



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Vaste Kamercommissie Digitale Zaken

Technische Briefing #1

woensdag **27 oktober 2021**

Ministerie van Justitie en Veiligheid

Ministerie van Economische Zaken en Klimaat

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties



Aanwezigen

- JenV** Hester Somsen
Plaatsvervangend Nationaal Coördinator Terrorismedbestrijding en Veiligheid
directeur Cybersecurity
- EZK** Focco Vijselaar
Directeur-generaal Bedrijfsleven en Innovatie
- BZK** Erik Akerboom
Directeur-generaal Algemene Inlichtingen en Veiligheidsdienst
- Lourens Visser
CIO Rijk



Opzet van de briefings

Briefing 1: Belang, dreigingen en weerbaarheid

- Opkomende en toekomstige technologieën
- Digitale infrastructuur en economie
- Online veiligheid en cybersecurity

Briefing 2: de burger, de overheid en digitalisering

- Digitale grondrechten, rechtsbescherming en data-ethiek
- Digitaal burgerschap en democratie
- Digitaliserende overheid

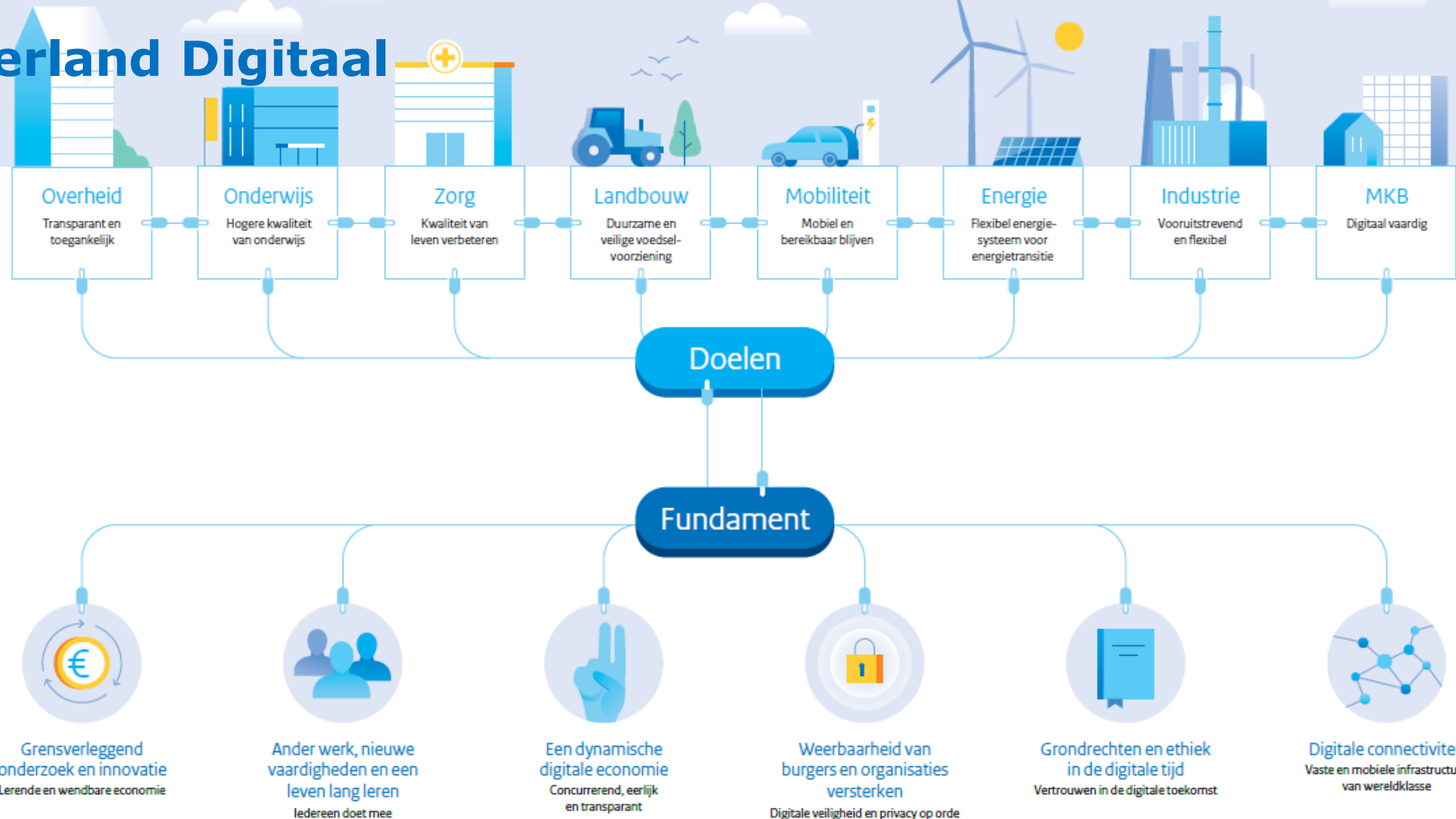


Introductie



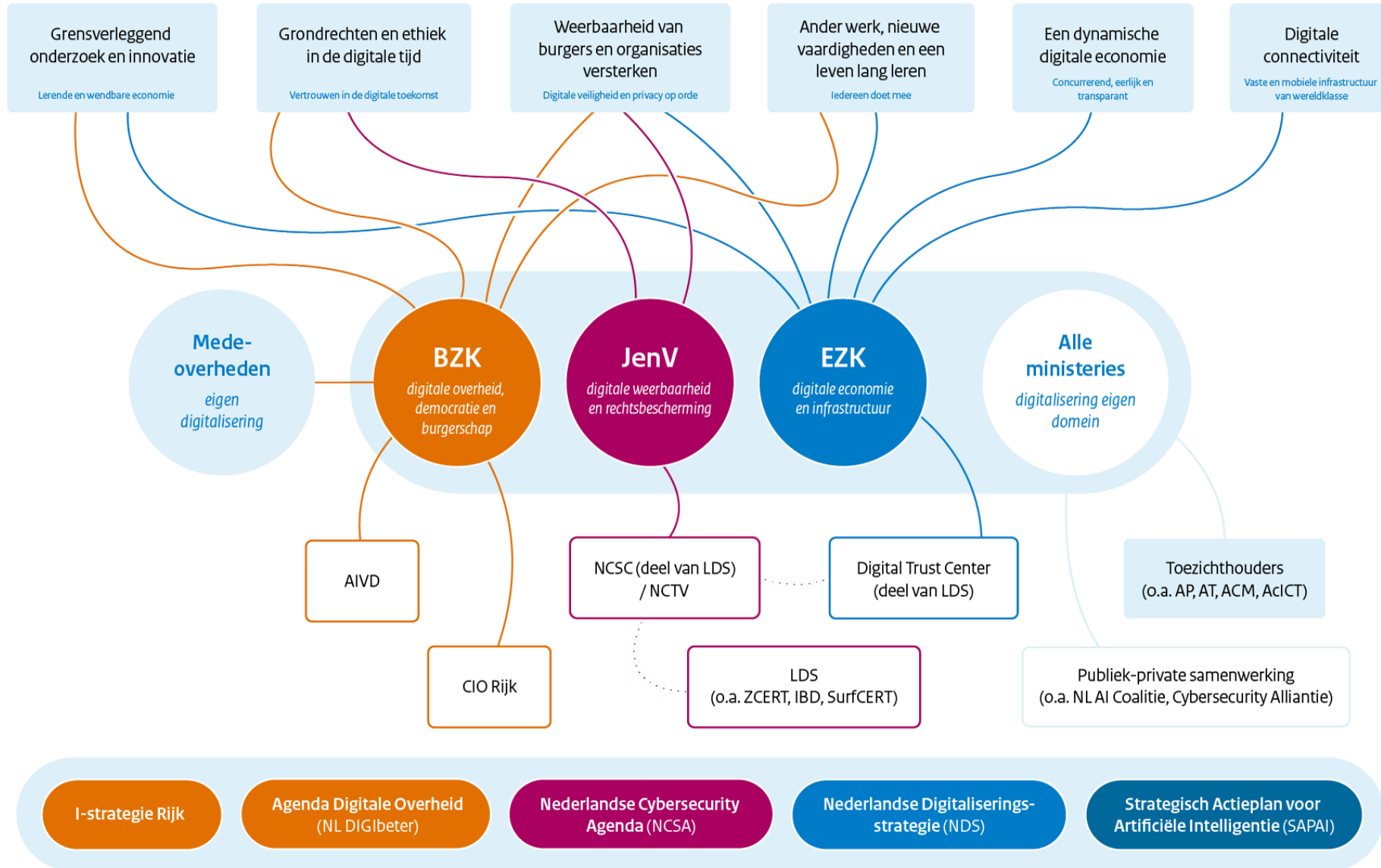


Nederland Digitaal





fundamenten, organisaties en strategieën





Digitale infrastructuur en economie



Digitale infrastructuur en economie

Van kabels en antennes naar data en cloud

Data

- › Kabinetsvisie op datadeling tussen bedrijven
- › Data Sharing Coalition
- › Europese data-strategie
- › Data Governance Act en Data Act

Cloud

- › Verklaring "Towards next generation Cloud Europe"
- › GAIA-X
- › IPCEI CIS (Cloudinfrastructure and Services)





Opkomende en toekomstige technologieën



Online veiligheid en cybersecurity: een weerbare samenleving



Digitale dreiging (1)

Een Nederland om veilig:

- Samen te leven
- Zaken te doen
- Privé te kunnen zijn
- Je mening te uiten
- Te innoveren
- Te leren
- Te werken
- Te kiezen

 – Dreigingsbeeld statelijke actoren

 – Quantum brochure



Digitale dreiging (2)

📖 – 'Offensief cyberprogramma een ideaal businessmodel voor staten'

De Telegraaf

Cyberlek van enorme omvang

Citrix legt Tweede Kamer, Schiphol en gemeenten lam: dit is het probleem

de Volkskrant

COMMENTAAR

Inzake digitale soevereiniteit valt in Nederland nog een wereld te winnen

Nederland past niet op zijn zaak: digitale soevereiniteit verdient een hoge plek op de politieke agenda.

RTLnieuws

5G-netwerken

Huawei definitief uit kern van Nederlandse telecomnetwerken

ED



▲ Werknemers van ASML aan het werk in een cleanroom. © Bart van Overbeeke / ASML

Amerikanen willen dat er nog minder ASML-machines naar China gaan



Digitale weerbaarheid (1)

Waar staan we nu?

- Toenemende digitalisering en toenemende dreiging
- Landelijk Dekkend Stelsel (LDS)
- Wet beveiliging netwerk- en informatiesystemen (Wbni)
- Roadmap digitaal veilige hard- en software



Digitale weerbaarheid (2)

Verwachte ontwikkelingen in de komende vier jaar

- De vrijblijvendheid voorbij:
 - Groter wordende rol voor de overheid
 - Wijziging wettelijk stelsel cybersecurity en vitaal (NIB2-richtlijn)
- Verdieping van cybersecurity, o.a.:
 - Meer aandacht voor ketenkwetsbaarheden
 - Versterken publiek-private samenwerking

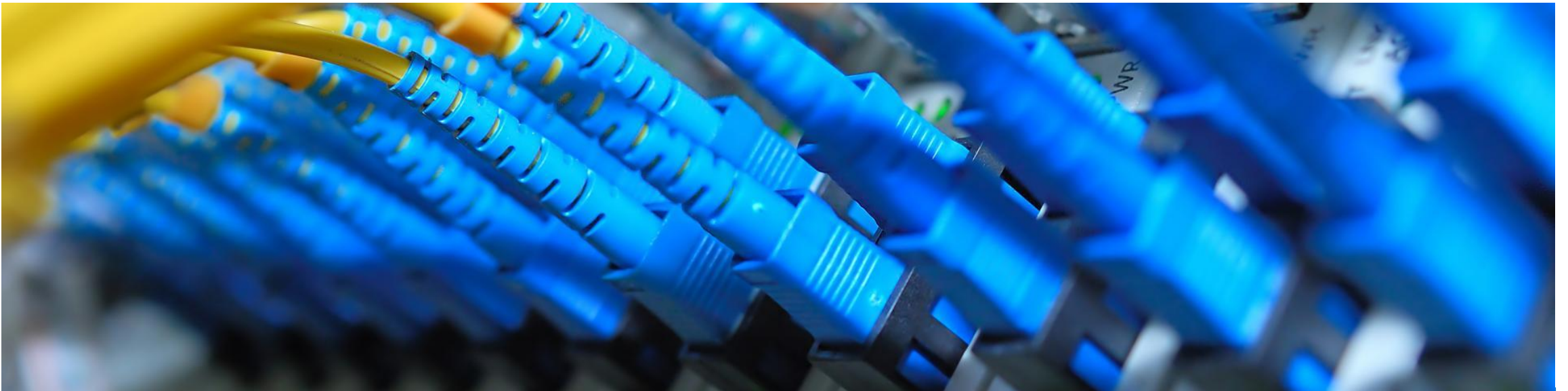


Online veiligheid en cybersecurity: een weerbare overheid



Kaders voor een veilige digitale overheid

- Baseline Informatiebeveiliging Overheid
- Inkooppeisen Cybersecurity Overheid
- Nationale Cryptostrategie





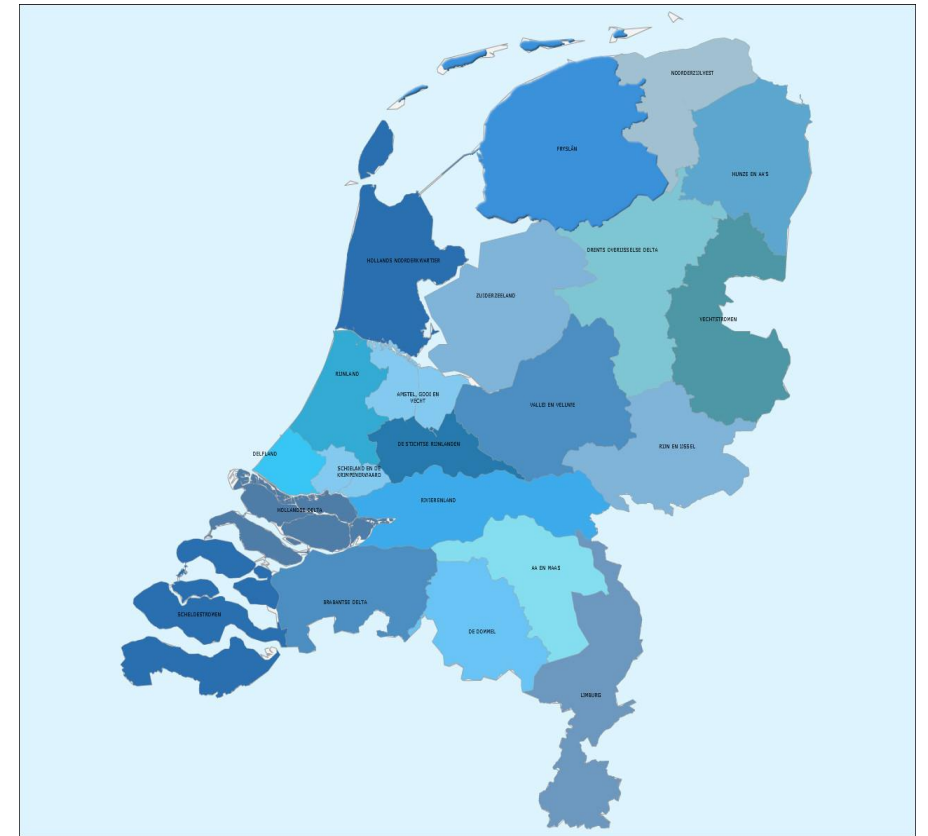
Governance digitale weerbaarheid van de overheid

- Computer Emergency Response Teams

Voor de digitale veiligheid van gemeenten, waterschappen, provincies en het Rijk

- CIO-stelsel Rijksdienst

CISO Rijk & CISO-raad





Vragen, vervolg en verdieping



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Vaste Kamercommissie Digitale Zaken

Technische Briefing #2

donderdag **28 oktober 2021**

Ministerie van Justitie en Veiligheid

Ministerie van Economische Zaken en Klimaat

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties



Aanwezigen

BZK Marieke van Wallenburg
Directeur-generaal Overheid en Organisatie

Wytze van der Woude
Directie Constitutionele Zaken en Wetgeving

JenV Anneke van Dijk
Directeur-generaal Rechtspleging en Rechtshandhaving

Michel van Leeuwen
Directeur Artificiële Intelligentie



Opzet van de briefings

Briefing 1: risico's en kansen van digitalisering

- Online veiligheid en cybersecurity
- Opkomende en toekomstige technologieën
- Digitale infrastructuur en economie

Briefing 2: de burger, de overheid en digitalisering

- Digitale grondrechten, rechtsbescherming en data-ethiek
- Digitaal burgerschap en democratie
- Digitaliserende overheid



Digitale grondrechten en data-ethiek



Inleiding – Grondrechten, rechtsbescherming en data-ethiek

- > Kansen en bescherming
- > Gedeelde verantwoordelijkheid BZK en JenV
- > Als volgt ingedeeld:
 1. Grondrechten en publieke waarden
 2. Rechtsstaat en rechtsbescherming
 3. Gegevensbescherming en data-ethiek



Grondrechten en publieke waarden

- > Verantwoordelijkheid voor een goede werking van de rechtsstaat en bescherming van de grondrechten en publieke waarden
- > Offline en online
- > Een samenleving waarin technologie op een verantwoorde wijze wordt ingezet
- > Door: beschermen en vormen



Grondrechten en publieke waarden: beschermende rol

- › Constitutionele toets
- › Instrumenten:
 - Handreiking non-discriminatie by design
 - Impactassessment mensenrechten en AI
 - Code goed digitaal openbaar bestuur
 - Code kinderrechten online
 - Transparantie instrumenten



Grondrechten en publieke waarden: vormende rol

- > Onderzoek
- > Experimenteren
- > Wetgeving: inzet EU en wijzigen wetgeving (Grondwet)



Grondrechten en publieke waarden: uitdagingen

- › Rechtsstatelijke uitdagingen voor de komende periode
 - Black-box karakter van AI maakt het moeilijker voor uitvoerende en rechtsprekende macht om het bestuur te controleren
 - Vertaling van wetgeving in code/beslisregels



Digitale rechtsstaat en rechtsbescherming

- › Digitale rechtshandhaving: maatschappelijke veiligheid
- › Digitale rechtspleging: invloed Europese regelgeving zoals e-Legislation, e-Law en e-Justice.
- › Digitale rechtsbescherming – borgen van normen voor de bescherming van burgers tegen negatieve inzet van digitalisering.
- › Toezicht en toegang tot het recht: normen in de praktijk, toegang tot het recht, toezicht op persoonsgegevens en algoritmen.



Algoritmische besluitvorming

- › Geen juridisch 'vacuüm'; wel redenen voor actie.
- › Voortgang AI en algoritmen: beleidsagenda normering en toezicht algoritmen. (2021)
- › Europese AI verordening
- › *Soft-law* instrumenten om verantwoorde toepassing van algoritmen te bevorderen: richtlijnen, handreikingen, gedragscodes voor data-ethiek.
- › In ontwikkeling: onderzoek transparantie-instrument voor overheden t.a.v. inzet algoritmen.



Gegevensbescherming en data-ethiek

- AVG en UAVG: AVG evaluatie, UAVG wijzigingen
- Biometrische gegevens: juridisch kader → AVG, Wpg, Wsjg. Gezichtsherkenning, AI verordening en aanverwante systemen.
- Gegevensbescherming voorbij de AVG: aandacht voor gegevensbescherming in aanverwante (EU) wetgeving

- Data Act
- AI Act
- E-privacy

Publiekscampagne horizontale privacy

Register FG

- *Naleving door de overheid:* Punt van aandacht. Onderzoek naar naleving door de overheid



Digitaal burgerschap en democratie: desinformatie



Inleiding – Desinformatie

- > **Definitie:** het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid.
- > **Doel van beleid:** stabiliteit en kwaliteit van onze democratische rechtsorde en onze open samenleving te beschermen, met inbegrip van de vrijheid van meningsuiting en pers.



Desinformatie – beleid

- › Preventie
- › Informatie positie verstevigen
- › (Indien nodig) reageren

- › Uitgangspunt: beschermen van grondrechten



Desinformatie – EU (regulering)

- › Europese trajecten
 - Digital Services Act
 - Europees Democratisch Actieplan
 - Herziening gedragscode tegen desinformatie



Desinformatie – gedragscode tegen desinformatie

- › Aanpakken van het verdienmodel rondom desinformatie;
- › De integriteit van diensten waarborgen (o.a. nepaccounts en bots tegengaan, meer inzicht in werking van algoritmen);
- › Positie en handelingsperspectief van gebruikers verbeteren (o.a. tools om foutieve of misleidende content te rapporteren);
- › Transparantie vergroten rondom politieke en *issue* advertenties;
- › Vergroting van zichtbaarheid van fact-checks en vergroting van de toegang tot data voor onderzoekers;



Desinformatie – uitdagingen

- › Constant ontwikkelende tactieken en technieken
- › Kader voor ongewenste content
 - Niet illegaal, maar wel ongewenste maatschappelijke reactie
 - Desinformatie kan een vorm van ongewenste content zijn
- › Vrijheid van meningsuiting vs bewegingsruimte en veiligheid van burgers online



Digitaliserende overheid



Digitaliserende overheid - Inleiding

- Een digitale samenleving waarin iedereen mee kan doen
- Maatschappelijke opgaven realiseren door verantwoorde en transparante inzet van (nieuwe) technologie
- Een toegankelijke, begrijpelijke, veilige en betrouwbare (digitale) dienstverlening realiseren
- Een Rijksdienst die voorop loopt in het verantwoord benutten van digitalisering voor onze maatschappelijke opgaven.



Digitaliserende overheid - Beleid

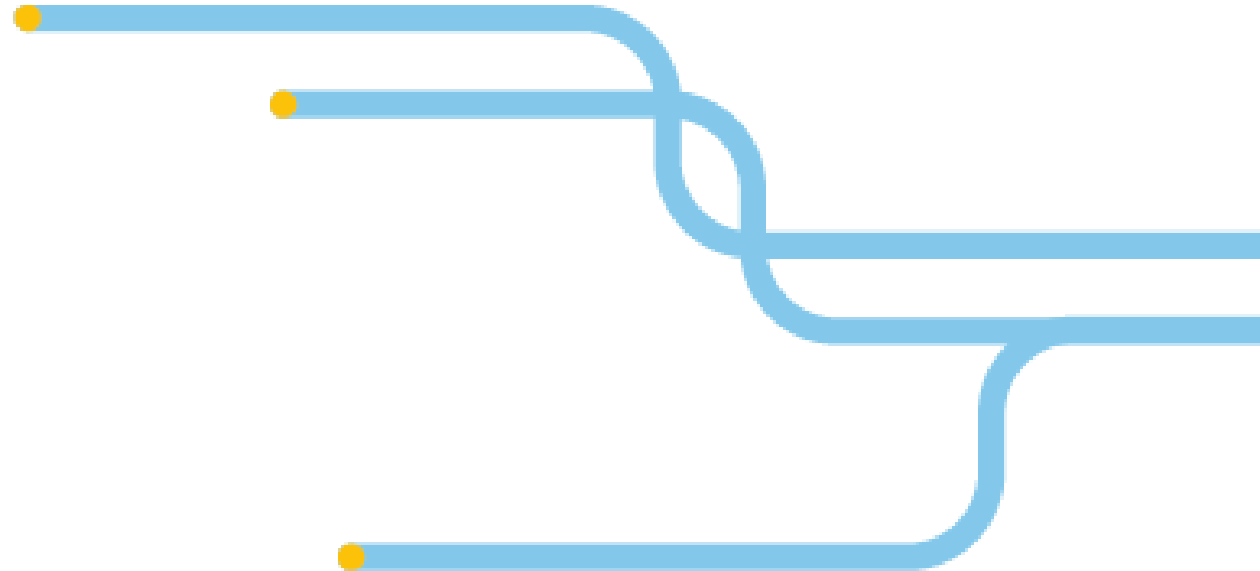
- Een betrouwbare, veilige en robuuste digitale overheidsinfrastructuur onderhouden en vernieuwen.
- Burgers de regie geven over hun eigen gegevens bij de overheid (Regie op Gegevens)
- Een betrouwbare, veilige en

gebruiksvriendelijke digitale identiteit.



Digitaliserende overheid Wetgeving

- Technologie ontwikkelt zich vaak sneller dan in wetgeving gevat kan worden.
- Wetgeving
 - Wet Digitale Overheid (WDO)





I-strategie Rijk 2021-2025

Doorpakken op
digitale transformatie



- 1 I in het hart
- 2 Digitale weerbaarheid
- 3 ICT-landschap
- 4 Generieke voorzieningen
- 5 Informatiehuishouding
- 6 Data en algoritmen
- 7 I-vakmanschap
- 8 Transparantie en inzicht
- 9 I-besturing
- 10 Markt en innovatie



CIO Rijk Rijks ICT-dashboard


- Dé startpagina voor ICT binnen de Rijksoverheid
- Inzicht in de impact van de digitaliserende overheid op onze leefwereld
- Toekomst: burger betrekken bij grote ICT-discussies





CIO Rijk

Meerjarige departementale informatieplannen

- Een plan per departement
 - Met de 5 tot 8 prioritaire doelstellingen
 - Voor de komende 3 tot 5 jaar
 - Vanaf 2022 jaarlijks elke tweede woensdag van november in de Tweede Kamer
- 



Afsluiting en vragen



Afsluiting

- Presentatie en achterliggende stukken worden gedeeld
- Wensen voor mogelijke verdiepende sessies
 - Onbekende kwetsbaarheden
 - Complementaire rol AIVD en NBV
 - Generieke Digitale Infrastructuur
 - Publieke waarden en grondrechten
 - Digitale toegang en identiteit
 - CIO-stelsel en Rijks ICT-dashboard



Relevante stukken

Digitale grondrechten, rechtsbescherming en data-ethiek

Handreiking non-discriminatie by design: [Handreiking non-discriminatie by design | Rapport | Rijksoverheid.nl](#)

Impactassessment mensenrechten en algoritmen: [Impact Assessment Mensenrechten en Algoritmes | Rapport | Rijksoverheid.nl](#)

Code goed digitaal openbaar bestuur: [Code Goed Digitaal Openbaar Bestuur | Rapport | Rijksoverheid.nl](#)

Code voor kinderrechten: [Code voor Kinderrechten](#)

Digitaal Burgerschap en Democratie

Kamerstukken:

Desinformatie strategie: [Beleidsinzet bescherming democratie tegen desinformatie | Tweede Kamer der Staten-Generaal](#)

Ontwikkelingen desinformatie strategie: [Nieuwe ontwikkelingen beleidsinzet bescherming democratie tegen desinformatie | Tweede Kamer der Staten-Generaal](#)

BNC-fiche: Mededeling Europees Democratie Actieplan: [Fiche: Mededeling Europees Democratie Actieplan | Tweede Kamer der Staten-Generaal](#)

BNC-fiche: Mededeling richtsnoeren versterking gedragscode tegen desinformatie: [Fiche: Mededeling richtsnoeren versterking gedragscode tegen desinformatie | Tweede Kamer der Staten-Generaal](#)

Content moderatie en vrijheid van meningsuiting op online platformen: [Content moderatie en vrijheid van meningsuiting op online platformen | Tweede Kamer der Staten-Generaal](#)

Onderzoeken:

Rapport Rathenau in opdracht van BZK: [Digitale dreigingen voor de democratie \(rathenau.nl\)](#)

Rapport Rathenau: [Online ontspoord \(rathenau.nl\)](#)

Rapport UvA/IViR: [het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties](#)

Rapport Rathenau: [tackling_deepfakes_in_european_policy_STOA.pdf \(rathenau.nl\)](#)

Digitaliserende overheid

[I-strategie Rijk 2021-2025 - Digitale Overheid](#)

[Besluit CIO-stelsel Rijksdienst 2021 | Besluit | Rijksoverheid.nl](#)

[Rijks ICT Dashboard](#)