Comment Crew)**	~2006	China (PLA Unit 61398)	Early IP theft, corporate espionage
3	**Fancy Bear (APT28)**	~2007	Russia (GRU)	Disinformation, military ops, election interference

Cyber Hygiene

Cyber Resilience

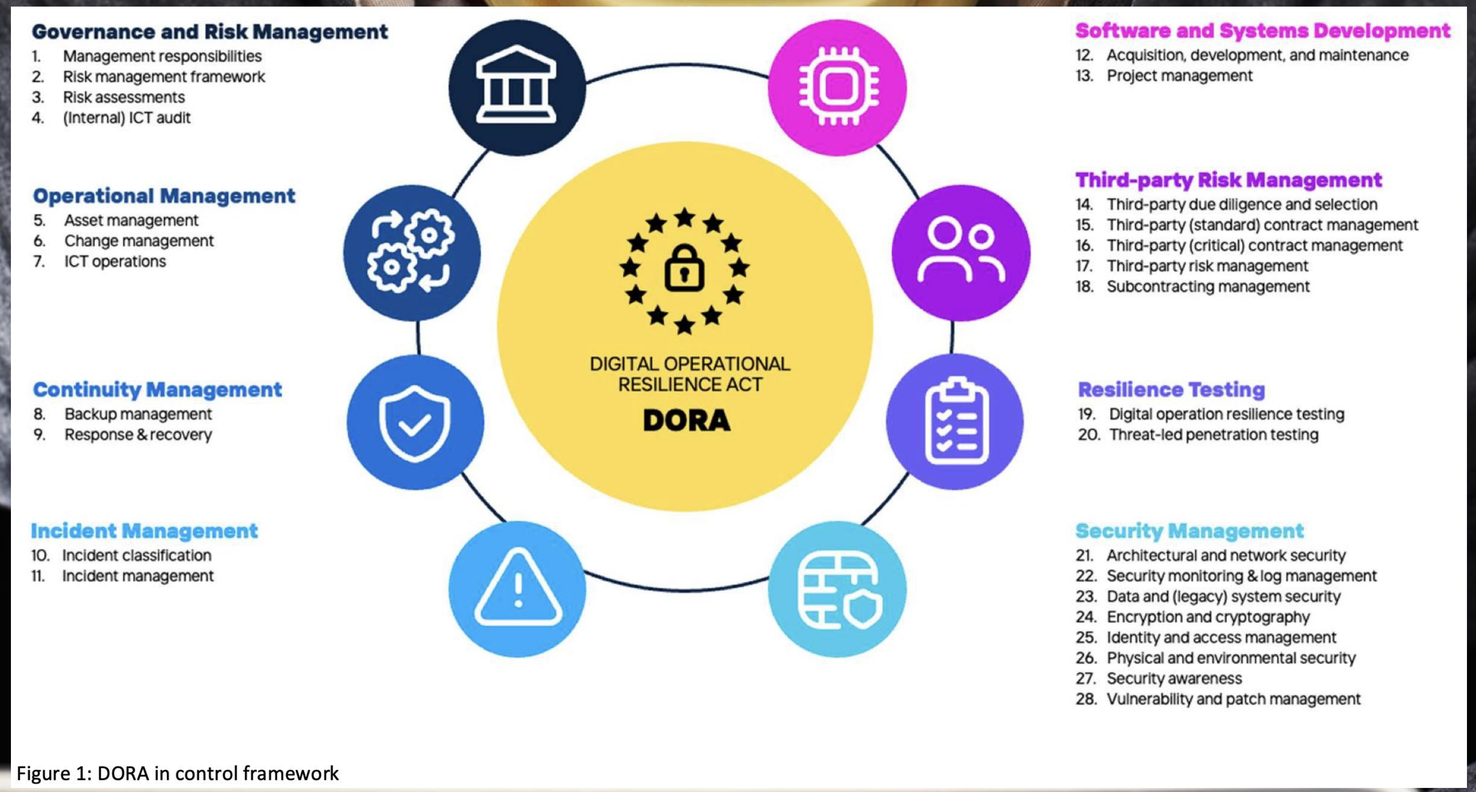


Figure 1: DORA in control framework

DNB: Cyberweerbaarheid in tijden van geopolitieke spanningen

DeNederlandscheBank
EUROSYSTEEM

Nieuws | Thema's | Voor de sector | Onderzoek | Statistieken | Over ons | Werken bij DNB | De Nieuwe Schatkamer

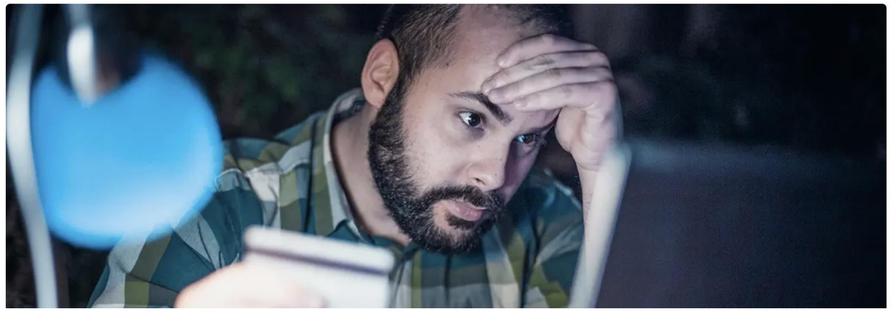
SPEECH

Cyberweerbaarheid in een tijd van geopolitieke spanningen

Lees voor

Wat als er een grootschalige, door een vijandige staat gesponsorde cyberaanval wordt uitgevoerd op de financiële sector van een EU-lidstaat? Hoeveel schade zou dat aanrichten? Hoelang zou het herstel duren? In zijn toespraak tijdens de jaarlijkse FinTech and Regulation Conference in Brussel ging Steven Maijoor vandaag in op deze vragen. Ook sprak hij over de noodzaak om de cyberweerbaarheid in de financiële sector en bij externe dienstverleners waarvan de sector afhankelijk is, verder te vergroten.

Gepubliceerd: 04 februari 2025



*In zijn speech benadrukt Steven Maijoor, directielid van DNB en ECB-toezichthouder, dat de dreiging van grootschalige cyberaanvallen door staten op de financiële sector **reëel en urgent** is.*

Hij wijst op voorbeelden van aanvallen in Oekraïne als wake-up call voor Europa en roept op tot versterking van de cyberweerbaarheid van zowel financiële instellingen als hun ICT-dienstverleners.

*Hij stelt aan de orde dat het bij aanvallen op financiële instellingen lang niet alleen meer gaat om diefstal en afpersing, maar steeds vaker **ook om chaos en wanorde** te creëren.*

*Daarbij is de financiële sector kwetsbaar omdat ze vaak van **dezelfde 'third party ICT providers'** werken.*

De nieuwe Europese DORA-Verordening biedt krachtige instrumenten voor toezicht, onder meer via verplichte penetratietests en strengere eisen aan uitbesteding.

Tot slot benadrukt Maijoor het belang van samenwerking tussen overheden, toezichthouders en vitale sectoren, want "een keten is slechts zo sterk als de zwakste schakel."

In Audit
Information Security

“Het is uit met Amerika”

“Het is uit met Amerika. De verkering is over. Wij hebben liefdesverdriet daarvan en dat kan misschien nog wel even duren.

Maar wij zullen ons daar snel overheen moeten zetten, want

Amerika is niet meer onze vriend”

TV uitzending Buitenhof
26 januari 2025
https://youtu.be/Vi4G0rN1AWY?si=qWepyoXC4FP-kEH5

Sandra Phlippen | Hoofdeconoom ABN AMRO

In Audit
Information Security

Europarlementariër Bart Groothuis waarschuwt: 'Nu of nooit om onze digitale vrijheid veilig te stellen'

Hans Stehouwer • 28 mei 2025 13:15

Een tot dusver onbekende Russische cybergroep met de naam Laundry Bear zit achter de grote hackaanval op de politie van vorig jaar september toen tienduizenden contactgegevens van politiemensen werden gestolen. Dat bleek uit onderzoek van de inlichtingendiensten AIVD en MIVD. Volgens Europarlementariër Bart Groothuis moet Nederland in actie komen om niet digitaal gekoloniseerd te worden.

20 s Samenvatting

Groothuis pleit voor digitale soevereiniteit. Dat is iets anders dan digitale autonomie, zo stelt de politicus in radioprogramma Sven op 1. "Het betekent niet dat je alles zelf moet doen en dat we ons lekker moeten terugtrekken op ons eigen eiland in Europa. We zijn ook afhankelijk en we handelen graag met andere landen. Het is wel zo dat je voor de toekomst strategische beslissingen kunt nemen over hoe je samenleving eruitziet en over je nationale veiligheid. Dat je niet bent overgeleverd aan een ander land."

In Audit
Information Security

Digitale toekomst eu | Artikel

Kim van Sparrentak: “Digitalisering is fucking politiek!”

“Digitalisering is fucking politiek!” Het kwam eruit met een ondertoon van frustratie over de onderhandelingen die ze voert in het Europees Parlement over digitale wetgeving. GroenLinks Europarlementariër Kim van Sparrentak wil dat de mens meer grip krijgt op het internet, maar dat gaat volgens haar niet gebeuren zolang rechtse partijen op de markt blijven vertrouwen. Afgelopen donderdag was ze de hoofdpersoon bij de jaarlijkse lezing ‘De staat van het internet’

Van Sparrentak wil dat Europa digitaal autonoom wordt en dus minder afhankelijk van Big Tech. We kunnen Europese middelen beter inzetten voor Europese initiatieven in plaats van miljarden te steken in Microsoft of Amazon Webservices, stelt ze. Maar dat stuit uiteraard op veel weerstand, want dit grijpt in op de verdienmodellen van grote techbedrijven. En hun invloed in Brussel is flink. “Er worden honderden miljoenen in de techlobby gestoken,” vertelt ze. “Die verdienmodellen moeten op z’n kop. Publieke waarden moeten de basis vormen van technologische vooruitgang, niet de financiële belangen van bedrijven.”

De lezing ‘De staat van het internet’ wordt jaarlijks georganiseerd door Waag Futerelab in samenwerking met de gemeente Amsterdam. Haar uitspraken vinden gehoor in een zaal vol gelijkgestemden in de bibliotheek van Amsterdam. Van Sparrentak is blij dat Waag zich heeft aangesloten bij de coalitie ‘against Big Tech’, die rond de onderhandelingen over de Digital Service Act (DSA) ook de nodige invloed heeft uitgeoefend.

> *“ Zolang de Europese aanbestedingsregels gericht zijn op de goedkoopste aanbieder blijven de grote techbedrijven 'aan de macht'. ”*
>
> *Kim van Sparrentak*

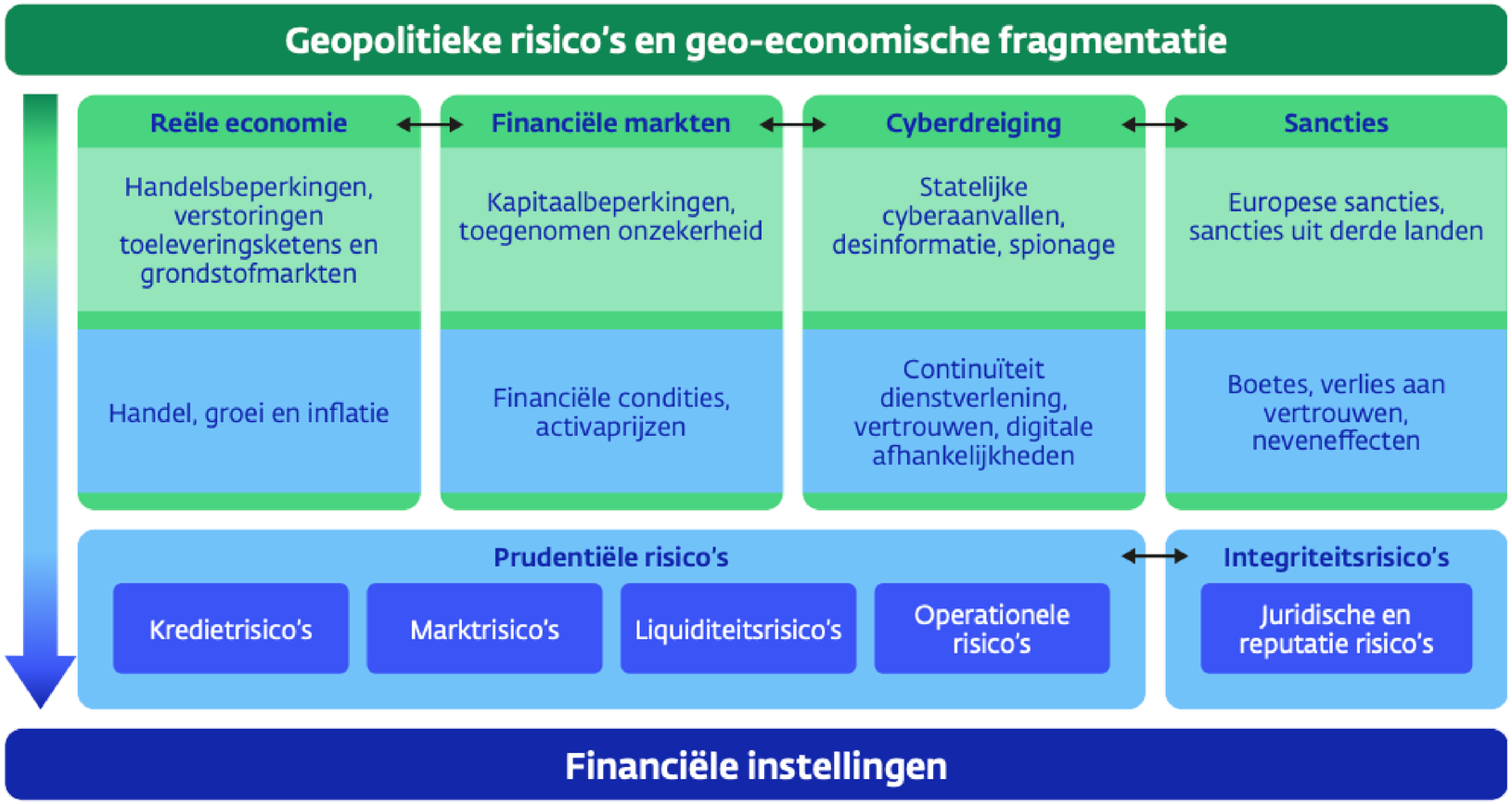
Uit het publiek komt de vraag waarom ze zelf nog steeds op X (voorheen Twitter) zit en niet actief is op Mastodon. Gevoelig puntje… “Ik wil graag X verlaten, maar dan liefst tegelijk met met alle Europarlementariërs,” antwoordt ze. “Anders word qua online zichtbaarheid meteen op achterstand gezet.” Daarmee verwoordt ze precies het dilemma van velen.

Europese cloud onhaalbaar?

Met de DMA wordt er meer mogelijk voor kleinere bedrijven. Nextcloud is een goed alternatief volgens Van Sparrentak. Maar zolang de Europese aanbestedingsregels gericht zijn op de goedkoopste aanbieder blijven de grote techbedrijven ‘aan de macht’. “Dat moet aangepast worden naar een aanbestedingssystematiek waarin strategische autonomie, publieke waarden en duurzaamheid centraal staan.”

In Audit
Information Security

Figuur 1 Geopolitieke ontwikkelingen en risico's voor financiële instellingen

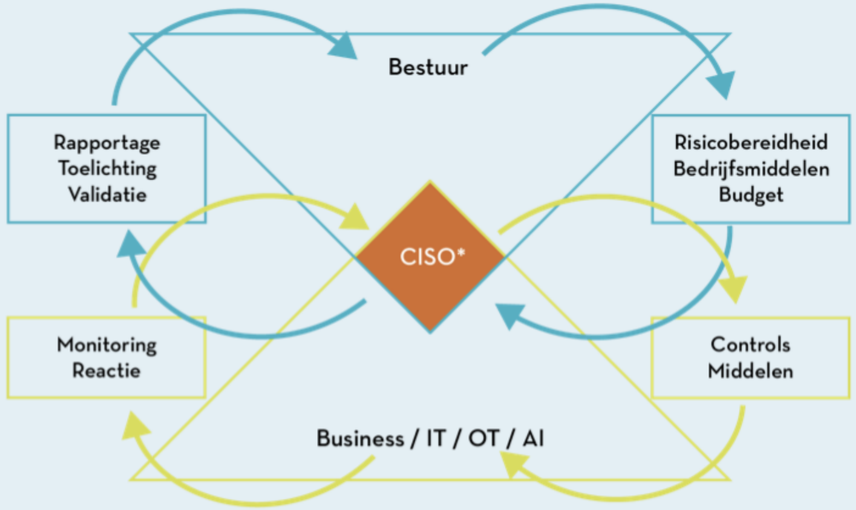


Bron: DNB (2024), mede op basis van IMF (2023).

https://www.dnb.nl/media/1nwjyfr1/weerbaar-in-een-gure-wereld.pdf

In Audit
Information Security

CSR en de rol van de CISO



Bovenstaande figuur illustreert een ideale situatie voor de *cyber governance*, de organisatie van besluitvorming, monitoring, rapportage en toezicht op het beheer van cyberbeveiligings-risico's. Uitgangspunt is dat organisaties een CISO (of vergelijkbare functionaris) aanstellen. De CISO neemt in de cyber governance een centrale positie in en is verantwoordelijk voor het ontwikkelen en uitvoeren van de maatregelen ter beheersing van de cyberbeveiligings-risico's. De CISO werkt hierbij nauw samen met de interne operationele diensten (business, ICT- en OT-operations, innovatie) en de risicobeheer- en auditfuncties.

In Audit
Information Security

Rijksoverheid

https://www.nctv.nl/actueel/nieuws/2024/12/06/kabinet-werkt-aan-verhogen-weerbaarheid-tegen-militaire-en-hybride-dreigingen

Versterken weerbaarheid tegen militaire en hybride dreigingen

Dreigingen

- Wereldwijd meer spanning en conflict
- Strategische rivaliteit
- Hybride dreigingen
- Technologische ontwikkelingen en digitale transformatie

Nationale veiligheidsbelangen

- Fysieke veiligheid
- Internationale rechtsorde en stabiliteit
- Territoriale veiligheid
- Economische veiligheid
- Sociale en politieke stabiliteit
- Ecologische veiligheid

Context

- Veiligheidsstrategie voor het Koninkrijk der Nederlanden
- NAVO
- EU

De opgave

De weerbaarheidsopgave bestaat uit 2 sporen en 6 pijlers:

Maatschappelijke weerbaarheid — Spoor 1

- *Pijler 1* Het beschermen van vitale en andere belangrijke processen in de maatschappij
- *Pijler 2* Een parate en veerkrachtige samenleving
- *Pijler 3* Het overeind houden van de Nederlandse democratie, rechtsstaat en overheid
- *Pijler 4* Een weerbare economie

Militaire paraatheid — Spoor 2

- *Pijler 5* Het beschermen en verdedigen van het eigen en bondgenootschappelijk grondgebied
- *Pijler 6* Het waarborgen van civiele ondersteuning aan de krijgsmacht bij de uitoefening van de militaire taak

Wat betekent dit voor de financiële sector ?

Bestuurders

- *Pijler 1* – Voorzien in informatiebeveiligingsbeleid gericht op continue verbetering en een effectieve positie van de CISO
- *Pijler 2* – Inzicht in de informatie-assets van de organisatie en de hoofdlijnen van de beveiliging daarvan
- *Pijler 3* – Focus op resilience analyses, zoals pentesten, audit rapportages en rapportages van de CISO
- *Pijler 4* – Ter beschikking stellen van voldoende middelen, mankracht en budget voor een effectieve beveiliging

IT management

- *Pijler 5* – Analyse van externe dreigingen en effectiviteit (en aantoonbaarheid) van de controls
- *Pijler 6* – Goede balans realiseren tussen bedrijfsstrategie, risico-analyse en aantoonbare beheersing

Kijk voor meer informatie op ***rijksoverheid.nl/dreiginnederland***

In Audit
Information Security

Qua cyberdreigingen geldt:

"Het is oorlog ..."

In Audit
Information Security

In cybersecurity geldt:

"Als ik maar zorg dat ik beter beveiligd ben dan andere organisaties, dan gaan ze het eerst daar proberen"

In Audit
Information Security

Over digitale souvereiniteit:

"Het is een illusie dat we nog ooit onafhankelijk gaan worden van Amerikaanse Big Tech … en het is ook niet nodig"

In Audit
Information Security

De menselijke scherpte als eerste verdedigingslijn:

"Als we iedereen scherp houden op cyber risico's,
dan houden we de aanvallers buiten"

In Audit
Information Security

Wat geeft jouw organisatie comfort over cyberdreigingen?

"Het is elke dag oorlog en ellende, dus we moeten voortdurend onze verdediging op orde hebben. Dus we hebben onze verdediging ook op orde, door ....."

In Audit
Information Security

Volg onze artikelen over cyber op www.inaudit.nl

In ons laatste magazine:

- Europese Cloudoplossingen
- Cyberbeveiligingswet
- Het ISMS-raamwerk in Confluence

InAudit BV

Spankerenseweg 16A

6974 BC Leuvenheim

T 055 – 303 2597

W www.inaudit.nl

E info@inaudit.nl

In Audit
Information Security