Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 200 VII **Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2023**

36 200 XIII **Vaststelling van de begrotingsstaten van het Ministerie van Economische Zaken en Klimaat (XIII) voor het jaar 2023**

36 200 VI **Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2023**

Nr. 58

VERSLAG HOUDENDE EEN LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 10 november 2022

De vaste commissie voor Digitale Zaken, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer verslag uit te brengen in de vorm van een lijst van vragen met de daarop gegeven antwoorden.

De vragen zijn op 29 september 2022 voorgelegd aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Bij brief van 8 november zijn ze door de Minister van Binnenlandse Zaken en Koninkrijksrelaties beantwoord.

Met de vaststelling van het verslag acht de commissie de openbare behandeling van het wetsvoorstel voldoende voorbereid.

De voorzitter van de commissie,
Kamminga

De griffier van de commissie,
Boeve

kst-36200-VII-58
ISSN 0921 - 7371
's-Gravenhage 2022

Vragen inzake vaststelling van de begrotingsstaten van het Ministerie van Binnelandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2023

1
Welke lokale overheden maken nu al gebruik van open data?

Antwoord
Vanuit het open data portaal worden geen uitgebreide gebruikersanalyses uitgevoerd, dus hier zijn geen specifieke cijfers over. Wel weten we op basis van dataverzoeken, dataleveringen en concrete toepassingen dat veel lokale overheden open data aanleveren en gebruiken.
Open data worden door lokale overheden bijvoorbeeld gebruikt voor de transitievisie warmte en de ontwikkeling van digital twins.
Lokale overheden bieden ook zelf open data aan. Deze data worden bijvoorbeeld gebruikt door marktpartijen die hiermee diensten ontwikkelen, zoals de app OmgevingsAlert waarmee burgers proactief meldingen krijgen als iemand in de wijk een vergunning aanvraagt.
Het beschikbaar stellen van open data is in beperkte mate verplicht onder de huidige implementatie van de Europese open datarichtlijn. Middels de Wet Open Overheid, Wet Hergebruik Overheidsinformatie en de Data Governance Act wordt deze verplichting uitgebreid.

2
Hoeveel mensen maken gebruik van de digitale ondersteuning bij bibliotheken?

Antwoord
Er zijn 19.777 vragen gesteld bij de Informatiepunten Digitale Overheid van 1 januari 2022 tot en met juli in 2022. In totaal sinds de start in 2019 zijn er 44.652 vragen gesteld. De bibliotheken registreren niet het aantal bezoekers maar het aantal gestelde vragen.
In 2021 hebben 6.700 cursisten een Klik en Tik cursus gevolgd bij bibliotheken (in 2019 waren dat er nog circa 12.000). In 2021 hebben 1.057 cursisten Werken met de e-overheid (Digisterker) met certificaat afgerond (in 2019 waren dat er 3.784). Deze daling is veroorzaakt door Covid-19. Eind 2022 verwacht de Koninklijke Bibliotheek hier een verdubbeling op te zien. In 2021 organiseerden de bibliotheken gezamenlijk ruim 13.000 educatieve activiteiten rondom digitalisering. Van de 139 bibliotheekorganisaties hebben 126 het aantal deelnemers opgegeven bij de Koninklijke Bibliotheek. Zij telden in 2021 bijna 58.000 deelnemers aan activiteiten rondom digitale geletterdheid voor volwassenen.

3
Welke acties worden ondernomen om het gebrek aan ICT-personeel op te lossen?

Antwoord
In aanvulling op departementale initiatieven loopt een rijksbreed programma met als doel het Rijk beter in staat te stellen tot het aantrekken, ontwikkelen en behouden van ICT-personeel. Dit programma heeft al de volgende succesvolle initiatieven ondernomen:
- Een rijksbreed I-Traineeprogramma voor het aantrekken van jong ICT-talent;
- Een structurele samenwerking tussen de Rijksoverheid en het hoger onderwijs met als doel de kennispositie van de overheid te versterken en de instroom te vergroten (het I-Partnerschap);
- Gerichte wervingscampagne voor de ICT-doelgroep om de Rijksoverheid als aantrekkelijke werkgever te presenteren.

In de brief «reactie toets op kwalificaties bij selecteren I-personeel» die op 29 september jl. naar uw Kamer is gestuurd wordt verder ingegaan op de stappen die we zetten naar meer competentiegericht werven en actief aan de slag gaan met Rijksorganisaties en de doelgroep om onnodige barrières in het aantrekken en ontwikkelen weg te nemen (Kamerstuk 26 643, nr. 916).

4
Hoe verhoudt de focus op privacybescherming in de begroting van Binnenlandse Zaken en Koninkrijksrelaties (BZK) zich tot de beleidsverantwoordelijkheid voor de Algemene Verordening Gegevensbescherming (AVG) en gegevensbescherming door Justitie en Veiligheid (JenV)?

Antwoord
De Minister voor Rechtsbescherming (MRb) is verantwoordelijk voor het wettelijk stelsel van gegevensbescherming als geheel. De MRb houdt zicht of (een onderdeel van) dat stelsel niet goed werkt. Zodra er overkoepelende vraagstukken spelen ten aanzien van de verwerking van persoonsgegevens raken, raakt dat de stelselverantwoordelijkheid van de MRb. Veel nationale regelgeving met betrekking tot gegevensbescherming is evenwel neergelegd in sectorale wetten. Daarover gaan de departementen zelf onder wiens eindverantwoordelijkheid die sectorale wetgeving tot stand is gekomen, zo ook BZK. De MRb gaat ook niet over de uitvoering van de AVG en het op orde brengen van de werkprocessen bij andere departementen, zoals BZK, maar komt hij wel in beeld als de normen uit de (U)AVG onevenredig zwaar zouden drukken op organisaties.
BZK is verantwoordelijk voor de borging van publieke waarden en mensenrechten bij digitalisering. Het kabinet heeft in de brief «Publieke controle op algoritmen» (Kamerstuk 26 643, nr. 924) de stappen verwoord om onder meer vanuit de AVG, in aanvulling op bestaande wettelijke kaders, burgers beter te beschermen.

5
Wanneer worden de resultaten van het onderzoek naar de AVG-naleving door de overheid verwacht?

Antwoord
Het onderzoek is inmiddels in de eindfase. De eindrapportage wordt omstreeks december van dit jaar verwacht.

6
Kunt u toelichten welke risico's er zijn voor de continuïteit van de Rijksdienst voor Identiteitsgegevens en het realiseren van beleidsdoelen vanwege het verwachte negatieve exploitatieresultaat in de periode 2023–2026?

Antwoord
Het verwachte negatieve exploitatieresultaat levert geen risico's op voor de continuïteit van de Rijksdienst voor Identiteitsgegevens en ook niet voor het realiseren van beleidsdoelen.
Het exploitatieresultaat over eerdere boekjaren met betrekking tot de BRP wordt met de gebruikers van de BRP vereffend door de staffelprijs van de BRP in 2023 en latere jaren te laten dalen ten opzichte van de staffelprijs in 2022. Hierdoor zijn de tarieven in 2023 niet volledig kostendekkend en ontstaat een begroot negatief saldo van baten en lasten. Dit negatieve saldo wordt echter met de openstaande schuld aan gebruikers BRP verrekend. Ultimo 2021 bedraagt de openstaande schuld € 30,1 mln. Er zijn dus voldoende middelen om de kosten te dekken.

7
Kunt u een overzicht geven van voorspellende risicomodellen/algoritmes die worden gebruikt door decentrale overheden, uitvoeringsinstanties en andere overheidsinstanties met het doel om fraude met bijstandsuitkeringen op te sporen?

Antwoord
Decentrale overheden, uitvoeringsinstanties en andere overheidsinstanties hebben veel verschillende algoritmen en risicomodellen in gebruik. Een overzicht van risicomodellen en algoritmen met het doel om fraude met bijstandsuitkeringen op te sporen, is nu nog niet te geven. De Rijksoverheid is momenteel een algoritmeregister aan het opstellen, waarin zal worden geregistreerd welke hoog-risico algoritmes worden ingezet voor welke doelen. De algoritmen die al zijn doorgelicht of onderzocht zullen zoveel mogelijk voor het einde van dit jaar hierin worden opgenomen. Het register wordt bovendien wettelijk verplicht. Een aantal gemeenten en een uitvoeringsorganisatie hebben inmiddels zelf een algoritmeregister opgesteld met in gebruik zijnde algoritmen. Deze zijn te vinden op het overzicht van algoritmeregisters (www.algoritmeregister.nl). Gemeenten, waar de uitvoering en handhaving van de bijstand belegd is, hebben beleidsvrijheid om het toezicht op de bijstand vorm te geven en daarvoor risicomodellen in te zetten. Overigens bleek uit een vragenlijst van de VNG die door 120 gemeenten is ingevuld in het kader van de inventarisatie nationaliteit SZW, dat 80% geen gebruik maakt van risicoselectie om misbruik of oneigenlijk gebruik te detecteren (Kamerstuk 26 448, nr. 653).

Vraag: Worden deze risicomodellen/algoritmes door de desbetreffende overheidsinstantie zelf ontwikkeld of aangekocht bij externe leveranciers?

Antwoord: Deze risicomodellen en algoritmen kunnen zowel door de instanties zelf als door externe leveranciers worden ontwikkeld.

Vraag: Kunt u een overzicht geven van bedrijven of instanties die dergelijke risicomodellen/algoritmes voor overheidsinstanties ontwikkelen?

Antwoord: Dit overzicht is niet te geven, maar op den duur kan het algoritmeregister van de Rijksoverheid ook deze informatie bevatten.

8
Kunt u toelichten op welke manier de Belastingdienst inkomende aanvragen voor kinderopvangtoeslag beoordeelt op juistheid en fraude sinds de afschaffing van het risicoclassificatiemodel? Indien de Belastingdienst gebruik maakt van een voorspellend risicomodel voor het beoordelen van aanvragen voor kinderopvangtoeslag, kunt u toelichten welke voorspellende indicatoren daarbij worden gebruikt?

Antwoord
Bij Toeslagen vinden op dit moment geen activiteiten plaats op het gebied van het intensieve toezicht, te weten de aanpak van misbruik en oneigenlijk gebruik. Toeslagen wil dit proces geborgd opstarten wanneer aan de benodigde randvoorwaarden is voldaan. Daarbij worden verbeteringen doorgevoerd die randvoorwaardelijk zijn in het kader van zorgvuldigheid en rechtsbescherming. De verwachting is dat Toeslagen begin 2023 het proces rond het intensief toezicht weer kan opstarten.
Het reguliere toezicht loopt nog wel door. Een belangrijk deel daarvan vindt plaats in de fase van voorlopige toekenning en daarmee in de actualiteit, zoals de controle op aanvragen met een hoog toeslagbedrag en de controle op zorgverzekerdheid. Ook vinden er thematische

toezichtacties plaats. Denk aan de situatie dat iemand zowel huurtoeslag ontvangt als hypotheekrenteaftrek. Ook wordt aan het einde van een toeslagjaar de definitieve toekenning van de toeslag beoordeeld. Al deze interventies zien op het bevorderen van de naleving. Ook vinden er acties plaats ten behoeve van dienstverlening. Bijvoorbeeld het attenderen dat iemand de AOW-leeftijd heeft bereikt of dat een kind 4 jaar is geworden.

9
Welke voorspellende risicomodellen worden momenteel gebruikt door de Belastingdienst om fraude met regelingen te identificeren?

Antwoord
De Belastingdienst gebruikt geen voorspellende risicomodellen om fraude met regelingen te identificeren. De Belastingdienst gebruikt risicomodellen om in verschillende werkprocessen selecties te kunnen maken van aangiften en/of aanvragen die nader handmatig onderzoek vragen. Deze risicomodellen worden ingezet in bijvoorbeeld de Omzetbelasting.

10
Kunt u een overzicht geven van voorspellende risicomodellen/algoritmes die worden gebruikt door decentrale overheden, uitvoeringsinstanties en andere overheidsinstanties?

Antwoord
Nee, er bestaat geen dergelijk overzicht. Momenteel worden wel meer algoritmische toepassingen waaronder voorspellende risicomodellen onderzocht, getoetst en afgewogen. Dat gebeurt door de Audit Dienst Rijk en de Algemene Rekenkamer of door onafhankelijke onderzoeken van bijvoorbeeld het Rathenau Instituut. Dit najaar wordt het algoritmeregister gelanceerd en is de verwachting dat in de loop van 2023 dit register geleidelijk gevuld gaat worden met tenminste hoog risico algoritmen waartoe ook voorspellende risicomodellen toebehoren. Het overzicht zal dus geleidelijk toenemen.

11
Hoe verhouden de digitaliseringsinvesteringen door BZK zich tot de budgetten die worden toebedeeld aan de digitale toezichthouders, zoals de Autoriteit Persoonsgegevens?

Antwoord

Zie het antwoord op vraag 182.

12
Kunt u de opbrengsten van het Kadaster uiteenzetten met de handel van persoonsgegevens?

Antwoord
Kadaster brengt kostendekkende tarieven in rekening, zonder enig winstoogmerk, voor de uitoefening van de publieke taak om inzicht te bieden in de rechten en beperkingen en de betrokken rechthebbenden, die zijn geregistreerd in de Basisregistratie Kadaster. Deze wettelijke levering van informatie is cruciaal voor de rechtszekerheid in Nederland. Op basis daarvan stelt het Kadaster deze informatie mede beschikbaar aan private partijen. Deze dataleveringen zijn strikt gekoppeld aan de doeleinden zoals geformuleerd in de Kadasterwet, en vastgelegd in contracten. Naast een duidelijke doelbindingtoets is er bijvoorbeeld een verbod op direct marketing. De vastgoedeconomie in Nederland is in grote mate afhankelijk van de dienstverlening en dataverstrekking van het Kadaster. Dit

betreft onder andere dataleveringen aan private/commerciële partijen zoals het notariaat, de makelaardij, banken en taxatiekantoren.

13
Zijn er financiële middelen nodig om te investeren in één overheidsloket voor digitale dienstverlening en zo ja, waar zijn die terug te vinden op de rijksbegroting?

Antwoord
Ja, er zijn financiële middelen, die onderdeel zijn van artikel 6.7 hoogwaardige dienstverlening één overheid. In samenhang wordt gewerkt aan initiatieven die ervoor zorgen dat een burger en ondernemer bij het gebruik van publieke dienstverlening altijd naar behoefte worden geholpen, ongeacht welk kanaal zij kiezen. De dienstverlening wordt zoveel mogelijk georganiseerd rondom levensgebeurtenissen, tenzij er sprake is van specifiek gerichte dienstverlening vanuit één dienstverlener en/of één concreet product. Initiatieven waar het om gaat zijn:

- Verbeteren van de informatievoorziening, inclusief klantcontact, via de overheidsbrede kanalen.
- Invulling geven aan de toepassing van Omnichannel op verschillende overheidskanalen.
- Uitbreiding van de Informatiepunten Digitale Overheid (IDO's) met meer locaties (aantal en vindplaatsen) en ontwikkelen tot informatiepunten publieke dienstverlening door uitbreiding van de aangeboden producten en diensten.
- Onderzoeken welke elementen van de loketfunctie effectief voor burgers zijn en deze implementeren door kleinschalig hiermee te starten.

Gezamenlijke overheidsbrede principes, standaarden en instrumenten voor dienstverlening worden opgesteld, gedeeld en onderhouden. In 2023 helpen we bestuursorganen met een leertraject om invulling te geven aan de zorgplicht.

De volgende financiële middelen zijn reeds toegekend om dit te kunnen realiseren:

Onderdeel	Financiële middelen 2023
Realiseren van een website, inclusief klantcontact, waar informatie in samenhang en rondom levensgebeurtenissen wordt aangeboden.	€ 6,6 mln.
(door)Ontwikkelen Levensgebeurtenissen.	€ 1,3 mln.
Ontwikkelen Omnichannel.	€ 3,98 mln.
Verbreding en uitbreiding IDO's.	€ 20,95 mln.
Lerend bouwen aan de loketfunctie	€ 2,8 mln.

14
Kunt u, als regievoerder van het digitaliseringsbeleid, een overzicht geven van alle investeringen in een stevig digitaal fundament en daarbij aangeven waar de benodigde middelen voor het digitaliseringsbeleid bij de verschillende departementen zijn begroot?

Antwoord
Nee dat kan nog niet. Uw Kamer ontvangt in november van alle departementen een meerjarig informatieplan.
Ook heeft uw Kamer ontvangt recent de «Werkagenda Waardengedreven Digitaliseren» met aanvullende informatie voor een stevig digitaal fundament ontvangen (Kamerstuk 2022Z21101).

15
Kan worden toegelicht wat de inzet is bij de vertaling van de aankomende Europese digitale wetgeving naar de Nederlandse context, alsook hoe partijen die dit implementeren gaan worden ondersteund?

Antwoord
Het kabinet maakt de implementeerbaarheid voor private en publieke partijen, waaronder toezicht en handhaving, en publieke waarden structureel tot onderdeel van de Europese inbreng. Daarbij zet het kabinet in op duidelijkheid en samenhang voor de gebruikers. Om partijen hierin te ondersteunen denkt het kabinet aan de inrichting van aanvullende ondersteunende instrumenten in afstemming met toezichthouders en private sector. Om de behoeftes goed in kaart te brengen wordt nauw contact onderhouden met belanghebbenden.

16
Kunt u toelichten wat u precies gaat doen als u schrijft werk te gaan maken van de vertaling van Europese wetgeving naar de Nederlandse context en partijen die dit implementeren actief zal gaan ondersteunen?

Antwoord
Zie het antwoord op vraag 15.

17
Welke stappen zijn al ondernomen om de Europese wetgeving, zoals de Digital Governance Act (DGA), de Digital Markets Act (DMA), eIDAS-Verordening en de Digital Services Act (DSA), te vertalen naar de Nederlandse context?

Antwoord
Over de nieuwe eIDAS-verordening wordt momenteel nog onderhandeld. Het definitieve voorstel is nog niet bekend, waardoor nog niet geheel duidelijk is welke stappen nodig zijn om deze te vertalen voor de Nederlandse context.
Voor de DGA, DMA, en DSA wordt u verwezen naar de beantwoording van de vragen 58 t/m 61 door de Minister van Economische Zaken en Klimaat.

18
Wat wordt bedoeld met de zin «We introduceren een Nederlandse publieke, vrijwillig te gebruiken, open source wallet en ontsluiten relevante gegevensbronnen»?

Antwoord
Om te zorgen dat alle burgers en bedrijven, volgens de doelstelling van de EU-verordening (eIDAS), in 2025 gebruik kunnen maken van een hoogwaardige ID-wallet zal het gestarte programma EDI Stelsel NL een eerste versie van een Nederlandse open source wallet neerzetten. Deze eerste wallet zal nadrukkelijk als open source voorbeeld dienen.

Open source bevordert dat het ontwerp en de werking van de wallet volledig transparant zullen zijn en door eenieder gecontroleerd zal kunnen worden. Dit draagt naast transparantie ook bij aan de kwaliteit van de code en volgt het uitgedragen beleid van «open source, tenzij». Uiteindelijk wordt in Nederland, naar voorbeeld van het stelsel van Toegang dat de Wet Digitale Overheid introduceert, een stelsel van wallets voorzien die voldoen aan de waarden en principes die wij belangrijk vinden.
In de Telecomraad van 3 juni 2022 heeft de Staatssecretaris van BZK benadrukt dat het gebruik van wallets vrijwillig moet zijn en dat burgers alternatieven moeten kunnen kiezen in het overheidsdomein, zoals ons

huidige DigiD (conform motie leden Van Haga en Leijten, Kamerstukken II 2021/22, 26 643, nr. 831).

De inrichting van de Nederlandse invulling van het Europese Digitale Identiteit raamwerk zal onder andere bestaan uit voorzieningen en afspraken om wallets te kunnen vullen met gegevens uit overheidsregisters. Het «ontsluiten van relevante gegevensbronnen» doelt op het voor burgers mogelijk maken om gegevens in je ID-wallet te zetten (Kamerstuk 26 643, nr. 902).

19
Kunt u toelichten hoe de vier thema's uit de hoofdlijnenbrief zich verhouden tot de vijf lijnen in de nog te ontvangen Werkagenda?

Antwoord
De «Werkagenda Waardengedreven Digitaliseren» vormt de komende jaren in principe de basis voor het beleid voor digitalisering van de samenleving, de overheid en het Rijk (Kamerstuk 2022Z21101). Centraal daarbij staan de mens, de samenleving en onze publieke waarden.
De eerste versie van deze werkagenda die in november aan uw kamer is gestuurd richt zich met lijnen 1, 2 en 3 op het digitale fundament en met lijn 4 op de digitale overheid. Lijn 5 van de werkagenda richt zich specifiek op het versterken van de digitale samenleving in het Caribisch deel van het Koninkrijk. De vijf lijnen vormen een geheel en zijn in hun uitwerking complementair aan elkaar.
Over de digitale economie (onderdeel 4 uit de hoofdlijnenbrief) heeft de Minister van Economische Zaken en Klimaat u toegezegd nog dit jaar een Kamerbrief toe te sturen. Onderdeel van het digitale fundament is cyberveiligheid, dit is onderdeel van de Nederlandse Cybersecurity Strategie die uw Kamer van de Minister van Justitie en Veiligheid heeft ontvangen.

20
Welke en hoeveel (financiële) middelen zijn de komende jaren nodig om te investeren in een stevig (digitaal) fundament en waar zijn de benodigde financiële middelen begroot op de rijksbegroting?

Antwoord
Zie het antwoord op vraag 14.

21
In hoeverre worden extra financiële middelen begroot voor het versterken van het toezicht op het gebruik van gegevens en algoritmes? Indien hiervoor extra middelen worden begroot, kunt u toelichten op welke begrotingsartikelen die extra middelen zijn begroot?

Antwoord
In het Coalitieakkoord staat vermeld dat er een algoritmetoezichthouder komt die regelt dat algoritmen gecontroleerd worden op transparantie, discriminatie en willekeur. In de budgettaire bijlage staan hiervoor vanaf 2023 middelen toegewezen aan de Autoriteit Persoonsgegevens. Het gaat om:

2023	2024	2025	Vanaf 2026
€ 1 mln.	€ 3 mln.	€ 3,6 mln.	Structureel € 3,6 mln.

Als het om de naleving van de Algemene verordening gegevensbescherming (AVG) gaat wordt het budget van de Autoriteit Persoonsge-

gevens structureel verhoogd. In 2023 en 2024 is er respectievelijk € 4 en € 6 mln. extra en vanaf 2025 komt er structureel € 8 mln. bij.
De begroting van de AP valt onder de budgetverantwoordelijkheid van het Ministerie van Justitie en Veiligheid (conform artikel 11 Uitvoeringswet Algemene verordening gegevensbescherming).

22
Welke en hoeveel (financiële) middelen zijn nodig om te investeren in één overheidsloket voor (digitale) dienstverlening en waar zijn die terug te vinden op de rijksbegroting?

Antwoord
Zie het antwoord op vraag 13.

23
Wat wordt bedoeld met «een federatief datastelsel voor het rechtmatig delen van (bron)gegevens»?

Antwoord
Het organiseren van een federatief datastelsel heeft tot doel om gegevens binnen de overheid – over organisatie- en sectorgrenzen heen – op een verantwoorde en veilige manier te gebruiken om maatschappelijke opgaven te realiseren en de dienstverlening van de overheid verder te verbeteren. Dat doen we door het maken van overheidsbrede afspraken en standaarden zodat publieke waarden zoals transparantie voor de burger, privacy by default en dataminimalisatie onderdeel zijn van de manier waarop overheidsorganisaties gegevens delen. Federatief wil zeggen dat er ruimte is voor sectorspecifieke eisen en toepassingen, zo vraagt de omgang met gegevens in de zorg andere afspraken dan de meer open data in de ruimtelijke omgeving. Het federatief datastelsel bouwt voort op het huidige stelsel van basisregistraties en is een van de bouwstenen van de Interbestuurlijke Datastrategie (Kamerstuk 26 643, nr. 797).

24
Kunt u toelichten met welk doel en verwacht resultaat geld vanuit het programma Werk aan Uitvoering aan artikel 6 is bijgedragen?

Antwoord
In totaal is voor 2023 een bedrag van € 74.4 mln toegevoegd vanuit Werk aan Uitvoering aan artikel 6. Deze toevoeging bestaat uit bijdragen aan de centrale financiering van de Generieke Digitale Infrastructuur (56,2 mln), Regie op Gegevens (1,8 mln), digitale identiteit (2,6 mln), de datastrategie (9,5 mln), het bouwen aan de loketfunctie en de Single Digital Gateway/ YourEurope (1,5 mln).
Met deze middelen wordt:
- De verbreding van het gebruik van de GDI ondersteund.
- Gaan we voor regie op gegevens inzage bieden in welke type persoonsgegevens de overheid voor overheidsbesluiten gebruikt.
- Uitvoering geven aan de Interbestuurlijke Datastrategie Nederland, dat streeft naar verantwoord datagebruik voor maatschappelijke opgaven. Binnen dit programma worden diverse projecten uitgevoerd, waaronder:
    - o Adviesfunctie verantwoord datagebruik, waarmee overheidspartijen onafhankelijk advies krijgen bij afwegingen tussen wat er kan en mag met data;
    - o Het organiseren van een aantal «datadialogen», waarmee het politiek-bestuurlijke gesprek wordt gefaciliteerd rondom publieke waarden en waardenspanning bij datagebruik.

- Uitvoeringsplan voor de ontwikkeling van een federatief datastelsel, dat de doorontwikkeling is van het huidige stelsel van basisregistraties. In 2023 wordt gewerkt aan een technische standaard om op meta-niveau inzicht te krijgen in het aanbod van open en gesloten data binnen de overheid.
- Interbestuurlijk kenniscentrum: zetten van eerste stappen om te komen tot een kenniscentrum waarin o.a. best practices rondom datagebruik interbestuurlijk worden gedeeld.
- Ondersteunen van en onderzoek naar concrete «use cases», waar rode draden uit worden gedistilleerd om tot een beter functionerend ecosysteem te komen om data op verantwoorde wijze in te zetten voor maatschappelijke opgaven.

- Wordt gewerkt aan nieuwe EU-ontwikkelingen op het gebied van digitale identiteit en de wallet.
- Wordt de implementatie van de EU-verordening voor de Single Digital Gateway gefinancierd.

25
Wat wordt bedoeld met «een centraal digitaal loket binnen Europa»?

Antwoord
Op grond van de Single Digital Gateway (SDG)-verordening krijgen burgers en ondernemers die in Europa willen wonen, werken, studeren of ondernemen via een centraal digitaal loket, Your Europe, op een eenvoudige manier toegang tot relevante overheidsdienstverlening van alle lidstaten. Dit centrale loket verwijst gebruikers vervolgens door naar de juiste website in de lidstaat waar zij iets willen regelen.

26
Kunt u toelichten hoeveel uitgaven in 2023 en verder begroot zijn die samenhangen met de ontwikkeling en voorbereiding op de Europese digitale identiteit? Waar zijn deze uitgaven op de begroting terug te vinden?

Antwoord
Deze vraag is lastig exact te beantwoorden omdat de onderhandelingen over het Europese wetsvoorstel (Europese Digitale Identiteit Raamwerk/ eIDAS revisie) momenteel nog lopen. Momenteel worden er vooral voorbereidende activiteiten gedaan, zoals het opbouwen van een programma en voorbereiden van het werk aan een publieke wallet. Deze uitgaven worden voor 2023 bekostigd uit de begrotingspost voor de Generieke Digitale Infrastructuur, artikel 6.8 en voor een klein deel uit middelen vanuit het identiteitsstelsel artikel 6.5.

27
Hoeveel geld is er begroot voor de Europese digitale identiteit? Hoeveel voor de Nederlandse?

Antwoord
De totale kosten voor de EU worden ingeschat op ruim € 3 miljard en betreffen vooral de kosten om publieke instanties gereed te maken voor uitwisseling van attributen uit authentieke bronnen en voor het realiseren en aanbieden van attributen door vertrouwensdiensten. De baten worden afhankelijk van de adoptiegraad door de EU ingeschat op bijna € 4 tot 10 miljard.
De Europese Commissie heeft voor vier Large Scale Pilots (LSP's) een bedrag van € 37 miljoen ter beschikking gesteld. De LSP's zullen officieel van start gaan in 2023 en kennen een doorlooptijd van 24 tot 36 maanden. Voor de Europese prototype wallet heeft de EU een tender uitgegeven

voor € 26 miljoen (Kamerstuk 22 112, nr. 3161 en Kamerstuk 26 643, nr. 902).
Zie voor de Nederlandse activiteiten het antwoord onder vraag 26.

28
Zorgt het nieuwe begrotingsartikel 6.8 ervoor dat er meer of minder geld dan voorheen beschikbaar is voor de Generieke Digitale Infrastructuur (GDI)? Kunt u toelichten of met het nieuwe artikel 6.8 meer geld dan voorheen beschikbaar is voor de GDI? Kunt u inzichtelijk maken hoeveel geld sinds 2019 beschikbaar was voor de GDI?

Antwoord
Met het begrotingsartikel 6.8 neemt het beschikbare budget voor de Generieke Digitale Infrastructuur (GDI) toe. Dat wordt mogelijk door de interbestuurlijke afspraken over de centrale financiering van de GDI m.i.v. 2023. Het budget wordt grotendeels gebruikt voor de beheer- en exploitatiekosten van de GDI. Beheer en exploitatie wordt uitgevoerd door Logius, KvK, RVO en RvIG. Ook de kosten van de doorontwikkeling en vernieuwing van de GDI worden uit dit budget betaald. In de onderstaande tabel is de ontwikkeling van de kosten van Logius en van de doorontwikkeling en vernieuwing vanaf 2019 opgenomen. Logius beheert meer dan 90% van de GDI, hierdoor geeft deze reeks een goed inzicht in het beschikbare budget, de kosten van de andere beheerorganisaties zijn jaarlijks constant.
In de onderstaande tabel is de ontwikkeling van de kosten van Logius en van de doorontwikkeling en vernieuwing vanaf 2019 opgenomen.

(v € 1 mln)	2019	2020	2021	2022	2023
Budget GDI	173,7	227,2	250,0	259,6	277,2

29
Kunt u in een tabel uiteenzetten waar het coalitieakkoord geld voor de inlichtingendiensten exact heen is gegaan? Kunt u vermelden welk deel van dit geld naar cybersecurity gaat?

Antwoord
Een substantieel deel van de beschikbare middelen zal worden ingezet om de slagkracht van de AIVD en MIVD te versterken, de diensten (technologisch) toekomstbestendig te maken en samen met partners een stap te zetten om de Nederlandse samenleving digitaal weerbaarder te maken. Daarnaast worden noodzakelijke intensiveringen gedaan op het terrein van cyber, economische veiligheid, vitale belangen en processen, en rechtsterrorisme. Het Ministerie van BZK kan niet in gaan op de exacte wijze waarop de diensten hun (extra) middelen hebben verdeeld. Wel kan het Ministerie van BZK aangeven dat cyberveiligheid onderdeel uitmaakt van deze verdeling, en ook nu al continue aandacht van de diensten heeft. Met Prinsjesdag is de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) vertrouwelijk geïnformeerd over de geheim gerubriceerde aspecten van de begroting van de AIVD.

30
Kunt u toelichten wat er wordt bedoeld met de reallocatie van de middelen voor de aanpak van digibetisme? Hoe worden de middelen die in het coalitieakkoord zijn opgenomen aangewend en hoe wordt de publiek-private aanpak uitgevoerd?

Antwoord
Met reallocatie wordt bedoeld dat de middelen voor het verbeteren van digitale vaardigheden geboekt worden op een ander financieel instrument. Dit betreft dus slechts een administratieve correctie waarbij de middelen beschikbaar komen voor uitgaven aan beleidsactiviteiten in plaats van externe inhuur voor personele capaciteit.
De middelen voor 2023 zullen voor het overgrote deel in lijn met 2022 worden besteed via een publiek-private aanpak. Belangrijke thema's daarin zijn de randvoorwaarden voor vaardigheden zoals apparaten en voldoende onderwijs- en opleidingsaanbod voor jong en oud, voor doelgroepen zonder vaardigheden en de meer gevorderden. Het grootste deel is in 2022 ingezet voor het verbeteren van digitale vaardigheden via een publiek-private aanpak vanuit de Alliantie Digitaal Samenleven. Dit is een netwerk van publieke en private partijen, opgericht door Vodafone/Ziggo, het Ministerie van BZK en Stichting Number Five. Daaronder valt onder meer de uitvoering en campagne rondom de telefonische Digihulplijn, de Actie Allemaal Digitaal, drie lokale proeftuinen met gemeenten en lokale hulporganisaties, maar ook evenementen zoals aanwezigheid op de 50+ beurs en een conferentie, de Dag van de digitale inclusie. Ook werkt de Alliantie aan verschillende publicaties en activiteiten op drie thema's; «gezonde digibalans», veilig internetten en het achterlaten van data op het internet (digitaal nalatenschap). Tot slot doen zij onderzoek naar betaalbare internetabonnementen voor kwetsbare groepen. Zonder internettoegang krijgen mensen ook geen vaardigheden. Overige middelen zijn besteed aan nader onderzoek naar de maatschappelijke opgave op kritische digitale vaardigheden en ontwikkeling van opleidingsaanbod.

31
Kunt u toelichten op welke manier de monitoring en evaluatie van de vijf lijnen in de Werkagenda een plek gaan krijgen in de Strategische Evaluatie Agenda?

Antwoord
De «Werkagenda Waardengedreven Digitaliseren» wordt jaarlijks geëvalueerd en geactualiseerd. Hiertoe wordt vanuit het werkprogramma momenteel de monitoring- en evaluatiefunctie ingericht. Als dit is uitgewerkt wordt dit onderdeel van de Strategische Evaluatie Agenda.

32
Kunt u toelichten waarom nog niet bekend is in welk jaar de beleidsdoorlichting van begrotingsartikel 6.7 «Hoogwaardige dienstverlening één overheid» wordt afgerond?

Antwoord
Het begrotingsartikel 6.7 «Hoogwaardige dienstverlening één overheid» bestaat sinds 2021. De planning van de beleidsdoorlichting volgt de reguliere begrotingscyclus van de Rijksoverheid. De afronding van de beleidsdoorlichting wordt dan ook op zijn vroegst verwacht in 2025 en uiterlijk in 2028.

Vragen inzake vaststelling van de begrotingsstaten van het Ministerie van Economische Zaken en Klimaat (XIII) voor het jaar 2023

33
Kunt u de opbrengsten van de Kamer van Koophandel uiteenzetten met de handel van persoonsgegevens?

Antwoord
De Kamer van Koophandel (KVK) brengt voor de verstrekking van openbare gegevens uit het Handelsregister wettelijk vastgestelde tarieven in rekening, die overigens slechts gedeeltelijk kostendekkend zijn. Bij de tariefstelling wordt rekening gehouden met de toegankelijkheid, ook financieel, van de informatie die voor een veilig en verantwoord handelsverkeer noodzakelijke is. KVK ontvangt daarnaast een rijksbijdrage om de kosten van instandhouding van het Handelsregister te dekken. In het kader van de Datavisie Handelsregister wordt overigens ook de kostendekking van het Handelsregister heroverwogen, onder andere omdat de tarieven op dataverstrekking niet optimaal samengaan met het wenselijke gebruik van gegevens zowel door publieke als private afnemers. De Minister van EZK heeft aangekondigd dit najaar een brief hierover aan de Kamer te sturen.

34
Kunt u de opbrengsten van de Centraal Bureau voor de Statistiek uiteenzetten met de handel van persoonsgegevens?

Antwoord
Het Centraal Bureau voor de Statistiek (CBS) verkoopt geen persoonsgegevens, dus heeft ook geen opbrengsten hieruit. Het CBS verzamelt o.a. persoonsgegevens voor statistisch onderzoek, maar deze gegevens verlaten het CBS niet. Het CBS gebruikt zogeheten gepseudonimiseerde gegevens voor de statistische diensten die het biedt.

35
Voldoet het vrijgemaakte budget voor Agentschap Telecom om te voldoen aan de nieuwe taken die het Agentschap Telecom gaat krijgen op het gebied van cyberveiligheid?

Antwoord
Het budget voor Agentschap Telecom (AT) is op dit moment voldoende om op het gebied van cybersecurity haar taken uit te voeren en toezicht te houden. Naast investeringen via de reguliere begrotingscyclus wordt een deel van de structurele additionele EZK-middelen uit het coalitieakkoord op cybersecurity geïnvesteerd in AT voor uitvoering en toezicht op Europese cybersecurity certificering van ICT-producten, diensten en processen op basis van de Cyber Security Act (CSA) en de aankomende cybersecurity markttoegangseisen voor draadloos verbonden apparaten onder de Radio Equipment Directive (RED). Het benodigde budget voor toekomstige taken van AT moet nog in de kaart worden gebracht en zal conform de reguliere begrotingssystematiek worden behandeld. Daarbij gaat het om de nationale implementatie van de herziene Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB2) en toekomstig toezicht op de Cyber Resilience Act (CRA). Het voorstel voor deze Europese horizontale verordening is 15 september jl. gepresenteerd. De Europese onderhandelingen zijn net gestart.

36
Hoeveel ondernemers zijn in 2021 slachtoffer geworden van een cyberaanval? Kan dit aantal worden afgezet tegen de aantallen in 2020 en 2019? Om hoeveel midden- en kleinbedrijven (mkb) ging het in 2021?

Antwoord
In juli dit jaar heeft het CBS de cybersecurity monitor 2021[1] gepubliceerd. Hierin wordt een beeld geschetst van de ICT-incidenten waar bedrijven en personen slachtoffer van zijn geworden.

[1] Cybersecuritymonitor 2021 (cbs.nl).

Uit het CBS-onderzoek is gebleken dat in 2016 bijna 40 procent van de grote bedrijven (250 of meer werknemers) met een ICT-veiligheidsincident te maken heeft gehad, terwijl dat in 2019 19 procent was. In 2020 is dit weer toegenomen tot 22 procent van de grote bedrijven die een ICT-veiligheidsincident melden door een aanval van buitenaf.
Wat opvalt in het onderzoek is dat grote bedrijven over de jaren heen meer incidenten rapporteren dan kleine bedrijven voor zowel interne incidenten als incidenten door een aanval van buitenaf. Voor een volledig overzicht van de uitkomsten verwijs ik u graag door naar de CBS Cybersecurity monitor.
Uit het jaarlijkse onderzoek naar het bewustzijn van Nederlanders rondom cybersecurity in opdracht van EZK – Cybersecurity Onderzoek Alert Online 2022 – komt daarbij naar voren dat een kwart van het kleine mkb in het geheel geen acties onderneemt om digitaal veilig te zijn. Dit maakt deze groep kwetsbaarder voor cybercrime en daardoor mogelijk ook sneller slachtoffer.
Aanvullend op het reeds bestaande onderzoek is in de Nederlandse Cybersecurity Strategie opgenomen om een expertisecentrum op te richten waar data over cyberaanvallen kan worden verzameld en geanalyseerd.

37
Kunt u een overzicht geven van alle concrete maatregelen en acties die worden ingezet om bedrijven en ondernemers beter te beschermen tegen cybercriminelen?

Antwoord
Hiervoor wil ik graag verwijzen naar de brief die ik deze zomer samen met mijn collega van Justitie en Veiligheid aan uw Kamer heb gestuurd (Kamerstuk 26 643, nr. 907) over preventie cybercrime in het midden- en kleinbedrijf. Daarnaast wordt gewerkt aan de algemene versterking van de cyber security en het tegengaan van cybercrime. De nieuwe Nederlandse Cyber Security Strategie is 10 oktober aan u toegezonden. In de NLCS zijn concrete maatregelen opgenomen om de weerbaarheid van bedrijven te verhogen. Over de integrale aanpak van cybercrime bent u ieder jaar geïnformeerd (Kamerstuk 26 643, nr. 768), meest recentelijk op 28 mei 2021.
Bij het verhogen van de digitale weerbaarheid ligt de nadruk op het stimuleren van het gebruik van diverse veiligheidsmaatregelen door bedrijven, zoals omschreven in de vijf basisprincipes van het Digital Trust Center. Het Digitale Trust Center en het Nationaal Cyber Security Centrum werken bovendien nauw samen. Door het delen van algemene en specifieke dreigingsinformatie kan het Digital Trust Center bijdragen aan het minimaliseren van de effecten van externe incidenten. Met het uitbreiden van de onderzoeken en diensten die als doel hebben de cyberweerbaarheid van het Nederlandse mkb in kaart te brengen, ontstaat bovendien meer inzicht in de cyberrisico's voor het mkb. Daarnaast kan de weerbaarheid worden verhoogd door bedrijven nog meer te stimuleren zelf veiligheids- en risicoanalyses uit te voeren. CBS-data laten zien dat slechts de helft van de bedrijven met meer dan 10 werknemers op reguliere basis een risicoanalyse uitvoert. Een verhoogde inzet op bekendheid van de tools van het Digital Trust Center kan veel bedrijven stimuleren hier de nodige stappen in te zetten.
In de City Deal «Lokale weerbaarheid cybercrime» zijn de afgelopen jaren lokale en regionale innovatieve pilots gestart om de weerbaarheid van mkb-ondernemers te verhogen. Uit evaluaties van deze eerste pilots blijkt dat ondernemers blij zijn met tips en handleidingen via digitale kanalen, waaronder die van het Digital Trust Center. In de praktijk blijkt het voor mkb-ondernemers lastig deze in te voeren in de eigen onderneming. In pilots van de afgelopen jaren werden ondernemers met raad en daad

ondersteund door ICT-studenten of ICT-leveranciers om de in scans gesignaleerde risico's aan te pakken en de geadviseerde maatregelen daadwerkelijk door te voeren.
Brancheorganisaties, Regionale Platforms Veilig Ondernemen, gemeenten en samenwerkingsverbanden van het Digital Trust Center kunnen voor ondernemers een belangrijke rol in spelen. Het Digital Trust Center zet daarom in op het opzetten en/of versterken van samenwerkingsverbanden die regionaal of branchegericht zijn. Op dit moment zijn er 48 samenwerkingsverbanden bij het Digital Trust Center aangesloten. Het streven is dat dit eind 2023 50 samenwerkingsverbanden zijn.
Het project Samen Digitaal Veilig, onderdeel van nieuwe samenwerkingsafspraken tussen de ondernemersorganisaties (MKB-Nederland en BOVAG) en de Ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat, richt zich op het weerbaar maken van bedrijven. Het platform Samen Digitaal Veilig biedt onder meer een elektronische leeromgeving voor medewerkers, met korte informatieve films en toetsen. Brancheorganisaties spelen in de verspreiding van die informatie een belangrijke rol. Zij kunnen, als vertrouwde partner van de bedrijven in de eigen branche, de leeromgeving onder de aandacht brengen.
MKB-Nederland en het Digital Trust Center hebben voor de brancheorganisaties diverse bijeenkomsten georganiseerd om het project meer bekendheid te geven, branches aan te sporen meer activiteiten op het gebied van cyberweerbaarheid te ontplooien en hen mee te nemen in de mogelijkheden van het project. Inmiddels hebben meerdere brancheverenigingen interesse getoond in het project. De pilotfase van dit project is bijna afgerond. Er lopen gesprekken over een vervolgsubsidie. Doel van deze subsidie is om gedragsonderzoek te doen naar de effectiviteit van het project. Op basis van de resultaten van het gedragsonderzoek wordt al dan niet ingezet op het breder uitrollen onder andere branches. Besluitvorming over de vervolgsubsidie zal voor einde van dit jaar plaatsvinden.

38
Wat was het budget van het Digital Trust Center (DTC) in 2021? Kan dit worden afgezet tegen het budget van de jaren daarvoor?

Antwoord
In 2021 was het budget € 4,5 miljoen. In de jaren daarvoor (2018–2020) was het budget € 2,5 miljoen.

39
Hoeveel mensen zijn fulltime werkzaam bij het Digital Trust Center? Hoeveel niet-vitale bedrijven bedient het Digital Trust Center?

Antwoord
Op dit moment werken er 23 fte bij het DTC waarvan 5 externe inhuur en 1 trainee. De doelgroep van niet-vitale bedrijven bedraagt zo'n twee miljoen ondernemers.

40
Hoeveel niet-vitale bedrijven heeft het Digital Trust Center al voorzien van dreigingsinformatie in 2021?

Antwoord
In 2021 zijn er 361 notificaties uitgestuurd aan bedrijven, dit betrof 15 kwetsbaarheden. Voor de volledigheid: in 2022 zijn er 4254 notificaties uitgestuurd betreffende 43 kwetsbaarheden. (Peildatum 5 oktober 2022).
Daarnaast wordt er ook algemene informatie over ernstige cyberdreigingen gedeeld via de zogenoemde partnerberichten, de website, de community en de sociale media kanalen. De partnerberichten worden

verstuurd naar alle 48 samenwerkingsverbanden die zijn aangesloten bij het DTC.
U bent bij brief (Kamerstuk 26 643, nr. 864) van 27 juni jl. nader geïnformeerd over de inrichting van de informatiedienst van het DTC.

41
Kunt u een overzicht geven van alle concrete maatregelen en acties die worden ingezet om slimme apparaten (Internet of Things-apparaten (IoT)) veiliger te maken?

Antwoord
De afgelopen jaren zijn diverse maatregelen en acties genomen om Internet *of Things* (IoT)-apparaten digitaal veiliger te maken op basis van de Roadmap Digitaal Veilige Hard- en Software (Kamerstuk 26 643, nr. 535). Een voorbeeld is de realisatie van Europese cybersecurity markttoegangseisen onder de Radio Equipment Directive (RED) die medio 2024 van kracht zullen worden. U bent jaarlijks over de voortgang geïnformeerd, waarvan meest recent op 30 november 2021 (Kamerstuk 26 643, nr. 801). De Roadmap Digitaal Veilige Hard- en Software is volledig geïntegreerd in de Nederlandse Cybersecurity Strategie (NLCS) (Kamerstuk 26 643, nr. 925) die u op 12 oktober jl. heeft ontvangen. Een voorbeeld is de Nederlandse inzet op een Europese cybersecurity zorgplicht voor alle ICT-producten en diensten in de aankomende Europese *Cyber Resilience Act* die op 15 september jl. is gepresenteerd door de Europese Commissie.

42
Hoe verhouden de digitaliseringsinvesteringen door het Ministerie van Economische Zaken en Klimaat zich tot de budgetten die worden toebedeeld aan de digitale toezichthouders, zoals de Autoriteit Persoonsgegevens (AP)?

Antwoord
Zie het antwoord op vraag 182.

43
Hoeveel huishoudens hebben naar schatting nog geen glasvezel in Nederland? Hoeveel huishouden hebben hier toegang toe?

Antwoord
Ongeveer 4,7 van de 8,1 miljoen Nederlandse huishoudens heeft in Q1 2022 glasvezelaansluiting, oftewel ca. 58%. De overige 3,4 miljoen huishoudens heeft dat nog niet. Verwacht wordt dat, gelet op de aanlegambities van de diverse glasvezelpartijen en hun huidige aanlegtempo (in het afgelopen jaar zijn ca. 840.000 woningen op glasvezel aangesloten), het merendeel van deze resterende huishoudens in de komende jaren alsnog van glasvezel wordt voorzien (ACM Telecommonitor 2022-Q1).
Het totale aantal huishoudens dat over een snelle vaste internetverbinding kan beschikken, via glasvezel of andere technieken, ligt overigens veel hoger: meer dan 99% van alle huishoudens in Nederland kan beschikken over een snelle vaste internetverbinding van ten minste 100 Mbps en bijna 90% al over 1 Gbps. Dat betekent dat momenteel minder dan 1% van alle huishoudens nog niet over een snelle vaste internetaansluiting kan beschikken. Daarvan is het overgrote deel gesitueerd in het buitengebied. De Tweede Kamer is voor de zomer geïnformeerd (Kamerstuk 29 517, nr. 222) over de resterende adressen in de buitengebieden en de mogelijkheden om de circa 19.000 adressen die dreigen achter te blijven alsnog van snel internet te kunnen voorzien.

44
Hoe gaat u de Europese samenwerking tussen lidstaten op het gebied van digitalisering versterken?

Antwoord
In het coalitieakkoord staat dat het kabinet het voortouw neemt om de samenwerking tussen lidstaten op het terrein van digitalisering te versterken. Dat doet het kabinet door nauw samen te werken tussen de ministeries en langs twee lijnen. In de eerste plaats werken we samen met gelijkgestemde lidstaten om publieke belangen als eerlijke concurrentie, (keuze)vrijheid, openheid, regie op data en gegevens en veiligheid in de digitale economie in de toekomst te waarborgen. Dit gebeurt voornamelijk via de Europese wetgevingsagenda voor digitalisering. Een goed voorbeeld is de recent gelanceerde Cyber Resilience Act waarbij het kabinet in een vroeg stadium samen met gelijkgestemde landen proactief gepleit heeft voor strengere cybersecurityeisen voor ICT-producten en diensten. Ook over de inrichting van het publieke toezicht op Europese regelgeving op het terrein van digitalisering wordt nadere afstemming gezocht met andere lidstaten om te bevorderen dat het toezicht effectief en zoveel mogelijk uniform is.
In de tweede plaats zoekt Nederland actief de samenwerking met Europese partners op het terrein van digitale innovatie. Met het Topteam ICT verkennen we momenteel de mogelijkheden tot versterking van de samenwerking met Duitsland, Frankrijk en België, o.a. op de terreinen van artificiële intelligentie en cyber security. Via deelname aan IPCEI Cloud wordt samengewerkt met Duitsland, Frankrijk, Spanje, Luxemburg, België, Italië, Hongarije, Polen, Slovenië, Oostenrijk en Letland om een nieuwe generatie veilige en duurzame cloudoplossingen te ontwikkelen. Ook rondom GAIA-X wordt de Europese samenwerking verder versterkt, o.a. via de deelname aan de Governmental Advisory Board van GAIA-X en de opgerichte Nederlandse GAIA-X hub.

45
Kunt u toelichten wat u verstaat onder risicovolle afhankelijkheden in de digitale economie? Op welke punten en met welke landen wilt u de samenwerking versterken?

Antwoord
De digitale economie bestaat uit een veelheid van onderlinge, wederzijdse afhankelijkheden die ons grote voordelen bieden. Tegelijkertijd kunnen risicovolle afhankelijkheden ontstaan van derde landen en technologiebedrijven, bijvoorbeeld ten aanzien van digitale sleuteltechnologieën, het data ecosysteem, of onze digitale infrastructuur. Door deze afhankelijkheden staat het vermogen van Nederland en de EU om de eigen publieke belangen, op basis van eigen inzichten en keuzes, te borgen en digitaal weerbaar te zijn in een onderling verbonden wereld onder druk.
Nederland streeft in Europees verband naar de versterking van de bescherming van deze belangen met behoud van zo veel mogelijk openheid. Het gaat hierbij om een breed palet van instrumenten: van het stimuleren van de eigen capaciteiten, bijvoorbeeld via Important Projects of Common European Interest (IPCEI) Cloud tot aan wet- en regelgeving zoals de Digital Markets Act, de AI Act, de Data Act en de Cyber Resilience Act. Ook is internationale samenwerking met onze strategische partners cruciaal om risicovolle afhankelijkheden efficiënt en effectief te adresseren en wederzijdse afhankelijkheden op een verantwoorde manier te laten voortbestaan. Het versterken van de samenwerking met de VS via de EU-US Trade and Technology Council (TTC) is hiervan een voorbeeld.

46
Welke risicovolle afhankelijkheden worden tegengaan?

Antwoord
Zoals aangegeven in de beantwoording van vraag 45 worden in de digitale economie met behulp van diverse instrumenten risicovolle afhankelijkheden tegengegaan die de borging van onze publieke belangen en digitale weerbaarheid onder druk zetten in een onderling verbonden wereld. Gezien de bredere ontwikkelingen en ook de uitwerking van de kabinetsinzet rond open strategische autonomie behoeft deze inzet nadere uitwerking. Het kabinet gaat daarom aan de slag met een nadere inventarisatie en verdere invulling van deze inzet, specifiek rond het vraagstuk van digitale autonomie. Uw Kamer wordt hier in de loop van 2023 nader over geïnformeerd.

47
Kunt u toelichten uw inzet is ten aanzien van het aanjagen van de (verdere) digitalisering van het bedrijfsleven en het vergroten van de cyberweerbaarheid van het bedrijfsleven, en specifiek voor het mkb?

Antwoord
Eind juni dit jaar heeft EZK de pilot Mijn Digitale Zaak gelanceerd waarbij ondernemers een subsidie kunnen krijgen om op een basisniveau van digitalisering te komen. Het verhogen van de cyberweerbaarheid hoort hier zeker bij. De pilot heeft een sectorale aanpak en is voor deze pilot alleen op de Retailondernemers gericht. Het pilotproject MijnDigitaleZaak is gezamenlijk door EZK, MKB-Nederland, KvK, RVO en brancheorganisatie INretail opgezet. De huidige cijfers geven een positief beeld. Na het aflopen van de subsidieregeling in december 2022 zal de pilot worden geëvalueerd. Bij een positieve evaluatie is het de intentie van de initiatiefnemers om de aanpak op te schalen naar andere sectoren, mits daar dan financiering voor wordt gevonden. De Tweede Kamer is 29 juni hierover geïnformeerd met de Kamerbrief Smart Industry Schaalsprongagenda. Ook zijn er de Digitale werkplaatsen, het vrijwel landelijk dekkend netwerk van digitale werkplaatsen waarbij studenten mkb'ers helpen met het implementeren van digitale technologieën. Het Smart Industry programma gaat over de digitale transformatie van de brede maakindustrie met een belangrijke focus op het MKB. Ook zijn er de European Digitale Innovation Hubs (EDHIs). Met het opzetten van een netwerk van EDIH's wil de Europese Commissie naar brede regionale ondersteuning voor het versnellen van de digitalisering. Dit wordt verder toegelicht in de beantwoording van vraag 62.
In het antwoord op vraag 37 wordt een verdere toelichting gegeven op de concrete maatregelen en acties die worden ingezet om de cyberweerbaarheid in het bedrijfsleven te verhogen.

48
Wanneer is er meer duidelijkheid over de genoemde investeringsvoorstellen op het terrein van AI en Important Project of Common European Interest (IPCEI) Cloud? Wanneer wordt hieromtrent informatie met de Kamer gedeeld?

Antwoord
Het verplichte goedkeuringsproces door de Europese Commissie neemt door de omvang en complexiteit van deze IPCEI aanzienlijk meer tijd in beslag dan eerder aangenomen door alle betrokken partijen. Eerder werd verwacht het proces rond de zomer van 2022 af te ronden, naar de huidige verwachting zal dit proces pas in de eerste helft van 2023 afgerond worden, waarna de Tweede Kamer geïnformeerd zal worden over de specifieke projecten. Voor investeringen in AI zie het antwoord op vraag 53.

49
Welk percentage van de huidige omvang van het Deep Tech Fund is tot nu toe belegd?

Antwoord
Het fonds is na de zomer van start gegaan, diverse aanvragen zitten in de pijplijn. We verwachten dit jaar ca. 10 mln. capital calls vanuit het Deep Tech Fonds. Op dit moment is er nog geen informatie beschikbaar over verrichte investeringen.

50
In welke technologieën heeft het Deep Tech Fund tot nu toe geïnvesteerd?

Antwoord
Het fonds is na de zomer van start gegaan, diverse aanvragen zitten in de pijplijn. We verwachten dit jaar ca. 10 mln. capital calls vanuit het Deep Tech Fonds. Op dit moment is er nog geen informatie beschikbaar over verrichte investeringen.

51
Kunt u toelichten hoe de strategie voor de digitale economie en de digitale infrastructuur zich verhouden tot de aangekondigde Werkagenda Digitalisering van het kabinet?

Antwoord
De «Werkagenda Waardengedreven Digitaliseren» vormt de komende jaren de basis voor het kabinetsbrede beleid voor digitalisering van de (digitale) overheid, samenleving en het Rijk. Dit is de eerste uitwerking van de thema «de digitale overheid» en een aantal onderdelen uit «het fundament» uit de hoofdlijnenbrief digitalisering (26 643, nr. 842). De strategie voor de digitale economie heeft betrekking op de ambitie en prioriteiten van het kabinet voor het thema «de digitale economie» uit de hoofdlijnenbrief digitalisering en de onderdelen «digitale infrastructuur en digitale autonomie en goedwerkende markten en diensten» uit het fundament. In de strategie voor de digitale economie zullen de prioriteiten voor de digitale economie worden uitgewerkt, zoals opgenomen in de hoofdlijnenbrief EZK (Kamerstuk 35 925 XIII, nr. 87), waaronder digitale innovatie en vaardigheden, goedwerkende digitale markten en diensten, een veilige, hoogwaardige en betrouwbare digitale infrastructuur en cybersecurity. Voor het thema digitale infrastructuur volgt een nadere verkenning en verdieping in het tweede kwartaal van 2023.

52
Wanneer worden de visie op de digitale infrastructuur en de strategie voor de digitale economie naar de Kamer gestuurd?

Antwoord
De Minister van Economische Zaken en Klimaat (EZK) heeft toegezegd de strategie digitale economie in Q4 2022 aan uw Kamer toe te sturen. De visie op de digitale infrastructuur volgt in Q2 2023.

53
Hoeveel geld uit het Nationaal Groeifonds is beschikbaar voor kunstmatige intelligentie?

Antwoord
Vanuit het Nationaal Groeifonds is in totaal 204,5 mln. euro beschikbaar gesteld specifiek voor onderzoek en innovatie op het gebied van kunstmatige intelligentie via het meerjarige investeringsprogramma AiNed. Het bedrag van 204,5 mln. euro bestaat uit een toekenning van 44 mln. euro,

een voorwaardelijke toekenning van 44 mln. euro en een toekenning van 116,5 mln. euro (kamerbrief van 14 april 2022, 35 925 XIX, nr. 12).

54
Kunt u toelichten wat het human capital programma precies inhoudt, en hoe het samenhangt met de inzet van het Ministerie van Onderwijs Cultuur en Wetenschap op dit terrein?

Antwoord
Het human capital programma bestaat uit twee onderdelen. Het eerste onderdeel is de human capital agenda ict (HCA ICT) die een bijdrage levert aan de oplossing van het tekort aan ict'ers. De HCA ICT is gericht op het stimuleren en ondersteunen van publiek-private samenwerking tussen (beroeps)onderwijs en bedrijfsleven. Een concreet project is het uitbreiden van het Make IT Work omscholingsprogramma naar het mbo. In het hbo zijn op deze manier al honderden mensen succesvol omgeschoold naar ICT'er. Dit sluit nauw aan bij initiatieven van OCW, zoals het Regionaal Investeringsfonds en Leven Lang Ontwikkelen.
Het tweede onderdeel, de Taskforce Diversiteit & Inclusie, richt zich op het verhogen van het aantal vrouwen en andere ondervertegenwoordigde groepen in de ICT. Hierin hebben bedrijven primair een belangrijke rol door o.a. het delen van goede voorbeelden. Dit sluit aan bij de doelstelling van de Europese Commissie om in 2030 genderconvergentie in de ICT te hebben en op emancipatiedoelen van OCW.

55
Kunt u toelichten hoeveel uitgaven begroot zijn voor de «human capital agenda» en welk deel daarvan wordt geïnvesteerd in het versterken van digitale vaardigheden?

Antwoord
In het regeerakkoord is er € 10 mln. beschikbaar gesteld voor het versterken van digitale basisvaardigheden (onderdeel van de BZK-begroting). Ook zijn er in het programma Smart Industry via de fieldlabs mogelijkheden voor het versterken van digitale vaardigheden voor werkenden (450 k€).
In de verlenging van de omscholingsregeling naar kansrijke beroepen in de ICT en techniek, die dit najaar opnieuw is opgegaan, is € 10 mln. beschikbaar. Met de omscholingsregeling worden werkgevers financieel ondersteund bij de omscholing van mensen richting essentiële tekortberoepen in de klimaat- en digitale transitie.
De human capital agenda heeft geen expliciete doelstelling op het versterken van digitale vaardigheden. Door samenwerking tussen (beroeps)onderwijs en bedrijfsleven worden innovaties in opleidingen gestimuleerd en sluiten die nauwer aan bij de eisen op de arbeidsmarkt. Hierdoor is er binnen opleidingen meer aandacht voor digitale vaardigheden. Voor de human capital agenda ICT is € 0,5 mln. beschikbaar en voor de taskforce diversiteit en inclusie is € 0,18 mln. beschikbaar. Zowel HCA al D&I zijn middels subsidiebeschikkingen toegekend.

56
Op welke manier zal er gewerkt worden aan het stimuleren van cybersecurity, AI en emerging tech kennisontwikkeling en innovatie?

Antwoord
Kennisontwikkeling en innovatie voor digitale en opkomende technologie worden op verschillende manieren door EZK gestimuleerd. Onder andere via het generieke instrumentarium, zoals de WBSO en de MIT Regeling. Daarnaast wordt ook specifiek ingezet op het versterken van de ontwikkeling en benutting van (digitale) sleuteltechnologie, zoals cyber security

als onderdeel van het Missiegedreven Topsectoren- en Innovatiebeleid. Het Nationaal Groeifonds is ook belangrijk voor investeringen in meerjarige programma's, zoals bijvoorbeeld AI en kwantum. Via het publiek-private samenwerkingsplatform dcypher wordt ingezet op meerjarige samenwerking op het gebied van cybersecurity kennis en innovatie.

57
Welke onderdelen van de rijksbrede Nederlandse Cybersecuritystrategie ten aanzien van consumentenbescherming, veiligheid van slimme producten en de cyberweerbaarheid van het bedrijfsleven zijn reeds geïmplementeerd? Welke onderdelen nog niet?

Antwoord
Cybersecurity is een complex, dynamisch en grensoverschrijdend vraagstuk waarbij op basis van een lerende aanpak maatregelen worden genomen en doorontwikkeld om de digitale weerbaarheid van Nederland te versterken voor burgers en bedrijven. De Nederlandse Cybersecurity Strategie (NLCS) die u op 10 oktober jl. heeft ontvangen bouwt voort op het beleid en de maatregelen van eerdere cybersecurity strategieën uit 2011, 2013 en 2018. U bent jaarlijks geïnformeerd (Kamerstuk 26 643, nr. 767) over de voortgang van de Rijksbrede cybersecurity aanpak door de Minister van JenV, meest recent op 28 juni 2021. Het actieplan bij de NLCS bevat een overzicht van de maatregelen die de komende periode worden genomen. Ten aanzien van consumentenbescherming en de veiligheid van slimme producten bent u jaarlijks geïnformeerd (Kamerstuk 26 643, nr. 801) over de voortgang van de Roadmap Digitaal Veilige Hard- en Software waarvan meest recent op 30 november 2021. Over de voortgang op de aanpak om de digitale weerbaarheid van het bedrijfsleven te verhogen bent u regelmatig geïnformeerd (Kamerstuk 26 643, nr. 817 & nr. 864) over de voortgang van het Digital Trust Center en de ontwikkeling van haar informatiedienst zoals op 7 februari jl. en op 27 juni jl. en over de voorgenomen integratie van het Digital Trust Center (DTC), Cybersecurity Incident Response Team voor digitale dienstverleners (CSIRT-DSP) en het Nationaal Cyber Security Centrum (NCSC) op 7 september jl. (Kamerstuk 2022Z16336) en 13 september jl. (Kamerstuk 26 643, nr. 915).

58
Kunt u toelichten wat de concrete consequenties zijn voor het toezicht op de DSA als het niet lukt om dit jaar aan voldoende gekwalificeerd personeel te komen, gezien de krapte op de arbeidsmarkt?

Antwoord
Op 4 oktober 2022 heeft de Raad van Ministers de Digital Services Act (DSA) aangenomen (https://www.consilium.europa.eu/en/meetings/ecofin/2022/10/04/). Op donderdag 27 oktober is de DSA vervolgens gepubliceerd (https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=uriserv:OJ.L_.2022.277.01.0001.01.NLD). Daardoor is de DSA per 17 februari 2024 van kracht voor alle andere ondernemingen dan zeer grote online platformen en zoekmachines. Voor hen treedt de DSA al eerder in werking. Maar het toezicht op die ondernemingen ligt vrijwel in het geheel bij de Europese Commissie. Nationaal moet de organisatie van het toezicht begin 2024 zijn geregeld.
Het werven van voldoende gekwalificeerd personeel is een essentieel onderdeel voor het toezicht en tevens een uitdaging. Zowel vanwege de krapte op de arbeidsmarkt, als ook de algemene schaarste van mensen met een technische scholing. Mede vanwege deze opgave en het feit dat de DSA erg snel van kracht wordt zijn er al sinds het begin van de onderhandelingen gesprekken gevoerd met toezichthouders. Daarbij gaat

het ook over de benodigde middelen en het werven van personeel. Omdat de DSA pas in 2024 van kracht wordt kan de werving nog in 2023 plaatsvinden en is er geen probleem als er in 2022 nog geen gekwalificeerd personeel kan worden geworven. Om werving in 2023 mogelijk te maken is er met input van diverse toezichthouders voor gezorgd dat er al in 2023 voldoende middelen beschikbaar komen.

59
Zijn er voldoende (personele) capaciteit en (financiële) middelen beschikbaar om het toezicht en de handhaving van de Digital Services Act (DSA) uit te voeren? Zijn er onder andere gelet op de krapte op de arbeidsmarkt risico's voor het toezicht op de DSA? Hoe gaat u consumenten en bedrijven informeren over de verplichtingen die voortvloeien uit de DSA?

Antwoord
Voor wat betreft de uitdagingen en risico's voor het werven van voldoende gekwalificeerd personeel wordt u verwezen naar het antwoord op vraag 58. Meer in het algemeen is er is op dit moment geen reden om aan te nemen dat er niet voldoende capaciteit en middelen beschikbaar kunnen worden gesteld.
Er wordt nog onderzocht hoe consumenten en bedrijven het beste kunnen worden geïnformeerd over de verplichtingen die voortvloeien uit de DSA, en door wie. Moet de overheid dat doen, of moeten de toezichthouder(s) op de DSA dat doen? Er moet bijvoorbeeld worden voorkomen dat het informeren van burgers of bedrijven door de overheid het werk van de onafhankelijk toezichthouder(s) in de weg zit. Het past misschien wel beter dat de toekomstig toezichthouder bedrijven, en eventueel ook consumenten, informeert over aanstaande verplichtingen en rechten. Dit onderwerp zal ook worden besproken in de gesprekken met toezichthouders die in de antwoorden 60 en 184 zijn genoemd.

60
Kunt u toelichten welke andere toezichthouders of instanties, naast de Autoriteit Consument & Markt (ACM), een rol zullen spelen bij de implementatie van de DSA? Welk (deel van het) budget is begroot om te zorgen voor voldoende capaciteit en toezichtmiddelen voor de implementatie van de DSA?

Antwoord
Zoals aangegeven in de beantwoording van Kamervragen van het lid Van der Plas is het voornemen om de Autoriteit Consument en Markt («ACM») aan te wijzen als digitale dienstencoördinator (Aanhangsel van de Handelingen 2021/22, nr. 2925. Zie antwoord op vraag 8). De ACM wordt naar verwachting ook de voornaamste toezichthouder op de rest van de DSA. Veel van de artikelen in de DSA gaan over de bescherming van consumenten en zakelijke gebruikers. De ACM is reeds toezichthouder voor veel wetgeving die consumenten en zakelijke gebruikers beschermt. Daarmee bezit de ACM al relevante inhoudelijke expertise en ervaring. Zowel met de bescherming van dit belang in de praktijk als ook met de wijze waarop daar effectief toezicht op kan worden gehouden.
Tegelijkertijd is het belangrijk om te onderkennen dat de DSA raakvlakken heeft met de taken van de Autoriteit Persoonsgegevens («AP») en het Commissariaat voor de Media («CvdM»). Dit speelt bijvoorbeeld bij de bepalingen waarin beperkingen worden gesteld aan adverteren, en het gebruik van persoonsgegevens daarbij. In die bepalingen wordt soms voortgebouwd op regels en definities uit de Algemene Verordening Gegevensbescherming (AVG). En sommige online platformen die onder de DSA vallen worden ook gereguleerd onder de Audiovisuele Mediadienstenrichtlijn, waar het Commissariaat voor de Media toezicht op houdt.

Samen met de genoemde toezichthouders wordt onderzocht welke rol zij naast de ACM moeten krijgen in, of bij, het toezicht op deze bepalingen. Daarnaast is en wordt er ook met andere toezichthouders gesproken over de DSA om te onderzoeken of die relevantie heeft voor hun taken en uitoefening van bevoegdheden. Zoals de NVWA, AFM, en ATKM. Het is zeer onwaarschijnlijk dat zij een directe rol krijgen in het toezicht op de DSA en de handhaving. Hun expertise kan niettemin van belang zijn voor de ACM bij het uitvoeren van haar taken op de DSA.
Er is met ACM en andere toezichthouders contact geweest over de benodigde middelen. Dit heeft erin geresulteerd dat er voor 2023 een bedrag van € 1.210.500 beschikbaar is gemaakt voor de voorbereiding op de aankomende toezichtstaken. Voor de jaren daarna zijn er mogelijk structureel meer middelen nodig. Hierover zijn gesprekken gaande. Daarbij zijn ook de toezichthouders betrokken.

61
Krijgt de ACM ook extra middelen om toezicht te houden op de implementatie van de Digital Markets Act (DMA) en DSA? Zo ja, hoeveel?

Antwoord
Ja, ACM krijgt extra middelen voor de voorbereidende werkzaamheden en om toezicht te houden op de DMA en DSA. Er is uitvoerig contact met ACM en andere toezichthouders over de organisatie van het toezicht, en het daarvoor benodigde budget. Aan de hand hiervan is een inschatting gemaakt van de benodigde middelen. Op basis van deze inschatting wordt voor 2023 € 807.000 beschikbaar gesteld voor het toezicht op de DMA en € 1.210.500 voor de voorbereiding op het toezicht op de DSA. Het geld voor de DSA moet nog worden verdeeld over de ACM en eventueel andere toezichthouders mochten die een rol krijgen. Zoals in het antwoord op vraag 60 is beschreven kunt u dan denken aan het AP en het CvdM. Daar is ook al beschreven dat er voor de periode na 2023 mogelijk structureel meer middelen nodig zijn.

62
In hoeverre kan het mkb profiteren van de investeringen in digitale innovatie en digitale vaardigheden, die zijn afgesproken in het coalitieakkoord?

Antwoord
Het MKB profiteert van diverse investeringen in onderzoek, innovatie en human capital, zoals het Nationaal Groeifonds. Zo kent het AiNed programma van het Nationaal Groeifonds specifieke actielijnen gericht op het helpen van het MKB, w.o. het bevorderen van R&D samenwerkingsprojecten en projecten met onderwijsinstellingen voor onderwijs en toegepast onderzoek bij het MKB. Daarnaast is er het vrijwel landelijk dekkend netwerk van digitale werkplaatsen waarbij studenten mkb'ers helpen met het implementeren van digitale technologieën. Ook zijn er de Europese Digitale Innovatiehubs (EDIHs) die zich richten op de toepassing van geavanceerde technologie in het mkb. Via de EDIHs kunnen mkb-bedrijven een beroep doen op technische expertise en ontstaan verschillende mogelijkheden voor financieringsadvies, opleidingen en testen via pilot- en demonstratieprojecten. Het programma Smart Industry heeft als doel om digitalisering te benutten in de brede maakindustrie. In de Smart Industry schaalsprongagenda 2022–2026 zijn concrete ambities opgenomen om mkb- bedrijven een significante stap te laten zetten op het gebied van digitalisering van hun fabrieken. Ook wordt er geïnvesteerd in scholing op het gebied van digitale vaardigheden waardoor nieuwe digitale technologieën in de bedrijfsomgeving toegepast kunnen worden.

63
Hoe wordt er, mede gelet op de beleidsdoelstellingen, aandacht besteed aan het vergroten van kennis bij het mkb over digitale weerbaarheid? Hoeveel financiële middelen stelt u hiervoor beschikbaar?

Antwoord
Zie hiervoor ook het antwoord op vragen 37, 40 en 62. Voor een toelichting op de financiële middelen verwijs ik naar het antwoord op vraag 38.

64
Welk budget is beschikbaar in 2022 voor de brede EZK-inzet op cybersecurity? Met de aangekondigde aanvullingen, hoe komt het budget er uit te zien in 2023?

Antwoord
In 2022 is het EZK-brede budget voor cybersecurity 27 miljoen euro. In 2023 is het budget 29,9 miljoen euro. Dit is inclusief het budget voor cybersecurity van het Agentschap Telecom, het budget voor het Digital Trust Center en het budget voor het Cybersecurity Incident Response Team voor digitale dienstverleners (CSIRT-DSP). Dit is ook inclusief de middelen uit het coalitieakkoord voor 2022 en 2023. Naast de versterking van EZK-onderdelen op cybersecurity wordt een deel van de middelen van het coalitieakkoord ook benut om incidentele middelen om te zetten in structurele middelen.

65
Hoe wordt de informatievoorziening van het Computer Security Incident Response Team (CSIRT) en het CSIRT-DSP uitgebreid? Welke concrete stappen worden hiervoor gezet?

Antwoord
De uitbreiding start met het vragen van meer technische details van de digitale dienstverleners (= Digital Service Providers, afgekort DSP's) zodat het CSIRT-DSP ze nog concreter kan informeren over hun kwetsbare systemen. Technische details zijn dan bijvoorbeeld AS-nummers, IP-adressen en DNS-namen van de DSP. Hierdoor wordt het mogelijk om de informatie uit de bronnen van het CSIRT-DSP beter terug te leiden tot de IT-systemen van de DSP. Deze uitbreiding zal geautomatiseerd worden zodat de informatie ook sneller terecht komt bij de DSP. Voor deze automatisering wordt samengewerkt met het DTC.

66
Aan welke groepen en bedrijven in niet-vitale sectoren die willen samenwerken op cybersecurity-terrein is reeds subsidie verstrekt?

Antwoord
De volgende samenwerkingsverbanden hebben subsidie ontvangen uit de regeling cyberweerbaarheid:
In 2018: Cyberweerbaarheid Nederlandse Defensie & Veiligheidsindustrie (NIDV), Cybersecurity Center Maakindustrie, Cyber Security Programma Noordzeekanaalgebied, Vergroting Cyberweerbaarheid Groentezaadveredelingsbedrijven, Cyberweerbaarheid in Limburg, Stichting Cyberweerbaarheid Noord Nederland.
In 2019: NuBNO (digitale veiligheid in zorginstellingen), Cyberweerbaarheidscentrum Brainport, CYSSEC, stichting Cyberwerkplaats, Cyberweerbaarheidsnetwerk Drechtsteden, Groep Educatieve Uitgeverijen: Cyberweerbaarheid in het educatieve domein, NBIP (Nationale Beheersorganisatie Internet Providers).

In 2020: Cybernetwerk Zuid Hollandse Eilanden, FERM, Cyberchain, MKB Cyber Heroes, Agrifood Cyberweerbaarheid, MKB Cyber Campus.
In 2021: Dutch Institute for Vulnerability Disclosure (DIVD), Cyberweerbaar tegen DDoS, Cyberweerbaarheidscentrum Greenport West Holland, Netwerk voor Risk Based Cyberweerbaarheid, MKB Cybersecurity Governance Scan.

67
Hoeveel geld is er de afgelopen vijf jaar uitgegeven aan het DTC?

Antwoord
Het DTC bestaat pas vanaf 2018. De uitgaven vanaf 2018 tot en met 2021 bedragen resp. € 2,368, € 2,407, € 2,336 en € 4,176 miljoen.

68
Hoeveel organisaties heeft het DTC de afgelopen vijf jaar bereikt?

Antwoord
Omdat het DTC veel werkt met schakelorganisaties, waaronder de 48 samenwerkingsverbanden, om de uiteindelijke doelgroep van ondernemend Nederland te bereiken is het niet mogelijk om exact aan te geven hoeveel organisaties het DTC de afgelopen 5 jaar bereikt heeft. Wel kunnen we een indicatie geven van het bereik van de diverse communicatiekanalen die het DTC tot haar beschikking heeft:
- de website heeft 227.126 bezoeken gehad in 2021;
- en in 2022 staat het aantal websitebezoeken nu op 168.879;
- de DTC Community heeft 1440 leden;
- het Twitterkanaal van het DTC telt 2.018 volgers;
- het LinkedInkanaal heeft 7.195 volgers.

Vragen inzake vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2023

69
Hoeveel geld komt er totaal extra bij op cybersecuritygebied op de gehele begroting? Kunt u dit afzetten tegen voorgaande jaren?

Antwoord
Dit kabinet heeft evenals het vorige kabinet structurele middelen vrijgemaakt die specifiek zijn gelabeld voor het verhogen van de digitale weerbaarheid. Het vorige kabinet heeft € 95 miljoen structureel geïnvesteerd in de versterking van digitale weerbaarheid. Dit kabinet investeert een extra € 111 miljoen euro structureel in cybersecurity. Voor JenV zal de uiteindelijk structurele investering opbouwen naar € 35.5 miljoen per jaar. In de tabel is de opbouw van de structurele investering weergegeven:

Ministerie	2022	2023	2024	2025	2026	2027 en verder
JenV	8,7	14,8	29,5	29,5	29,5	35,5
waarvan NCSC	6,6	13,7	27,5	27,5	27,5	33

Deze gelden komen bovenop de structurele investering van € 16 miljoen die JenV vanaf 2021 structureel krijgt (opgebouwd van € 14 miljoen structurele investering in 2019, naar € 15 miljoen in 2020, tot € 16 miljoen vanaf 2021).

70
Wat was het budget van het Nationaal Cyber Security Centrum (NCSC) in 2021? Hoe zag dat budget er uit in 2020 en 2019?

Antwoord
Het budget van het Nationaal Cyber Security Centrum bedroeg in 2021 € 27,1 miljoen. In 2020 en 2019 bedroeg het budget respectievelijk € 26,797 miljoen en € 23,729 miljoen.

71
Waar is het geld van de begrotingsstaten van het Ministerie van Justitie en Veiligheid voor de inlichtingendiensten voor bedoeld?

Antwoord
Het geld van de begrotingsstaten van het Ministerie van Justitie en Veiligheid voor de inlichtingendiensten komt uit een bredere structurele investering van € 60 miljoen in 2022 oplopend tot € 300 miljoen structureel vanaf 2027. Met deze investering worden onder meer de AIVD en MIVD versterkt en investeringen op het gebied van economische veiligheid en de vitale infrastructuur gedaan. De dreiging kennen en begrijpen is de eerste stap richting een digitaal weerbaar Nederland. Het kabinet investeert daarom in de onderzoekscapaciteit van de Inlichtingen en Veiligheidsdiensten ten behoeve van inlichtingenmatig-diepteonderzoek. Hierdoor ontstaat breder zicht in huidige en voorstelbare digitale dreiging. Daarmee worden unieke inlichtingen vertaald naar specifiek handelingsperspectief zodat afnemers zich beter kunnen weren.

72
Hoeveel geld ontvangt de Dutch Institute for Vulnerability Disclosure (DIVD) van de Rijksoverheid? Hoeveel was dit voorafgaande jaren?

Antwoord
Vanuit het Digital Trust Center heeft DIVD, vanuit de subsidieregeling 2021 (uitgevoerd door de Rijksdienst voor Ondernemend Nederland), een bedrag van in totaal € 197.500 subsidie ontvangen.

73
Hoeveel van het extra geld voor cybersecurity gaat naar de Nationaal Coördinator Terrorisme en Veiligheid (NCTV)? Waar wordt dit geld aan besteed?

Antwoord
De NCTV heeft zelf geen extra middelen gekregen voor cybersecurity. De NCTV had al een coördinerende rol onder vorige kabinetten en strategieën en dit wordt voortgezet.

74
Hoeveel cyberaanvallen hebben in 2021 plaatsgevonden in Nederland? Kan dit aantal worden afgezet tegen andere jaren zoals 2020,2019 en 2018?

Antwoord
Het NCSC heeft geen zicht op alle cyberaanvallen die in Nederland hebben plaatsgevonden. Het NCSC houdt een registratie bij van cyberincidenten die bij het NCSC gemeld worden door organisaties binnen de Rijksoverheid en vitale infrastructuur en partners. Dit betreft bijvoorbeeld meldingen van kwetsbaarheden in systemen, ransomwareaanvallen, DDoS-aanvallen en malware-samples. In 2021 zijn er van dit soort incidenten 2059 meldingen binnengekomen. Dit is een stijgende lijn ten opzichte van de jaren 2020, 2019 en 2018.

Er is dus geen centrale registratie van het aantal cyberaanvallen dat in heel Nederland plaatsvindt. Hoeveel cyberaanvallen hebben plaatsgevonden is daardoor niet bekend.
Registratie van cyberaanvallen is complex om uiteenlopende redenen, waaronder de definitie: wat wordt precies bedoeld met een cyberaanval? Een uniforme definitie ontbreekt daarvoor.

75
Hoeveel vitale bedrijven/instellingen zijn in 2021 slachtoffer geworden van cyberaanvallen?

Antwoord
Hoeveel vitale bedrijven/instellingen slachtoffer zijn geworden van cyberaanvallen is niet bekend bij de NCTV.
Het NCSC heeft namelijk alleen zicht op (geslaagde) cyberaanvallen bij vitale aanbieders die gemeld zijn bij het NCSC. Vitale aanbieders mogen vrijwillig een melding doen bij het NCSC van incidenten of zijn verplicht daartoe wanneer het een meldplichtig incident betreft. Het NCSC heeft alleen zicht op het totaal aantal incidenten dat gemeld is bij het NCSC door onder andere vitale aanbieders.

76
Hoeveel en welke computercrisisteams zijn bij ministeriële regeling krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) aangewezen? Wat zijn hun taken?

Antwoord
De volgende organisaties zijn bij ministeriële regeling aangewezen als computercrisisteams:
- de Informatiebeveiligingsdienst, onderdeel van VNG Realisatie B.V.;
- de Stichting Z-CERT;
- SURFcert, onderdeel van SURFnet B.V. en;
- CERT Watermanagement, onderdeel van het openbaar lichaam Het Waterschapshuis.

Computercrisisteams hebben als taak om aan andere aanbieders binnen hun sector bijstand te verlenen bij dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.

77
Welke organisaties die objectief kenbaar tot taak hebben om organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's) telt Nederland buiten het Digtal Trust Center (DTC)?

Antwoord
Naast het DTC zijn de volgende organisaties aangewezen tot OKTT: Vereniging Abuse Information Exchange, de Nationale Beheersorganisatie Internetproviders (NBIP), Stichting Cyber Weerbaarheidscentrum Brainport (CWB), Cyberveilig Nederland, Connect2Trust en FERM Rotterdam (opgericht voor bedrijven die onderdeel zijn van de Rotterdamse haven).

78
Hoe ziet het totale Landelijk Dekkend Stelsel (LDS) dat Nederland kent er uit? Uit welke organisaties en instellingen is het opgebouwd?

Antwoord
Op de website van de NCTV staat een interactief overzicht van het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS) gepubliceerd, zie https://www.nctv.nl/onderwerpen/landelijk-

dekkend-stelsel. Hierin staan alle type schakelorganisaties afgebeeld en de verschillende doelgroepen die zij bedienen.

Binnen het stelsel fungeert het Nationaal Cybersecurity Centrum (NCSC) als knooppunt in het netwerk ten opzichte van andere schakelorganisaties. Waarbij het NCSC en CSIRT-DSP via verschillende bronnen informatie ontvangen over digitale dreigingen en kwetsbaarheden.
Als nationaal Cyber Security Incident Response Team (CSIRT) voor digitale dienstverleners biedt het CSIRT-DSP ondersteuning en advies aan digitale dienstverleners. Daarnaast deelt het CSIRT-DSP actuele dreiging- en kwetsbaarhedeninformatie met haar doelgroep.

De doelgroep van het NCSC bestaat uit alle Rijksoverheidsorganisaties en vitale aanbieders. Ook deelt het NCSC bepaalde informatie over dreigingen en kwetsbaarheden aan andere schakelorganisaties, zodat ook partijen buiten de doelgroep van het NCSC deze informatie kunnen ontvangen. Deze schakelorganisaties zijn de krachtens de WBNI aangewezen CERTs en OKTTs.
CERT staat voor Computer Emergency Response Team. Een team van deskundigen dat beveiligingsincidenten oplost. Binnen het Landelijk Dekkend Stelsel (LDS) worden organisaties aangewezen als CERT door de NCTV en het NCSC om zo wederzijdse informatie-uitwisseling mogelijk te maken binnen de wet. De aangewezen CERTs binnen het LDS zijn de Informatiebeveiligingsdienst voor gemeenten als onderdeel van de Vereniging van Nederlandse Gemeenten, Stichting Z-CERT voor organisaties in de zorgsector, CERT Watermanagement voor de waterschappen als onderdeel van het Waterschapshuis en SURFcert voor Nederlandse universiteiten, hogescholen, umc's, mbo-instellingen en onderzoeksinstellingen.

OKTT is een afkorting voor een organisatie die «objectief kenbaar tot taak» heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk en informatiesystemen. Objectief kenbaar betekent dat het duidelijk moet zijn dat het delen van dit soort informatie een taak is van de betreffende schakelorganisatie. Een OKTT vertegenwoordigt een sector, regio, ecosysteem of ander relevant verband en heeft een duidelijk gemarkeerde doelgroep.

Voorbeelden van OKTTs zijn het Digital Trust Center, Vereniging Abuse Information Exchange, Stichting Nationale Beheersorganisatie Internetproviders, Stichting Cyber Weerbaarheidscentrum Brainport, Cyberveilig Nederland, Connect2Trust en FERM Rotterdam (opgericht voor bedrijven die onderdeel zijn van de Rotterdamse haven).

79
Hoeveel aangiftes gerelateerd aan cybercriminaliteit zijn in 2021 geregistreerd bij de politie? Kan dit aantal worden afgezet tegen de aantallen in 2020 en 2019?

Antwoord
Onderstaande tabel geeft in de eerste rij een overzicht van de aangiftes gerelateerd aan cybercrime in enge zin. Daarnaast is ter informatie opgenomen het aantal aangiftes van fraude met onlinehandel en het aandeel internetaangiften van overige horizontale fraude (d.w.z. whatsappfraude). Voor whatsappfraude geldt dat dit vanaf mei 2020 als aangifte wordt geregistreerd.

Aangifte opgenomen	2019	2020	2021
Fraude met online handel	49.688	56.796	49.530
Overige horizontale fraude	7	18.850	20.691
Totaal	54.176	85.891	83.704

80
In hoeveel gevallen van de cybercrime is overgegaan tot vervolging? Kan dit worden afgezet tegen 2020 en 2019?

Antwoord
In de jaren 2019 t/m 2021 betrof het aantal gevallen waar is overgegaan tot vervolging:

2019	182
2020	257
2021	352

Deze aantallen betreffen cybercrime (in enge zin) en zijn een optelsom van dagvaardingen, voegingen, OM-transacties en strafbeschikkingen.

81
Hoeveel cybercriminelen zijn in 2021 veroordeeld? Kunt u deze categorie uitsplitsen per soort straf?

Antwoord
In 2021 zijn er in eerste aanleg 123 zaken geweest met een al dan niet onherroepelijke veroordeling voor een cybercrimefeit. In 1 van die zaken werd door de rechter geen straf opgelegd en in 122 zaken werd wel straf opgelegd, te weten: in 82 zaken een vrijheidsstraf, in 7 zaken een geldboete, in 73 zaken een werkstraf en in 4 zaken een leerstraf. In een zaak kunnen combinaties van meerdere soorten straf worden opgelegd.

82
Wat was de verhouding meerder/minderjarig bij het aantal veroordeelde cybercriminelen in 2021? Hoe verhoudt zich dit tot voorgaande jaren?

Antwoord
In 18% van de 123 zaken in 2021 met een al dan niet onherroepelijke veroordeling voor een cybercrimefeit, was de veroordeelde op het moment van het plegen van het cybercrimefeit minderjarig. Over de hele periode 2017 t/m 2021 bezien was 12% van de veroordeelden voor een cybercrimefeit minderjarig.

83
In hoeveel gevallen is in 2021 het traject Hack_Right opgelegd bij minderjarigen als aanvullend straftraject? Kan dit aantal worden afgezet tot de jaren 2020 en 2019?

Antwoord
In de tabel is weergegeven hoe vaak een Hack_Right-traject is opgelegd, zowel binnen als buiten het strafrecht. Binnen Hack_Right zijn er verschillende onderdelen die in het kader van een Halt-afdoening, een bijzondere voorwaarde of een werkstraf kunnen worden ingezet. Hack_Right kan dus zowel buitenstrafrechtelijk (uitvoering via Halt) als binnen het strafrecht worden ingezet (uitvoering door onder meer de Reclassering).

Aantal HR-trajecten (instroom) → Jaar ↓	Reclassering	Halt
2019	6	8
2020	6	4
2021	5	3
2022	3	–

84
Hoeveel minderjarigen hebben het traject Hack_Right succesvol afgerond?

Antwoord
Het trajecten in 2019, 2020 en 2021 zoals genoemd in de tabel bij vraag 83 zijn allen succesvol afgrond. De trajecten gestart in 2022 zijn nog gaande.

85
Hoe ziet het straftraject Hack_Right er uit qua lengte en inhoud?

Antwoord
Het straftraject Hack_Right is een alternatief of aanvullend straftraject voor jongeren en jongvolwassenen die voor het eerst een cyberdelict hebben gepleegd. Het doel van Hack_Right is om recidive te voorkomen en het talent van jongeren verder te ontwikkelen binnen de kaders van de wet. Binnen Hack_Right zijn er verschillende onderdelen die in het kader van een Halt-afdoening, een bijzondere voorwaarde of een werkstraf kunnen worden ingezet. Hack_Right kan dus zowel buitenstrafrechtelijk (uitvoering via Halt) als binnen het strafrecht worden ingezet (uitvoering door onder meer de Reclassering).

De onderdelen van Hack_Right spelen in op criminogene factoren voor het plegen van het delict. Het traject kent, afhankelijk van de toepassing, een korte (maximaal 20 uur) en lange variant (maximaal 240 uur). Hack_Right bestaat op hoofdlijnen uit vier onderdelen: juridische en ethische grenzen, impactbesef, excuus en schadeherstel, en digitaal talent en digitale weerbaarheid. Tijdens een Hack_Right-traject voert de deelnemer ook één of meerdere opdrachten en werkzaamheden uit bij een bedrijf of organisatie gespecialiseerd in ICT.

86
Hoeveel is besteed aan het straftraject Hack_Right in 2021?

Antwoord
Voor 2020 en 2021 is een subsidie van € 278.000 verstrekt.

87
Hoeveel (voorlichting)campagnes gerelateerd aan cybercriminaliteit lopen momenteel in Nederland? Hoeveel campagnes zijn reeds voltooid? Om welke campagnes gaat het?

Antwoord
Op 6 juli 2022 bent u geïnformeerd over de preventieactiviteiten voor het tegengaan van cybercrime in het midden- en kleinbedrijf. Bij deze brief is als bijlage een overzicht opgenomen van de campagnes ter bewustwording van online veiligheid, zowel in Nederland als in andere lidstaten van de Europese Unie, zoals toegezegd door de toenmalige Minister van Justitie en Veiligheid in het Commissiedebat Online Veiligheid en Cybersecurity op 1 december 2021 (kamerstuk 26 643, nr. 907).

88
Hoeveel politieagenten waren in 2021 fulltime bezig met de opsporing van cybercriminaliteit? Hoeveel agenten deden dit parttime in hetzelfde jaar? Kan dit aantal worden afgezet tegen de jaren 2020 en 2019?

Antwoord
De politie heeft het Team High Tech Crime (THTC), met een capaciteit van 120 fte. Vanaf 2016 is de politie gestart met de opbouw cybercrimeteams in de regionale eenheden met een gemiddelde grootte van 10 fte. Met de gelden die beschikbaar kwamen vanuit het vorige Regeerakkoord en de Miljoenennota 2018 zijn vanaf 2019 in totaal 145 fte extra ingestroomd voor cybercrime, waarvan 95 fte in de cybercrimeteams van de regionale eenheden en de overige fte o.a. bij de Landelijke eenheid voor het verbeteren van de informatiepositie op het gebied van cybercrime. Het THTC en de regionale cybercrimeteams werken eenheidsoverstijgend samen in de aanpak van cybercriminele fenomenen en dadergroepen. Daarnaast worden reguliere cybercrime onderzoeken ook uitgevoerd door districtsrecherches en basisteams.

89
Hoeveel rechercheurs zijn momenteel werkzaam bij de High Tech Crime teams van de politie?

Antwoord
Zie het antwoord op vraag 88.

90
Welke maatregelen worden concreet ingezet om verdienmodellen van cybercriminelen aan te pakken?

Antwoord
In opsporingsonderzoeken naar cybercriminele fenomenen wordt naast of aanvullend op het opsporen en vervolgen van de daders ook ingezet op het verstoren van de criminele werkwijze. Daarbij kan het bijvoorbeeld gaan om het offline halen van systemen om DDoS- of ransomwareaanvallen te stoppen of het informeren van personen dat criminelen hun inloggegevens hebben buitgemaakt, zodat deze kunnen worden gewijzigd voordat er misbruik van wordt gemaakt. Daarmee worden slachtofferschap en schade beperkt. In het oog springende voorbeelden van grotere publiek-private projecten om criminele verdienmodellen tegen te gaan zijn de al langer bestaande website NoMoreRansom.org, waar onder meer bij de politie en securitybedrijven bekende ontsleutelgegevens van ransomware worden gedeeld, en NoMoreDDoS, waarin publieke en private partners samenwerken om DDoS-aanvallen te kunnen voorkómen en beperken.

91
Welke concrete maatregelen zijn tot dusver genomen om de aangiftebereidheid van cyberdelicten te verhogen?

Antwoord
De politie heeft het voor diverse cybercriminele fenomenen mogelijk gemaakt om online aangifte doen, waardoor aangifte doen eenvoudiger is geworden en minder tijd kost.

92
Hoeveel cross-sectorale oefeningen met vitale aanbieders zijn tot nu toe georganiseerd door het NCSC de afgelopen jaren? Hoeveel oefeningen zijn georganiseerd in 2021? Hoeveel waren dit er in 2020? Hoeveel oefeningen staan op de planning de komende tijd?

Antwoord
Het NCSC organiseert de ISIDOOR-oefening voor vitale aanbieders. Deze is in 2015, 2017 en 2021 uitgevoerd en is opnieuw gepland voor 2023. Ook sluit het NCSC met regelmaat aan bij andere oefeningen die door de sectoren of door (internationale) partners worden georganiseerd. Daarnaast publiceert het NCSC, samen met partners, kennisproducten waarmee organisaties zelf oefeningen kunnen organiseren.

93
Met welke concrete voorstellen en stappen wordt de motie-Hermans c.s. (Kamerstuk 35 788, nr. 120) uitgevoerd?

Antwoord
In de brief over de preventieactiviteiten voor het tegengaan van cybercrime in het midden- en kleinbedrijf van 6 juli 2022 (kamerstuk 26 643, nr. 907) bent u geïnformeerd over de uitvoering van de motie-Hermans.

94
Kunt u een overzicht geven van alle maatregelen en middelen die het Ministerie van Justitie en Veiligheid inzet ten aanzien van cybersecurity en cybercrime?

Antwoord
De maatregelen die het Ministerie van JenV inzet ten aanzien van cybersecurity zijn beschreven in de Nederlandse cybersecuritystrategie (NLCS) en het bijbehorende actieplan die op 10 oktober 2022 zijn aangeboden aan de Tweede Kamer. Dit kabinet heeft structurele middelen vrijgemaakt die specifiek zijn gelabeld voor het verhogen van de digitale weerbaarheid. Dit kabinet investeert een extra € 111 miljoen euro structureel in cybersecurity (zie antwoord op vraag 189). De middelen die specifiek het Ministerie van JenV inzet zijn weergegeven in bijlage 1 van de NLCS. Van dat bedrag zet het Ministerie van JenV € 35,5 mln. via een oplopende reeks in op versterking van cybersecurity waarvan € 33 mln. t.b.v. het Nationaal Cyber Security Centrum. Daarnaast heeft het vorige kabinet in totaal € 95 miljoen structureel geïnvesteerd in de versterking van digitale weerbaarheid waarvan het Ministerie van JenV € 29 mln. heeft ingezet t.a.v. cybersecurity. Een totaaloverzicht van alle middelen die het Ministerie van JenV inzet t.a.v. cybersecurity is niet precies te geven omdat de middelen die het ministerie besteedt aan de digitale veiligheid van de eigen organisatie onderdeel zijn in het bedrijfsvoeringsbudget.

Wat betreft de inzet op cybercrime wordt door JenV uit de coalitieakkoordmiddelen tot structureel € 2,5 mln. per jaar uitgegeven aan tegengaan van cybercrime, waarvan een groot deel gereserveerd is voor preventieve maatregelen (zie de tabel in het antwoord op vraag 189). Daarnaast wordt er in de jaren 2022–2025 jaarlijks, via het Centrum voor Criminaliteitspreventie en Veiligheid, € 2 mln. euro geïnvesteerd in de City Deal «Lokale weerbaarheid Cybercrime» om succesvolle en effectieve pilots landelijk op te schalen en te verspreiden onder gemeenten, en om Platforms Veilig Ondernemen en regionale samenwerkingsverbanden voor Openbare Orde en Veiligheid te ondersteunen. Het doel is om het versterken van de weerbaarheid tegen cybercrime een vast onderdeel van de activiteiten van het lokaal bestuur te maken door gemeenten te stimuleren (op termijn) de preventie van cybercriminaliteit op te nemen in de Integrale Veiligheidsplannen. Een nadere detaillering van de maatregelen ten aanzien van cybercrime is te vinden in de Kamerbrief integrale aanpak cybercrime van 28 mei 2021 (Kamerstuk 26 643, nr. 768) en de Kamerbrief over preventieactiviteiten voor het tegengaan van cybercrime in het midden- en kleinbedrijf van 6 juli 2022 (kamerstuk 26 643, nr. 907). U heeft 4 november een Kamerbrief ontvangen over de integrale aanpak van cybercrime.

95
Kunt u toelichten waarom gekozen wordt om een nulmeting uit te voeren van de Nederlandse Cybersecuritystrategie?

Antwoord
Om inzicht te krijgen in de effecten van de realisatie van de Nederlandse Cybersecurity Strategie (NLCS), van deze effecten te leren, mogelijk bij te sturen en verantwoording te kunnen afleggen over de uitvoering van de NLCS, bevat de NLCS een evaluatieplan. Drie jaar na de start van de uitvoering van de NLCS -dat komt neer op halverwege de looptijd- zal er in elk geval een evaluatieonderzoek worden uitgevoerd. Ter voorbereiding op dit evaluatieonderzoek wordt voorafgaand aan de implementatie van de NLCS een nulmeting uitgevoerd.

96
Wat zijn de resultaten van eerdere evaluaties, gelet op het feit dat er regelmatig wordt geëvalueerd of het juridisch kader nog goed is toegesneden op nieuwe technologieën? Op welke manier wordt hieraan gevolg gegeven?

Antwoord
Zie het antwoord op vraag 107.

97
Met welke partijen wordt werkt u samen om voldoende informatie te verzamelen over nieuwe technologieën en de gevolgen daarvan?

Antwoord
We werken samen met/consulteren vele partijen om voldoende informatie te verzamelen over nieuwe technologieën en de mogelijke gevolgen daarvan. Te denken valt aan de volgende (categorieën van) partijen:
- Adviesorganen zoals de Wetenschappelijke Raad voor het Regeringsbeleid, het Rathenau Instituut en de Cyber Security Raad;
- Diverse (technische) universiteiten en hogescholen;
- Kennisinstellingen zoals de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek, het Nederlands Instituut voor Publieke Veiligheid, het Rijksinstituut voor Volksgezondheid en Milieu (Analistennetwerk Nationale Veiligheid) en Stichting Toekomstbeeld der Techniek;
- Maatschappelijke organisaties zoals Amnesty International, Bits of Freedom, Open State Foundation en de Waag;
- Bedrijven/adviesbureaus zoals Microsoft, Gartner, Forrester en SOGETI/ Verkenningsinstituut voor Nieuwe Technologie;
- Europese/internationale organisaties zoals de Europese Unie, de Raad van Europa, de Organisatie voor Economische Samenwerking en Ontwikkeling (Regulatory Policy Committee) en de International Civil Aviation Organization (werkgroep Public Key Directory);
- Publiek-private samenwerkingen zoals de AI-Coalitie, Hague Security Delta en ECP/Platform voor de InformatieSamenleving.

Uiteraard voeren we over nieuwe technologieën ook het gesprek met de politie, het openbaar ministerie en de rechterlijke macht. Ook wordt voor JenV onderzoek gedaan of uitbesteed door het Wetenschappelijk Onderzoek- en Documentatiecentrum. Binnen de overheid werken we samen in bijvoorbeeld de Werkgroep Technologieverkenningen, de Rijks Innovatie Community en de RijksAcademie voor Digitalisering en Informatisering Overheid.

98
Hoe verhoudt de totale hoeveelheid schade van cybercrime en gedigitaliseerde criminaliteit zich ten opzichte van traditionele criminaliteit, gezien het feit dat beide vormen van criminaliteit net zo vaak slachtoffers maken?

Antwoord
Het CBS heeft op 22 september een onderzoek naar de schade van vermogensdelicten tegen privépersonen gepubliceerd. Daaruit blijkt dat 3,2 miljoen vermogensdelicten en 1 miljoen vernielingen zijn gepleegd in 2021. De totale financiële schade van deze criminaliteit bedroeg € 2,5 miljard. Ongeveer een kwart hiervan betrof online criminaliteit, een kwart betrof diefstal van voertuigen, een kwart diefstal van ander goed en een kwart werd veroorzaakt door vernieling.

Delicten tegen organisaties zijn hierin niet meegenomen. De schade daarvan is niet bekend. Er zijn in het verleden diverse schattingen over de omvang van de schade gepubliceerd, onder meer door bedrijven die zich bezighouden met cybersecurity. Deze kunnen echter niet worden bevestigd.

99
Hoe hoog is het opsporingspercentage van cybercrime en gedigitaliseerde criminaliteit? Hoe verhoudt dat zich tot het opsporingspercentage van traditionele criminaliteit?

Antwoord
Het ophelderingspercentage voor cybercrime was in 2021 7%. Gedigitaliseerde criminaliteit is een zeer breed begrip en omvat vele soorten criminaliteit. Enkele veel voorkomende vormen zijn vriend-in-noodfraude en fraude met online handel. Voor vriend-in-noodfraude is het ophelderingspercentage 2% en voor fraude met online handel is het 2%. Het ophelderingspercentage van alle geregistreerde misdrijven in 2021 is 28%.

100
Kunt u toelichten hoe de evaluatie van de Autoriteit Persoonsgegevens (AP) in 2023 er precies uit gaat zien?

Antwoord
In 2023 bestaat de AP vijf jaar. Volgens art. 39 van de kaderwet zelfstandig bestuursorganen moet er iedere vijf jaar een evaluatie naar doelmatigheid en doeltreffendheid van het functioneren van de AP worden uitgevoerd. Over de uitvoering van de evaluatie is JenV op dit moment in gesprek met de AP.

101
Hoeveel slachtoffers hebben cybercriminelen in 2021 gemaakt?

Antwoord
Uit de Veiligheidsmonitor 2021 blijkt dat 6,9% van de ondervraagden slachtoffer is geworden van hacken. Het betreft natuurlijke personen.

Uit het Cybersecurityonderzoek Alert Online 2022 blijkt dat in 2021 1,7% van de ondervraagde ICT-medewerkers bij bedrijven te maken heeft gehad met ransomware, 1,2% met een systeem dat door malware niet meer werkte, 1,1% met ongeautoriseerde toegang tot een apparaat en 0,7% met ongeautoriseerde toegang tot een account.
Deze aantallen betreffen cybercrime in enge zin. Het slachtofferschap van vormen van gedigitaliseerde criminaliteit (zoals online bedreiging of fraude) is hierin niet meegenomen.

102
Wat was in 2021 het budget van het Openbaar Ministerie om te besteden aan de aanpak van cybercrime en gedigitaliseerde criminaliteit? Hoe zag dit budget er uit in 2020 en 2019?

Antwoord
Het betrof € 2,7 miljoen voor elk jaar.

103
Welke concrete projecten of afspraken worden opgesteld en gemaakt tussen de bewindspersonen van Binnenlandse Zaken (BZK), Justitie en Veiligheid (JenV) en Economische Zaken en Klimaat (EZK) om gezamenlijk op te trekken in de strijd tegen cybercrime?

Antwoord
De Ministeries van BZK, EZK en JenV geven samen vorm aan de integrale aanpak van cybercrime. Binnen die aanpak is JenV actief op het gebied van preventie, opsporing, vervolging en verstoring. EZK (Digitale Economie) en BZK (Digitale samenleving) ontplooien met name activiteiten op het gebied van preventie. De preventieactiviteiten worden onderling afgestemd of gezamenlijk vormgegeven. De inzet op preventie concentreert zich op drie onderdelen: (potentiële) slachtoffers weerbaarder te maken tegen cybercrime (slachtofferpreventie) door hun basisveiligheid te vergroten, de daderpopulatie te verkleinen (daderpreventie) door middel van gerichte interventies om daderschap te ontmoedigen en recidive te beperken, en systemen en producten veiliger maken (situationele preventie). Sinds 2018 bent u ieder jaar over de aanpak geïnformeerd, meest recentelijk op 28 mei 2021 (Kamerstuk 26 643, nr. 768). In de bijlage bij die brief is een overzicht van maatregelen opgenomen. Voorbeelden daarvan zijn diverse preventiecampagnes, de ondersteuning van het niet-vitale bedrijfsleven door het Digital Trust Center, de ondersteuning van gemeenten bij de lokale aanpak van cybercrime en de verbetering van veilige hard- en software.

104
Kunt u toelichten wat de aanleiding is voor het willen formuleren van een strategische visie op internationale gegevensstromen?

Antwoord
In de huidige geglobaliseerde wereld wordt op grote schaal grensoverschrijdend persoonsgegevens verwerkt. Deze persoonsgegevens worden niet exclusief in Nederland of de Europese Unie (EU) opgeslagen, en soms verdeeld over verschillende landen. De Algemene verordening gegevensbescherming (AVG) regelt dat de bescherming die wordt geboden meegaat met die gegevens, wat betekent dat de regels ter bescherming van persoonsgegevens van toepassing blijven, ongeacht waar de gegevens terechtkomen. Dit geldt ook wanneer gegevens worden doorgegeven aan een derde land. Desondanks is inzicht in dergelijke gegevensstromen beperkt. Met behulp van een strategische visie wil het kabinet meer grip en inzicht krijgen op deze gegevensstromen en bezien of de bescherming die geboden wordt adequaat is.

105
Wat behelst de strategische visie op internationale gegevensstromen?

Antwoord
Zie het antwoord op vraag 104.

106
Waar bestaat het initiatief Cyber Info/Intel Cel uit? Welke concrete taken en verantwoordelijkheden hebben zij?

Antwoord
De Cyber Info/ Intel Cel is een versterkt samenwerkingsverband bestaande uit vijf organisaties die een opsporings-, inlichtingen- of weerbaarheidstaak hebben op het gebied van cybersecurity of daar nauw aan verbonden zijn. Het betreffen de volgende organisaties:
- de Nationale Politie;
- de Algemene Inlichtingen- en Veiligheidsdienst;
- de Militaire Inlichtingen- en Veiligheidsdienst;
- het Nationaal Cyber Security Centrum en
- het Openbaar Ministerie.

Deze versterkte samenwerking en afspraken daarover zijn vastgelegd in een convenant dat op 15 juni 2020 in de Staatscourant is gepubliceerd. In dit convenant is vastgelegd dat deze organisaties fysiek samenwerking op een locatie en daarnaast zijn er afspraken gemaakt over de vertrouwelijke verwerking van gegevens. Het doel van deze geïntensiveerde samenwerking is het versterken van het landelijk situationeel beeld, door meer en sneller handelingsperspectief met de deelnemende organisaties te kunnen delen. Hiermee wordt de digitale slagkracht en vergroot en de digitale veiligheid versterkt.

107
Kunt u op een rij zetten welke evaluaties u sinds 2018 heeft geïnitieerd gericht op de vragen of het juridisch kader nog is toegesneden op nieuwe technologieën (zoals deepfakes, gezichtsherkenning, immersieve technologieën) en of het nodig is te reguleren of bestaande normen te verhelderen? Kunt u hierbij aan aangeven welke acties zijn voortgekomen uit die evaluaties?

Antwoord
De Stand van zaken Uitvoering Agenda horizontale privacy van 5 februari 2021 bevat een overzicht van onderzoeken en de beleidsreactie daarop naar aanleiding van de vraag of het huidige juridische kader is toegesneden op nieuwe technologieën (Kamerstukken II 2020/2021, 2953300). Zo heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) onder meer onderzoek laten verrichten naar de vraag of het strafrecht en privacyregelgeving het gebruik (en misbruik) van hobbydrones en apparaten waarmee heimelijk informatie over personen kan worden verzameld, goed reguleert. Zoals uiteen wordt gezet in de Uitvoering Agenda horizontale privacy heeft dit onderzoek onder meer geleid tot een privacyhandleiding voor dronevliegers.

Met betrekking tot gezichtsherkenning, waarover in 2020 het WODC onderzoek «Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties» is gepubliceerd, heeft het kabinet het wettelijk kader in het voorstel Uitvoeringswet AVG (Verzamelwet gegevensbescherming) aangescherpt, opdat nog duidelijker is dat de verwerking van bijzondere persoonsgegevens slechts onder zeer strikte voorwaarden kan worden toegestaan. Dit voorstel zal nog dit najaar aan uw Kamer worden aangeboden. In reactie op de in de vraag genoemde onderzoeken naar regulering van deepfakes en regulering van immersieve technologieën (naar aanleiding van motie Van der Graaf/Van der Staaij: Kamerstukken II 2019/20, 35 300 VI, nr. 73), verwacht het kabinet nog dit najaar een beleidsreactie aan de Tweede Kamer te verzenden.

108
Hoe wordt beoordeeld of het juridisch kader nog is toegesneden op nieuwe technologieën (zoals deepfakes, gezichtsherkenning, immersieve technologieën) en of het nodig is te reguleren of bestaande normen te verhelderen? Waarom is hier niets over te vinden in de Strategische Evaluatie Agenda?

Antwoord
De systematiek van de Strategische Evaluatie Agenda is in 2022 geïmplementeerd. Die is in een opbouwfase en niet limitatief. In de beantwoording van vraag 107 heb ik aangegeven hoe de inzichten uit de diverse WODC-onderzoeken naar de door u genoemde technologische ontwikkelingen worden verwerkt in het juridisch kader. Gegeven de status van die trajecten is evaluatie op dit moment niet aan de orde.

109
Kunt u toelichten waarom in de Strategische Evaluatie Agenda geen evaluaties zijn opgenomen naar de vragen of het juridisch kader nog is toegesneden op nieuwe technologieën (zoals deepfakes, gezichtsherkenning, immersieve technologieën) en of het nodig is te reguleren of bestaande normen te verhelderen?

Antwoord
Zie het antwoord op vraag 108.

110
Krijgt de NCTV extra middelen voor de coördinatie van het actieplan dat volgt uit de Nederlandse Cybersecurity Strategie? Zo ja, waar zijn die in de begroting te vinden? Zo nee, hoe zorgt u ervoor dat de NCTV deze verantwoordelijkheid desondanks zal kunnen dragen?

Antwoord
Nee, de NCTV krijgt geen extra middelen voor de coördinatie van het actieplan dat volgt uit de Nederlandse Cybersecuritystrategie. Het coördineren van cybersecuritymaatregelen is onderdeel van de vaste taken van de NCTV. Zo heeft de NCTV de afgelopen jaren de uitvoering van de Nederlandse Cybersecurity Agenda (NCSA) gecoördineerd, en zal zij de komende jaren de uitvoering van het actieplan volgend uit de nieuwe Nederlandse Cybersecuritystrategie coördineren.

111
Waaraan voldoet een toekomstbestendig cybersecuritystelsel, waar in te tekst naar verwezen wordt?

Antwoord
Men kan spreken van een toekomstbestendig cybersecuritystelsel wanneer alle organisaties in Nederland tijdig informatie over dreigingen en kwetsbaarheden ontvangen op een manier die past bij het volwassenheidsniveau van de organisatie. Om dit te realiseren moet de beschikbare capaciteit en expertise zo effectief mogelijk ingezet worden. Versnippering binnen het cybersecurityinformatiedelingsstelsel moet zoveel mogelijk worden tegengegaan om te zorgen voor heldere aanspreekpunten. Het Nationaal Cybersecurity Center, het Digital Trust Center en het Cyber Security Incident Response Team (CSIRT) voor digitale dienstverleners worden daarom samengevoegd tot één nationale CSIRT. Dit is de nationale cybersecurity autoriteit. Deze nieuwe organisatie zal in samenwerking met publiek en private partners, vitale en niet-vitale organisaties, overheden en burgers voorzien van beveiligingsinformatie en handelingsperspectief, passend bij hun volwassenheidsniveau.

Nieuwe (Europese) wetgeving vormt het kader waarbinnen het stelsel effectief en in samenhang kan opereren. Samen met publieke en private partners binnen dit Landelijk Dekkend Stelsel van cyber security samenwerkingsverbanden (LDS) zal worden beoordeeld welke taken (zoals beveiligingsinformatie verspreiden; bijstand verlenen; oefeningen organiseren etc.) centraal (bij de nationale cybersecurity autoriteit) of sectoraal belegd moeten worden. Het verhogen van de Nederlandse cyberweerbaarheid dient in publiek-privaat verband aangepakt te worden. Een belangrijk element hierin is gezamenlijk verzamelen en duiden van dreigingsinformatie. Daarom start het kabinet met uitwerken van publiek-privaat platform voor informatie-en kennisdeling.

112
Met welke ministeries werkt u samen om weerbaar te zijn tegen hybride dreigingen? Welke acties worden ondernomen om deze dreigingen het hoofd te bieden?

Antwoord
Om hybride dreigingen het hoofd te bieden wordt zoveel mogelijk een «whole of government» benadering gekozen. Statelijke actoren zetten steeds vaker een breed spectrum aan (machts)middelen in om hun politieke ambities te verwezenlijken. Hierbij kan gedacht worden aan cyberaanvallen, desinformatie campagnes of de inzet van economische middelen. Deze acties vinden vaak heimelijk of met dubbele agenda's plaats, en «traditionele» juridische, diplomatieke en militaire middelen bieden geen afdoende antwoord meer op deze hybride dreigingen. Momenteel wordt daarom gewerkt aan een strategisch raamwerk voor hybride weerbaarheid ten behoeve van een inlichtingen en informatie gestuurde aanpak, waarbinnen een breed scala aan instrumenten, binnen de bestaande wettelijke kaders, kan worden ingezet. U wordt voor het einde van het jaar schriftelijk nader geïnformeerd over dit raamwerk in de brief Aanpak statelijke dreigingen.

113
Op welke manier wordt de kennis van het Openbaar Ministerie rond cybercrime verbeterd? Wordt er hierbij samengewerkt met andere (overheids-)organisaties?

Antwoord
Vanuit het Openbaar Ministerie wordt in partnerschap met het Studiecentrum Rechtspleging (SSR) gewerkt aan de realisatie van een praktijkgericht leer- en opleidingsaanbod op het gebied van cybercrime. Hiertoe wordt onder meer samengewerkt met de Raad voor de Rechtspraak, de Politie, het Ministerie van Justitie en Veiligheid en andere ketenpartners binnen het Justitienetwerk. Verder werkt het Openbaar Ministerie aan het beter ontsluiten en delen van cybercrime-expertise binnen de eigen organisatie, met ketenpartners en in publiek-private samenwerkingsverbanden.

114
Op welke manier wordt voortgebouwd op initiatieven als het Cyber Info/Intel Cel?

Antwoord
In de Nederlandse Cybersecurity Agenda (NCSA) 2018 was de ambitie opgenomen om het landelijk situationeel beeld te versterken met de inrichting van een samenwerkingsplatform met het oogmerk om meer en sneller handelingsperspectief te kunnen delen.

De oprichting van de Cyber Info/Intel Cel was de eerste stap in de versterkte samenwerking. De volgende stap is het breder informatie-uitwisselen met zowel publieke als private organisaties.
Daartoe heeft er in de afgelopen maanden een verkenning plaatsgevonden om gezamenlijk sneller en gerichter informatie te delen rondom (dreigende) cyberincidenten in publiek-privaatverband.
Deze verkenning heeft geresulteerd in een rapport met aanbevelingen. Hierin wordt geadviseerd om een publiek-privaat samenwerkingsplatform op te richten, waar breder informatie wordt gedeeld, geanalyseerd en gedistribueerd.
Bij de publicatie van de Nederlandse Cyber Security Strategie is uw Kamer over de resultaten van de verkenning geïnformeerd.

115
Kunt u toelichten waarvoor Helios wordt gebruikt, en daarbij specifiek ingaan op het type criminaliteitsfenomenen waarvoor Helios wordt ingezet?

Antwoord
Het doel van Helios is om bij te dragen aan het binnen de politie creëren van één intelligencepositie op thema's. Vanuit deze centrale intelligencepositie worden, met behulp van gevalideerde datamodellen, inzichten gegenereerd die het politiewerk op strategisch, tactisch en operationeel niveau ondersteunen. Denk hierbij aan inzicht in ontwikkelingen op de cocaïnemarkt en de invloed die dit heeft op criminele samenwerkingsverbanden die zich op die markt begeven. Aan de hand van zulke beelden kan ingeschat worden welke interventies binnen die netwerken het meest effectief kunnen zijn. Met Helios kunnen politiemensen extra geduide informatie toevoegen aan reeds bestaande informatie zodat beelden sneller gegenereerd kunnen worden.
Helios wordt dan ook ingezet om inzicht te krijgen in geprioriteerde veiligheidsthema's. Deze komen voort uit de Landelijke Veiligheidsagenda en worden bepaald en bijgesteld door de politie in samenspraak met het bevoegd gezag.

116
Kunt u toelichten of Helios gebruikt maakt van kunstmatige intelligentie (AI)/algoritmen, big data en/of (semi-)geautomatiseerde risicoprofielen?

Antwoord
Voor de toepassing van Helios wordt gebruik gemaakt van gegevens die zich al in de informatiesystemen van de politie bevinden en waarvan het mogelijk is om deze voor het doel van het verkrijgen van inzichten verder te verwerken. Daartoe kwalificeren verscheidene categorieën gegevens. Er is geen uniforme opvatting over de drempelwaarde wanneer er sprake is van «big data», maar het ligt voor de hand om in het geval van Helios te spreken over een «big data» toepassing. De toepassing van algoritmen hierbij bevindt zich momenteel in een voorbereidende fase. Op dit moment is er nog geen sprake van de operationele inzet van zelflerende systemen, algoritmes of (semi-) geautomatiseerde risico-profielen. Het Wetboek van strafvordering en de Wet politiegegevens, alsook het geldende normenkader, bepalen de mogelijkheden voor het verder verwerken van gegevens binnen de politie.

117
Hoeveel capaciteit gaat er naar het ontwikkelen (inclusief toetsen) van Helios?

Antwoord
Het programma Helios wordt uitgevoerd in opdracht van de portefeuille intelligence. Helios is een programma dat bestaat uit ICT-specialisten, data-specialisten en experts uit de intelligence-organisatie van de politie. De samenstelling van de betrokken experts varieert gedurende de ontwikkeling. Zodoende is het capaciteitsbeslag van het ontwikkelen en toetsen van Helios niet eenduidig aan te geven.

118
Is Helios door de politie aangekocht of zelf ontwikkeld, of een combinatie daarvan?

Antwoord
Helios is geen enkelvoudige ICT-toepassing maar een applicatie waarin primair geregistreerde broninformatie verrijkt kan worden. Helios maakt voor wat betreft de softwareontwikkeling gebruik van een mix van producten die binnen de politie aanwezig zijn, producten die worden aangekocht en door de politie zelf ontwikkelde componenten. De ontwikkeling van de data-toepassingen en algoritmes geschiedt door data scientists die binnen de politie werkzaam zijn.

119
Kunt u een overzicht geven van AI-toepassingen die worden ingezet ten behoeve van proactief politiewerk?

Antwoord
De definitie van Artificial Intelligence is diffuus en niet altijd even eenduidig. Om die reden spreken we hier over de toepassing van machine learning technieken. Het meest bekende voorbeeld daarvan is het Criminaliteits Anticipatie Systeem. Het CAS is een voorbeeld van een hotspot-benadering waarbij op basis van bestaande data wordt bepaald waar het waarschijnlijk is dat bepaalde vormen van verstoring van de openbare orde of criminaliteit voorkomen. Gebruik van het CAS levert een verwachting voor een bepaald gebied op en geeft geen output die tot personen te herleiden is. De data die wordt gebruikt betreft o.a. criminaliteitshistorie, die hoofdzakelijk is gebaseerd op aangiftes van burgers, oftewel informatie die naar de politie toe komt en niet door haar eigen optreden bepaald wordt. Hiermee wordt een versterking van eventuele eigen vooringenomenheid door het algoritme beperkt. Het CAS wordt gebruikt ter voorkoming van verschillende veelvoorkomende delicten zoals woninginbraak, vernieling en drugshandel. De aanwezigheid van de politie op plekken waar een verhoogde kans is op deze en andere soorten delicten kan bijdragen aan de voorkoming ervan.

120
Kunt u een overzicht geven van AI-toepassingen die worden ingezet ten behoeve van intelligence/proactief politiewerk in het kader van het informatieknooppunt Contraterrorisme, Extremisme en Radicalisering van de Landelijk Eenheid van de politie (CTER)?

Antwoord
Op dit moment wordt geen machine learning ingezet in het kader van de aanpak van CTER.

121
Kunt u een overzicht geven van AI-toepassingen die worden ingezet ten behoeve van open source intelligence (OSINT)?

Antwoord
De NCTV gebruikt geen AI-toepassingen die worden ingezet ten behoeve van open source intelligence. De politie maakt hier (ook) geen gebruik van.

122
Kunt u een overzicht geven van de AI-toepassingen die worden ingezet ten behoeve van sociale-media-monitoring?

Antwoord
Raadplegen van openbare informatie op sociale media gebeurt binnen wettelijke kaders en daarbij vindt geen verwerking van persoonsgegevens plaats. De politie maakt hierbij geen gebruik van AI-toepassingen.

123
Hoeveel capaciteit gaat er naar het ontwikkelen van AI-toepassingen voor intelligence?

Antwoord
Voor de politie is het lastig om precies te duiden hoeveel capaciteit aan het ontwikkelen van AI-toepassingen voor intelligence wordt toegekend, omdat de politiemedewerkers die hieraan werken ook andere technologie en werkprocessen ontwikkelen. Intelligence-werkzaamheden zijn immers ook verweven met opsporing. In algemene zin houden de medewerkers die worden toegerekend aan het Nationaal Politielab AI zich bezig met onderzoek en conceptontwikkeling rondom AI, verder vindt er in de operatie ook ontwikkeling van toepassingen plaats. Op dit moment zijn er ca. 30 fte werkzaam bij het Nationaal Politielab AI, onder wie ca. 15 promovendi van verschillende universiteiten.

124
Hoeveel teams zijn er binnen de politie die zich bezighouden met het zelf ontwikkelen van en/of doorontwikkelen van ingekochte AI-toepassingen voor intelligence?

Antwoord
Binnen verschillende onderdelen van de politie wordt, onder andere door data scientists gewerkt aan de (door)ontwikkeling van algoritmes. Het Nationaal Politielab AI houdt zich specifiek bezig met het al dan niet in concept ontwikkelen van AI-toepassingen. Daarnaast wordt in de operatie aan de ontwikkeling van technologie en ICT, waaronder AI, gewerkt. Deze werkzaamheden zijn niet in specifieke teams belegd, AI maakt als gevestigde technologie onderdeel uit van het brede palet aan datascience werkzaamheden en statistische technieken.

125
Kunt u een overzicht geven van de aanbestedingen voor AI-toepassingen en software?

Antwoord
Nee, dit overzicht is niet leverbaar. Over de aanbesteding voor AI-toepassingen en software wordt niet op een wijze geregistreerd waardoor op concernniveau een rapportage te generen is.

126
Hoeveel capaciteit gaat er naar het ontwikkelen en implementeren van het Kwaliteitskader Big Data?

Antwoord
Politie en het openbaar ministerie (OM) werken samen in een projectteam dat het verder ontwikkelen en implementeren van het Kwaliteitskader Big Data in beide organisaties begeleidt. Daarnaast is er in elke politie-eenheid en elk arrondissement een verantwoordelijke «driehoek» van medewerkers die samenwerken. Landelijk vormen zij een netwerk in de vorm van een klankbordgroep die regelmatig met elkaar afstemt. Een stuurgroep van politie en OM overziet dit proces. De verdere implementatie en uitvoering zijn aan de eenheden, resp. arrondissementen.

127
Kunt u toelichten in hoeverre de ontwikkeling van een vernieuwd integraal wettelijk kader voor crisisbeheersing en brandweerzorg ook betrekking heeft op digitale crises?

Antwoord
Het kabinet werkt aan de verdere beleids- en wetsontwikkeling voor één goed functionerend landelijk dekkend stelsel van crisisbeheersing om een grote verscheidenheid aan typen incidenten en crises te kunnen beheersen. Een stelsel dat leunt op een basis van lokaal en regionaal georganiseerde incident- en crisisbeheersing in een structurele samenwerking met crisis-specifieke, functionele en nationale partners. Dit stelsel heeft ook betrekking op digitale crises.

128
Kunt u een overzicht geven van de technologische tools/software die worden gebruikt voor proactief politiewerk en uitsplitsen naar technologie die wordt aangekocht, zelf ontwikkeld of een combinatie hiervan is?

Antwoord
Terughoudendheid over precieze informatie welke technologische tools/software de politie in gebruik heeft, is omwille van de handhavings- en opsporingsaken van de politie aangewezen. Als vuistregel geldt dat de politie zelf software ontwikkelt die (nog) niet als een courant product vanuit de markt wordt aangeboden of wanneer met de levering van het systeem de leverancier ongewenst inzage in operationele politiedata kan krijgen. De politie ontwikkelt samen (cosourcing) met leveranciers wanneer de politie de noodzakelijke knowhow (nog) niet afdoende zelfstandig in huis heeft. Vanuit de markt wordt aangekocht wanneer het product courant is en als de politie de toegang tot operationele politiedata afdoende kan afschermen voor de leverancier.
Het meest bekende hulpmiddel dat de politie gebruikt voor proactief politiewerk is het Criminaliteits Anticipatie Systeem, welke binnen de politie is ontwikkeld. Zie verder bij vraag 119. De politie maakt gebruikt van eigen ontwikkelplatforms, waaronder een zelf gebouwd Advanced Analytics Platform, gebaseerd op open source cloud technologie.

129
Kunt u aangeven bij welke bedrijven de politie technologische tools/software inkoopt?

Antwoord
Nagenoeg alle software koopt de politie in bij software resellers. De politie is deelnemer in de rijksbrede mantelovereenkomst voor software, EASP2019. Een klein aantal applicaties is onder afscherming gekocht. Terughoudendheid over precieze informatie welke technologische tools/software de politie in gebruik heeft, is omwille van de handhavings- en opsporingsaken van de politie aangewezen. Mede met het oog op risico's cyberaanvallen (ransomware) gericht op de leverancier.

130
Kunt u een overzicht geven van de landen waaruit de bedrijven afkomstig zijn waar de politie technologische tools/software inkoopt?

Antwoord
Nee, dit overzicht is niet leverbaar, want de herkomst van tools en software wordt niet op die manier geregistreerd.

131
Kunt u aangeven hoe de politie bij de aankoop van technologie van bedrijven rekening houdt met de mensenrechtensituatie in het land waar het bedrijf gevestigd is?

Antwoord
De politie hanteert de dwingende uitsluitingsgronden voor partijen (ondernemers) zoals die in de Aanbestedingswet 2012 zijn opgenomen. Daar zit een check in of een partij onherroepelijk is veroordeeld voor criminele geldstromen, witwassen maar ook op kinderarbeid en mensenrechten.

Sinds 2020 heeft de politie aanvullende bepalingen opgenomen die kunnen gelden als uitsluitingsgrond: Dit is de bepaling dat partijen die niet handelen in lijn met verdragen waar Nederland aan deelneemt, uitgesloten kunnen worden, en de bepaling dat partijen die risico's met zich meebrengen op het gebied van spionage uitgesloten kunnen worden. De focus is gericht op de wijze waarop de partij (ondernemer) invulling geeft aan de naleving van de mensenrechten.

132
Kunt u een overzicht geven van de technologie die wordt gebruikt voor het slim koppelen van systemen en uitsplitsen naar tools/software die zijn aangekocht, zelf ontwikkeld of een combinatie is hiervan?

Antwoord
Zoals geschetst in de beantwoording op vraag 128 past terughoudendheid over precieze informatie welke technologische tools/software de politie in gebruik heeft, omwille van de handhavings- en opsporingsaken van de politie.

Als vuistregel geldt dat de politie zelf software ontwikkelt die (nog) niet als een courant product vanuit de markt wordt aangeboden of wanneer met de levering van het systeem de leverancier ongewenst inzage in operationele politiedata kan krijgen. De politie ontwikkelt samen (cosourcing) met leveranciers wanneer de politie de noodzakelijke knowhow (nog) niet afdoende zelfstandig in huis heeft. Vanuit de markt wordt aangekocht wanneer het product courant is en als de politie de toegang tot operationele politiedata afdoende kan afschermen voor de leverancier.

133
Kunt u inzicht geven in hoe het Kwaliteitskader Big Data is aangepast ten opzichte van versie 1.0 die in 2020 met de Tweede Kamer is gedeeld?

Antwoord
Het Kwaliteitskader Big Data is een levend document, maar is zelf thans niet aangepast. Toekomstige ontwikkelingen zoals bijvoorbeeld nieuwe of aangepaste wetgeving kunnen leiden tot aanpassing van het kader. Er is een extra toelichting voor het gebruik van het kader verschenen. Er loopt binnen de politie al enige tijd een traject om het Kwaliteitskader Big Data te integreren in de tool die gebruikt wordt voor het maken van een gegevenseffectbeoordeling (GEB), dit omdat er een overlap zit in de te

beantwoorden vragen. Het doel van deze integratie is mede om het doorlopen van het Kwaliteitskader Big Data gebruiksvriendelijker te maken. Parallel speelt al enige tijd de discussie om voor de hele overheid specifieke instrumenten en kaders te ontwikkelen. Toezichthouders hebben ook eigen instrumenten ontwikkeld. Het is op dit moment nog onduidelijk wat dit voor het gebruik van het Kwaliteitskader Big Data betekent. Zie ook het antwoord op vraag 135.

134
Kunt u inzicht geven in hoe het Kwaliteitskader Big Data in de praktijk wordt gebruikt?

Antwoord
Bij de ontwikkeling van algoritmes en modellen in de eenheden zijn deze zelf verantwoordelijk voor het gebruik van het Kwaliteitskader Big Data en het vastleggen van de uitkomsten. Dit gebeurt nu nog handmatig. Zoals hiervoor vermeld wordt gewerkt aan een integratie met een geautomatiseerd hulpmiddel, dat de politie ook voor de GEB toepast. Politie en OM werken in elke eenheid en (het gekoppelde) arrondissement samen in het construct zoals beschreven bij vraag 126. Landelijk is er een afstemming over resultaten in een klankbordgroep. Het Kwaliteitskader Big Data is specifiek van toepassing op het gebruik van (big) data en algoritmes en modellen ten behoeve van de opsporing maar het kan in principe ook voor andere toepassingen worden gebruikt.

135
Kunt u inzicht geven in hoe het Kwaliteitskader Big Data zich verhoudt tot de Impact Assessment Mensenrechten en Algoritmes (IAMA)?

Antwoord
Het Kwaliteitskader Big Data is een door de politie en het OM in 2019 ontwikkelde methodologie om te helpen de juiste (zowel juridische als data-wetenschappelijke) vragen te stellen voor projecten die gebruik maken van verschillende vormen van data en waar als resultaat algoritmen en modellen uitkomen. De politie en het OM nemen, na de beantwoording van de vragen in het kwaliteitskader en het geschetste plan van aanpak van het project, gezamenlijk een standpunt in over het gebruik en de inzetbaarheid van de technologie en de daaruit voortvloeiende informatie. Per fase wordt in het Kader geduid welke publieke waarden moeten worden beschermd. Hierbij is gebruik gemaakt van het Rapport van het Rathenau Instituut «Opwaarderen: Borgen van publieke waarden in de digitale samenleving.» Het is nog de vraag in het licht van de Verzamelbrief publieke controle op algoritme (Kamerstuk 26 643, nr. 924) op welke wijze het IAMA, het Kwaliteitskader Big Data en andere toetsingskaders zich tot elkaar verhouden. De vraag of gekozen wordt voor één universeel toetsingskader zal blijkens die brief verder worden uitgewerkt in samenwerking met verschillende organisaties, waaronder de politie.

136
Hoeveel beslisalgoritmes ten behoeve van proactief politiewerk zijn er momenteel actief?

Antwoord
De politie maakt geen gebruik van beslisalgoritmes die zonder menselijke tussenkomst leiden tot het nemen van een besluit.

137
Hoeveel profileringsalgoritmes/geautomatiseerde risicoprofielen zijn momenteel actief?

138
Hoeveel capaciteit gaat er naar het ontwikkelen van profileringsalgoritmes?

139
Hoeveel capaciteit gaat er naar het toetsen van profileringsalgoritmes aan ethische en mensenrechtenkaders?

140
Welk deel van de profileringsalgoritmes is ingekocht bij bedrijven of onderzoeksinstellingen of andere externe partijen?

141
Hoeveel geld wordt er besteed aan het inkopen van profileringsalgoritmen?

Antwoord
Voor de vragen 137 t/m 141 is een overzicht niet leverbaar, dit wordt niet geregistreerd op een manier waardoor hierover op concernniveau een rapportage te genereren is.

142
Hoeveel capaciteit gaat er naar OSINT?

Antwoord
JenV gebruikt, net als ieder ander onderdeel van de Rijksoverheid, open bronnen (OSINT) zoals kranten en wetenschappelijke publicaties voor haar werkzaamheden. Dit is onderdeel van de reguliere activiteiten van de medewerkers. Raadplegen van openbare informatie gebeurt binnen wettelijke kaders en daarbij vindt geen verwerking van persoonsgegevens plaats.

Het NCSC heeft als wettelijke taak om onderzoek te doen naar dreigingen, incidenten en kwetsbaarheden in relatie tot vitale aanbieders en Rijksoverheidsorganisaties. Daarbij maakt het NCSC ook gebruik van open bronnen. Dit maakt integraal onderdeel uit van de werkzaamheden die het NCSC uitvoert in het kader van zijn wettelijke taken, daarom is het niet mogelijk om specifiek aan te geven hoeveel capaciteit hiervoor wordt aangewend.

Het OSINT werk vormt een integraal onderdeel van de werkzaamheden van de politie. Het is niet mogelijk om specifiek aan te geven hoeveel capaciteit hiervoor wordt aangewend.

143
Hoeveel capaciteit gaat er naar social-media-monitoring?

Antwoord
Raadplegen van openbare informatie op sociale media gebeurt binnen wettelijke kaders en daarbij vindt geen verwerking van persoonsgegevens plaats. Voor de politie vormt het op specifieke thema's raadplegen van social media een integraal onderdeel van de OSINT-werkzaamheden. Zie tevens de beantwoording op vraag 142.

144
Welke investeringen worden in 2023–2027 gedaan in OSINT?

Antwoord
Afhankelijk van afhandeling van het wetsvoorstel wettelijke grondslag voor verwerking persoonsgegevens NCTV zal, mogelijk binnen de daartoe

gestelde kaders, worden voorzien in handmatige (niet-geautomatiseerde) toegang tot social-media. Op deze investeringen is bij de politie geen specifiek zicht.

145
Kunt u aangeven welke tools/software wordt gebruikt voor OSINT en uitsplitsen naar tools/software die door de politie zijn aangekocht, zelf ontwikkeld of een combinatie hiervan is?

Antwoord
Zie het antwoord op vraag 128.

146
Hoeveel capaciteit gaat er naar het ontwikkelen (inclusief testen) van tools/software voor geautomatiseerde OSINT?

Antwoord
De NCTV heeft geen capaciteit ingezet voor het ontwikkelen of testen van tools/software voor geautomatiseerde OSINT. Er is bij de politie geen specifieke capaciteit toegewezen aan dergelijke ontwikkelingen.

147
Hoeveel geld wordt er besteed aan het aankopen van tools/software voor (semi-) geautomatiseerde OSINT en kunt u dit uitsplitsen naar tool/software?

Antwoord
Het is onduidelijk wat wordt bedoeld met geautomatiseerde OSINT. Zie verder het antwoord op vraag 148.

148
Hoeveel capaciteit gaat er naar het toetsen van tools/software voor ((semi-)geautomatiseerde) OSINT aan ethische en mensenrechtenkaders?

Antwoord
Zoals aangegeven bij de beantwoording van vraag 147 is het niet duidelijk wat er wordt bedoeld met (semi)geautomatiseerde OSINT. De politie besteedt aandacht aan en investeert in de toetsing van tools en software binnen de daarvoor geldende kaders, maar in algemene zin is het lastig om precies te duiden om hoeveel capaciteit het hierbij gaat. Zie voorts de antwoorden op de vragen 126 en 135.

149
Hoeveel capaciteit gaat er naar het programma Sensing?

Antwoord
Sensing is een breed begrip. Om deze en de volgende vragen goed te kunnen beantwoorden is het belangrijk om enkele definities te geven. Bij sensing gaat het om het waarnemen en verzamelen van gegevens met behulp van een sensor. Sensoren zijn in de kern een verlenging van de menselijke zintuigen. ANPR-camera's, bodycams en gemeentelijk cameratoezicht zijn voorbeelden van sensing.
Het programma Sensing heeft begin 2022 haar opdracht afgerond. Het programma heeft gewerkt aan versterking van de politieorganisatie in het gebruik van sensing-toepassingen. De doorontwikkeling is overgedragen aan de lijnorganisatie.

150
Welke investeringen worden in 2023–2027 gedaan in Sensing?

Antwoord
Dat is niet in detail aan te geven. In de politiebegroting is geen aparte post opgenomen voor sensingtoepassingen. Investeringen in de verschillende vormen van sensingtoepassingen worden bekostigd vanuit verschillende onderdelen van de politieorganisatie. Het budget voor ANPR-camera's is gecentraliseerd naar de Landelijke Eenheid, ten behoeve van de hele nationale politie. De eenheden financieren tijdelijke inzetten ten behoeve van lokale problematiek.
Vanuit de ondermijningsgelden zal naar verwachting een deel ten goede komen aan de doorontwikkeling van het sensingplatform en het ondersteunen van de eenheden in het goed toepassen van sensing. Definitieve besluitvorming hierover moet nog plaatsvinden.

151
Hoeveel projecten met sensing-toepassingen zijn momenteel actief en hoeveel zijn er gepland?

Antwoord
Voor de beantwoording van deze vraag wordt de term project geïnterpreteerd als een activiteit waarbij sensingtoepassingen worden ontwikkeld en niet als een activiteit (zoals een opsporingsproject) waar sensingtoepassingen worden gebruikt.
In dit kader zijn er meerdere projecten, waarvan een belangrijke de bouw van een sensingplatform is, waarop in eerste instantie alle ANPR-data (art. 3 PW) wordt verwerkt. Dit platform vervangt twee andere applicaties en heeft als doel om ook andere sensoren te gaan ontsluiten. Een voorbeeld van een ander lopend project zijn de aanpassingen naar aanleiding van het WODC- en auditrapport over artikel 126jj Sv.

152
Hoeveel experimenten/proeftuinen met sensing-toepassingen zijn momenteel actief en hoeveel zijn er gepland?

Antwoord
Bij de publicatie van het Eerste Halfjaarbericht 2022 gaf de politie aan dat zij op dat moment geen proeftuinen had lopen op het gebied van sensingtechnologie. Op dit moment is er wel een proeftuin in de opstartfase. Het betreft het zogenoemde Flexibel Reactieconcept (FRC), waarover ik uw Kamer eerder heb geïnformeerd. De politie start een proeftuin als zij nieuwe sensortechnologieën wil testen in een praktijksituatie. De ontwikkelingen die plaatsvinden vanuit van het FRC kunnen gezien worden als proeftuinen. Binnen dit concept worden meerdere ontwikkelingen samengebracht om gezamenlijk zaken te kunnen uitproberen en meer aan de voorkant van het identificeren van mogelijke verstoringen te komen. Onder andere door verschillende soorten gegevens/informatie aan elkaar te koppelen. Hierbij is sensing een middel en geen doel.

153
Welke sensing-toepassingen vinden plaats ten behoeve van proactief politiewerk?

Antwoord
De politie maakt geen gebruik van sensing-toepassingen specifiek voor proactief politiewerk. Wel gebruikt de politie verschillende andere toepassingen ten behoeve van proactief politiewerk. Voorbeelden daarvan zijn CAS en de i-trechter. Deze toepassingen putten data uit bestaande databronnen en maken geen gebruik van sensoren.

154
Kunt u een overzicht geven van sensing-toepassingen die momenteel worden ingezet voor risicoprofilering, intelligence en/of proactief politiewerk en dit overzicht uitsplitsen naar toepassingen die door de politie zijn aangekocht, zelf ontwikkeld of een combinatie hiervan zijn?

Antwoord
Nee. Zoals ik in mijn antwoord op vraag 149 aangaf is sensing een breed begrip. De politie maakt bijvoorbeeld gebruik van sensoren zoals ANPR-camera's, bodycams, en drones die zijn uitgerust met een sensor zoals een camera. Sensing-toepassingen worden op de markt gekocht en ook door de politie zelf ontwikkeld.

155
Hoeveel capaciteit gaat er naar het ontwikkelen (inclusief testen) van sensingtechnologie?

Antwoord
In principe wordt zoveel als mogelijk aangesloten bij ontwikkelingen in de markt en bij kennisinstellingen. Daarnaast heeft de politie kennis in huis om zelf sensoren te ontwikkelen. De capaciteit die nodig is voor het ontwikkelen (inclusief testen) hiervan is afhankelijk van de toepassing en afkomstig van verschillende onderdelen van de politieorganisatie. Een overzicht hiervan is niet beschikbaar.

156
Hoeveel geld wordt er besteed aan het aankopen van sensingtechnologie?

Antwoord
Voor de beantwoording van deze vraag verwijs ik u naar het antwoord op vraag 150.

157
Kunt u aangeven welk deel van de aangekochte technologie voor OSINT, sensing en andere ai- en big data-technologie is ingekocht bij Chinese bedrijven?

Antwoord
De NCTV heeft geen inzicht in wie welke apparatuur uit China gebruikt. Risico's bij het inkopen van producten en diensten worden altijd case by case bezien. Het proces is echter altijd hetzelfde: er wordt gekeken welke nationale veiligheidsbelangen kunnen worden geraakt bij een aanbesteding, welke dreiging we daartegen zien en welke maatregelen nodig zijn om de risico's af te vangen. Er wordt altijd gekeken of er maatregelen mogelijk zijn die veilig gebruik mogelijk maken. Het kabinet heeft een instrumentarium ontwikkeld en uitgerold binnen het Rijk en de vitale infrastructuur voor veilige inkoop en aanbesteding, waarin deze werkwijze wordt gevolgd. Daarnaast zijn er ook, in het kader van de NCSA, cybersecurity inkoopeisen voor de overheid (ICO-wizard) ontwikkeld: hiermee worden cybersecurity-eisen geselecteerd die passen bij de producten/diensten die organisaties aanbesteden. Het kabinet gaat daarnaast de mogelijkheid van het neerleggen van nationale veiligheidsrichtlijnen voor het gebruik van producten en diensten binnen de Rijksoverheid, vitale infrastructuur en medeoverheden verkennen.

Het NCSC doet in beginsel geen uitspraken over leveranciers van hard- en software. Bij de aanschaf van hard- en software voert het NCSC altijd een zorgvuldige risicoanalyse uit op basis waarvan besloten wordt of het bepaalde producten zal toepassen.

De politie doet (ook) in beginsel geen uitspraken over leveranciers van hard- en software. Inzake dergelijke aanschaf voert de politie ook standaard een zorgvuldige, voorafgaande risicoanalyse uit op basis waarvan besloten wordt of de politie een product toepast. Zie ook vraag 131

158
Hoeveel geld komt er bij voor de AP? Hoeveel extra geld is er bij de AP gekomen naast de CA-gelden?

Antwoord
Naast de gelden die voortvloeien uit het coalitieakkoord, die in 2023 4 miljoen en 1 miljoen euro bedragen, komt er extra voor de AP in 2023 vanuit de Werk aan Uitvoering (WaU)-middelen structureel 2.6 miljoen euro bij.

159
Kunt u in een tabel de ontwikkeling van het aantal fte's bij de AP schetsen, afgezet tegen het aantal gevoerde onderzoeken?

Antwoord
Op basis van de AP jaarverslagen van 2018 tot en met 2021 is het volgende beeld te schetsen:

Jaar	Aantal FTE's	Onderzoeken
2018	157,1	16
2019	174,0	87
2020	184,0	68
2021	172,2	29

Onder de term onderzoeken rekent de AP nationale onderzoeken, internationale onderzoeken, verkennende onderzoeken, sectorbeelden en Europese onderzoeken op het gebied van politie, justitie en grensbewaking.
Het aantal gestarte onderzoeken is in 2019 toegenomen. Sinds de inwerkingtreding van de AVG in 2018 heeft de AP nadrukkelijk ruimte gegeven aan organisaties om de nieuwe regels goed te implementeren. In 2019 heeft de AP meer nadruk gelegd op onderzoek en handhaving, waardoor er meer onderzoeken konden worden gestart.
Ten opzichte van 2020 laat 2021 een daling zien in het totale aantal onderzoeken. Het jaarverslag van 2021 licht dit als volgt toe: «De daling van het aantal onderzoeken ten opzichte van 2020 is vooral ingegeven doordat de AP in 2021 bewust minder capaciteit heeft ingezet op het opstarten en afronden van onderzoek, teneinde de achterstanden bij de afdeling Handhaven op te kunnen lossen.»

160
Hoeveel van de AP begroting gaat naar preventie? Hoeveel naar onderzoek?

Antwoord
De AP streeft ernaar om gelijk in te zetten op preventief (voorlichting etc.) en repressief toezicht (onderzoeken, handhaving etc). Dit betekent dat de AP 50% van haar capaciteit en middelen beoogt te besteden aan beide vormen van toezicht.

161
Is het toebedeelde budget voor de algoritmetoezichthouder voldoende om ervoor te zorgen dat (alle overheids)algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur?

Antwoord
In het regeerakkoord staan ambities over de inzet van algoritmes en de rol van de AP als «algoritmewaakhond». De AP ontvangt voor deze opdracht vanaf 2023 1 miljoen euro oplopend naar structureel 3,6 miljoen euro in 2026. Met behulp van een algoritmetoezichthouder onder de AP werkt dit kabinet om het toezicht verder te verankeren, om hiermee ook het vertrouwen te vergroten. Het sectorale toezicht blijft daarnaast ook in stand. Het kabinet verduidelijkt dit in de brief «Publieke controle op algoritmen» (Kamerstuk 26 643, nr. 924). De AP zal daar periodiek over rapporteren aan de Staatssecretaris Koninkrijksrelaties en Digitalisering. Het vorige kabinet heeft daarnaast eerder geconcludeerd dat algoritmen niet in een juridisch vacuüm vallen. Het huidig (algemene) wettelijk kader bestaat uit onder meer mensenrechtenverdragen, de Grondwet, de Algemene wet bestuursrecht (Awb), het Burgerlijk Wetboek (BW), gelijke behandelingswetgeving, en de AVG.

162
Wat is de betrokkenheid van de digitale toezichthouders, waaronder de AP, bij de uitwerking en vormgeving van het toezicht op de nieuwe Europese regelgeving zoals de AI-Act, Data Governance Act (DGA), Digital Markets Act (DMA), eIDAS-verordening en Digital Services Act (DSA)?

Antwoord
De AP volgt de uitwerking en vormgeving van de nieuwe regelgeving op de voet, zowel nationaal – waaronder binnen het Samenwerkingsplatform Digitale Toezichthouders (SDT) – als Europees. Geregeld deelt de AP ook haar standpunten met de Tweede Kamer of – via de EDPB – met het Europees Parlement en de Europese Commissie. Zie verder het antwoord op vraag 184.

163
Hoe verhoudt de snelheid van de digitale transitie zich tot de (achterlopende) budgetten van de digitale toezichthouders, waaronder de AP?

Antwoord
Zie het antwoord op de vraag 182.

164
In hoeverre reflecteren de verschillende taken die de AP, vanuit meerdere beleidsgebieden uitvoert, in de verschillende begrotingen?

Antwoord
De AP is een onafhankelijke toezichthouder die wordt gefinancierd via de begroting van het Ministerie van Justitie en Veiligheid. De financiering van de verschillende taken die de AP, vanuit meerdere beleidsgebieden uitvoert, komt samen in één begrotingsartikel in de begrotingsstaten van dit ministerie.

165
Kunt u uiteenzetten hoeveel geld en fte beschikbaar zijn voor de verschillende taken van de AP en hoe zich dat in de toekomst ontwikkelt?

Antwoord
Het budget van de AP ontwikkelt zich de komende jaren als volgt in mln.:

2022	2023	2024	2025	2026	2027
€ 29,020	34,478	37,829	40,694	41,429	41,294

De AP verwacht dat het aantal fte op basis van bovenstaande cijfers in 2023 zal groeien naar circa 235. Per begrotingsjaar zal worden aangegeven met hoeveel.

166
Waarom wordt het toezicht op algoritmes ondergebracht bij de AP?

Antwoord
In het coalitieakkoord staat vermeld dat er een algoritmetoezichthouder komt die regelt dat algoritmen gecontroleerd worden op transparantie, discriminatie en willekeur. In de budgettaire bijlage staan hiervoor vanaf 2023 middelen toegewezen aan de Autoriteit Persoonsgegevens (hierna: AP). De AP is een onafhankelijke toezichthouder die zich – conform de Algemene verordening gegevensbescherming (AVG) – richt op het toezicht houden op de bescherming van persoonsgegevens. Een groot deel van de algoritmen die een risico met zich meebrengen wat betreft impact op grondrechten en fundamentele vrijheden (zoals non-discriminatie) bevat persoonsgegevens. Voor algoritmen die geen persoonsgegevens bevatten is een goede samenwerking met alle betrokken toezichthouders van groot belang. Het bestaande toezicht blijft daarbij intact.

167
Kunt u aangeven wanneer de algoritmetoezichthouder start met haar werkzaamheden en wanneer het wettelijk kader hiervoor naar de Kamer wordt gestuurd? Hoe groot wordt het budget per jaar voor de komende vier jaar?

Antwoord
BZK is gestart met het opstellen van scenario's voor de inrichting van de algoritmetoezichthouder. De komende periode worden verschillende expertsessies georganiseerd waarbij een breed scala aan experts om input wordt gevraagd. Dit zal worden gebruikt om samen met andere bewindspersonen tot besluitvorming te komen.
Op die manier kan de algoritmetoezichthouder begin 2023 al van start met taken waarvoor de bevoegdheden niet wettelijk hoeven te worden geregeld. De inrichtingsnotitie die hiervoor nodig is zal met de Kamer worden gedeeld. Voor (eventuele) taken en bevoegdheden die een nieuwe wettelijke grondslag vereisen is meer tijd nodig, omdat daarvoor wetgeving nodig is. In de budgettaire bijlage van het coalitieakkoord staan concreet vanaf 2023 middelen toegewezen aan de AP voor de rol van algoritmetoezichthouder. Het gaat het om:
- € 1 miljoen per 2023,
- € 3 miljoen per 2024,
- € 3,6 miljoen per 2025
- Structureel € 3,6 miljoen vanaf 2026.

168
Kunt u toelichten wanneer de algoritmetoezichthouder wordt opgericht en start met haar werkzaamheden?

Antwoord
Zie het antwoord op de vraag 167.

169
In hoeverre beschikt de algoritmetoezichthouder over eigen middelen en capaciteit en hoe groot is het budget per jaar voor de komende vier jaar?

Antwoord
Zie het antwoord op de vraag 167.

170
Hoeveel capaciteit gaat er naar het in lijn brengen van basispolitiesystemen (BVH, BVI, etc.) met de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg)?

Antwoord
Het is lastig om precies te duiden hoeveel capaciteit aan het in lijn brengen van basispolitiesystemen met de AVG en de Wpg wordt toegekend, omdat deze werkzaamheden onderdeel uitmaken van de (door)ontwikkeling van deze politiesystemen. Dit specifieke werk maakt namelijk onderdeel uit van het geheel van verbeteractiviteiten op het gebied van AVG en Wpg. Er is onlangs extra geïnvesteerd in hiervoor benodigde specifieke expertise. Werkzaamheden die bijdragen aan privacy by design en het voldoen aan AVG en Wpg worden geprioriteerd binnen het geheel van werkzaamheden, die bijvoorbeeld ook bijdragen aan functionele verbetering. Daarbij is er een continue afweging tussen tijdsinvestering in de nieuwe (toekomstbestendige) systemen en tijdsinvestering in de systemen waarvan het einde van de levensduur nabij is

171
Kunt u aangeven in welk jaar de basispolitiesystemen in lijn zullen zijn met de privacyregelgeving zoals neergelegd in de AVG en de Wpg?

Antwoord
Uw Kamer is eerder op verschillende momenten geïnformeerd over de planmatige aanpak ter verbetering van 36 politiesystemen, waaronder de basispolitiesystemen (Kamerstuk 29 628, nummer 944, vraag 4 van D66 en 11 van Groen Links, en Kamerstuk 35 925 VI, nummer 30, vraagnummer 15). Deze aanpak is nog gaande. Er is geen jaartal te noemen waarin de basispolitiesystemen in lijn met de AVG en Wpg zijn. Dit vergt een grote inspanning en hangt mede af van de voortgang van de vervanging van bestaande systemen. Het Programma Vernieuwend Registreren, dat 13 basispolitiesystemen vervangt, kent een doorlooptijd tot 2028. Tot die tijd worden waar mogelijk technisch en organisatorische maatregelen getroffen om de risico's voor betrokkenen te mitigeren.

172
Hoeveel capaciteit gaat er naar de functie Functionaris Gegevensbescherming (inclusief ondersteuning)?

Antwoord
De Functionaris Gegevensbescherming (FG) bestaat voor het Ministerie van Justitie en Veiligheid, inclusief de NCTV, uit 1 Fte. Tevens wordt door de Minister voor Rechtsbescherming gekeken naar de huidige rol van de FG als toezichthouder binnen een organisatie. Onderzocht wordt of deze functie verder kan worden versterkt.

173
Hoeveel geld komt er bij voor het Nationaal Cyber Security Centrum (NCSC)?

Antwoord
Vanuit het Coalitieakkoord worden voor het NCSC aanvullende middelen beschikbaar gesteld, oplopend van € 6,8 mln. in 2022 naar structureel € 33 mln. vanaf 2027.

174
Kunt u uitsplitsen waar het geld voor het NCSC naar toe gaat?

Antwoord
Het hoofddoel van de investeringen is om het NCSC te versterken tot een nationaal cybersecuritycentrum met de operationele slagkracht om toenemende digitale dreigingen het hoofd te bieden. Het is noodzakelijk dat het NCSC meer sectoren en organisaties bereikt en een stevigere kennispositie opbouwt om de digitale weerbaarheid in Nederland te verhogen. Deze investeringen komen ten goede aan het gehele cybersecuritystelsel. De investeringen zijn noodzakelijk om:
- Voldoende operationele slagkracht te organiseren om de groei van het aantal vitale organisaties op te vangen. Daarnaast dient het NCSC voorbereidingen te treffen op aanvullende forse groei van de doelgroep (extra sectoren) o.a. vanuit Europese wetgeving (NIB2).
- Verouderde informatievoorzieningen (IV) te professionaliseren en toekomstbestendig te maken en te houden.
- Als gevolg van deze groei van het NCSC dient ook de organisatie te worden versterkt.

175
Klopt het dat het kabinet de komende jaren extra investeert in het Nationaal NCSC en zo ja, hoeveel?

Antwoord
Ja, zie antwoord vraag 173.
Vanuit het Coalitieakkoord worden voor het NCSC aanvullende middelen beschikbaar gesteld, oplopend van € 6,8 mln. in 2022 naar structureel € 33 mln. vanaf 2027.

176
Waaraan wordt de significant gestegen bijdrage aan het NCSC (+220%) besteed? Waar ligt precies het verschil met afgelopen jaar?

Antwoord
Zie het antwoord op vraag 174.

177
Hoeveel geld van de 12 miljoen die is vrijgemaakt voor een versterking van de ICT en de opsporing bij het OM ten behoeve van de bestrijding van cybercrime en digitale criminaliteit, gaat direct naar de opsporing en hoeveel gaat naar de versterking van de ICT?

Antwoord
Het OM heeft structurele middelen toebedeeld gekregen oplopend van € 4 miljoen in 2022, naar € 8 miljoen in 2023 en € 12 miljoen vanaf 2024. Deze middelen zijn bedoeld om de basis op orde te krijgen en worden primair ingezet ten behoeve van de opsporing en vervolging van cybercrime (in enge zin). Een exacte verdeling van de uitgaven is nog niet gereed. Wel is voorzien dat de middelen vooral worden besteed aan capaciteit, kennis en kunde, onder meer door opleidingen. Het vergroten van kennis en kunde komt, naast de aanpak van cybercrime, bovendien tegemoet aan de aanpak van gedigitaliseerde criminaliteit. Er zijn uit deze bedragen geen specifieke investeringen in ICT-middelen voorzien.

178
Welke maatregelen zijn tot dusver genomen om logistieke ketens binnen de Rotterdamse haven digitaal veiliger te maken om weerbaarder te zijn tegen drugscriminelen en smokkelaars?

Antwoord
Bij cybersecurity-incidenten gaat het om incidenten waarbij de ICT-voorzieningen uitvallen, verminderd functioneren of worden gecompromitteerd. Zij kunnen diverse oorzaken hebben, zoals fouten in software, maar ook moedwillige computervredebreuk. Het cybersecuritybeleid is niet specifiek gericht op het bestrijden van drugscriminaliteit of smokkel. Het havenbedrijf Rotterdam is vitaal verklaard en valt hiermee onder de doelgroep van het Nationaal Cyber Security Centrum. Het Nationaal Cyber Security Centrum kan het havenbedrijf hierdoor informeren, adviseren en eventueel bijstaan in geval van een cybersecurity incident. Daarnaast bestaat de haven uit meerdere bedrijven die niet vitaal zijn verklaard. Deze bedrijven hebben zich voor een deel wel verenigd in een schakelorganisatie: FERM. Ook worden middels ondermijningsgelden vanuit JenV 150 bedrijven gestimuleerd zich aan te sluiten bij FERM. Deze bedrijven krijgen vouchers, te besteden aan cyberweerbaarheidsdienstverlening voor het tegengaan van digitale ondermijning. Op dit moment mag het Nationaal Cyber Security Centrum dreigings- en incidentinformatie nog niet in alle gevallen delen met FERM. Het wetsvoorstel tot wijziging van de Wbni maakt het mogelijk om in ruimere zin dreigings- en incidentinformatie te delen met schakelorganisaties zoals FERM. Hierdoor kunnen de niet-vitale bedrijven in de Rotterdamse haven zich weerbaarder maken tegen digitale aanvallen.

179
Kunt u toelichten wanneer de ex-ante evaluatie naar cybersecurity gereed is en of deze met de Kamer wordt gedeeld? Kunt u de in de Strategische Evaluatie Agenda genoemde onderzoeksagenda van de NCTV over cybersecurity delen met de Kamer?

Antwoord
Onder het vorige kabinet is er voor het eerst een evaluatie uitgevoerd van de Nederlandse Cybersecurity Agenda (NCSA) die op 11 juni 2021 is aangeboden aan de Tweede Kamer. Naar aanleiding van de ervaringen met de NCSA is er bij het opstellen van de Nederlandse Cybersecurity Strategie (NLCS) voor gekozen om een striktere scheiding tussen strategie en actieplan aan te brengen. De strategie kan meer toekomstgericht en duurzaam zijn, met daarbij een adaptief actieplan om bij veranderingen in de belangen, de dreiging, de weerbaarheid of andere politiek-bestuurlijke behoeften te kunnen bijsturen of intensiveren. Daarnaast kunnen acties die afgerond zijn weer leiden tot vervolgacties, bijvoorbeeld als er een verkenning of onderzoek wordt gedaan. Andere aandachtspunten die uit deze evaluatie meegenomen (of meegenomen worden in het opstellen van de actieplannen) zijn het expliciet beleggen van eigenaarschap en verantwoordelijkheden en beoogde acties en effecten concreter te beschrijven. Tenslotte is het van belang om meer aandacht te schenken aan de meetbaarheid van de beoogde resultaten en effecten van de strategie en (tussentijdse) evaluatie. In de evaluatie van de NCSA wordt een methodiek voorgesteld om te komen tot een logische opbouw van een strategie. Deze is gevolgd door hoofddoelen te formuleren die een gewenste situatie of een te realiseren effect in de toekomst beschrijven. Onder de hoofddoelen vallen subdoelen die bijdragen aan de realisatie ervan. De doelen worden uitgewerkt in een actieplan, waarin de maatregelen worden beschreven die vanuit de overheid worden genomen om het bereiken van deze doelen dichterbij te brengen. De activiteiten of

maatregelen zijn duidelijk gekoppeld aan het te realiseren effect dat in de (hoofd- en sub)doelstellingen beschreven staat.
De onderzoeksagenda van de NCTV bevindt zich op dit moment in een afrondende fase. De agenda zal in Q1 2023 gepubliceerd worden.

Overige vragen die betrekking hebben op de drie bovenstaande begrotingen

180
Hoe verhoudt de borging van de beginselen van privacy-by-design en dataminimalisatie uit de Algemene Verordening Gegevensbescherming (AVG) door BZK zich tot de beleidsplannen van het Ministerie van EZK?

Antwoord
EZK zet zich in om voorwaarden te scheppen voor een goed functionerende digitale economie. Een belangrijke voorwaarden voor een goed functionerende digitale economie is dat burgers en bedrijven vertrouwen hebben in digitalisering en grip op hun gegevens houden. De AVG en de gegevensbescherming die het biedt zijn daarin cruciaal.
Bij de onderhandelingen over Europese wetgevingstrajecten die bijdragen aan een goed functionerende digitale economie (bijv. AI en Data Act) zet het kabinet zich ervoor in dat de verhouding met de AVG duidelijk is, en dat de wetgeving geen afbreuk doet aan het niveau van gegevensbescherming dat de AVG biedt. Aanbieders van producten, diensten en AI-systemen die onder deze wetgeving vallen zullen zich naast de maatregelen die worden opgelegd, ook aan de principes van de AVG zoals dataminimalisatie moeten blijven houden. Het kabinet doet concrete voorstellen om dit te borgen.

181
Hoe verhoudt de borging van de privacy-by-design en dataminimalisatie beginselen uit de AVG zich tot het techno-optimisme dat volgt uit de beleidsplannen van JenV en EZK?

Antwoord
De digitale transitie biedt grote kansen voor de economie en de maatschappij en is essentieel om maatschappelijke uitdagingen het hoofd te bieden. Het kabinet wil de kansen die de digitale transitie biedt benutten. Zoals in de beantwoording van vraag 180 omschreven zijn er belangrijke randvoorwaarden waaraan moet worden voldaan om die kansen te kunnen benutten. Het borgen van de AVG en de beginselen daaruit zijn daarin essentieel.
Naast dat het kabinet zich inzet om de kansen van de digitale transitie en nieuwe technologieën te benutten zet het zich ook actief in om waar nodig te reguleren om de risico's van de digitale transitie het hoofd te bieden. Gezien de grensoverschrijdende werking van digitalisering is vooral het Europese speelveld daarbij van belang. Zo is het kabinet actief pleitbezorger geweest van onder andere de Digital Markets Act (DMA), Digital Services Act (DSA), de AI Act en de Dataverordening. Zoals aangegeven in de beantwoording van vraag 180 zet het kabinet zich bij de onderhandelingen over Europese wetgeving er actief voor in dat deze geen afbreuk doet aan het niveau van gegevensbescherming dat de AVG biedt.

182
Hoe verhouden de door BZK, EZK en JenV voorgestelde investeringen in digitalisering zich tot de budgetten die worden toebedeeld aan de digitale toezichthouders, zoals de Autoriteit Persoonsgegevens (AP)?

Antwoord
Het kabinet wil fundamentele rechten online beter beschermen. Daar hoort ook passend en toereikend toezicht bij. Daarom trekt het kabinet extra middelen uit voor het toezicht. Als het gaat om het toezicht op privacy krijgt de AP er € 2 miljoen bij. In 2023 en 2024 is dat respectievelijk 4 en 6 miljoen €. Vanaf 2025 krijgt de AP er structureel € 8 miljoen bij.
Het kabinet investeert ook in het toezicht op algoritmen. Van belang is dat deze gecontroleerd worden op transparantie, discriminatie en willekeur. In de budgettaire bijlage van het coalitieakkoord staan concreet vanaf 2023 middelen toegewezen aan de AP voor de rol van algoritmetoezichthouder. Het gaat om € 1 miljoen per 2023. In 2024 en 2025 is dat respectievelijk 3 en 3,6 miljoen €. Vanaf 2026 wordt de structurele financiering € 3,6 miljoen.
Voor andere toezichtstaken en toezichthouders wordt verwezen naar de antwoorden op de vragen 35 en 61.

183
Wat is de verhouding tussen de budgetten van de digitale toezichthouders, waaronder de AP, en de ervaren druk op waarden als privacy door digitalisering?

Antwoord
Zie het antwoord op vraag 182.

184
Hoe worden de digitale toezichthouders betrokken bij de implementatie van nieuwe EU regelgeving, zoals de AI Act, Digital Services Act (DSA), Digital Markets Act (DMA) en Data Governance Act (DGA)?

Antwoord
Voor het implementeren van de toezichtstaken die voorvloeien uit de nieuwe EU wetgeving vindt overleg plaats met andere departementen en toezichthouders. Zie bijvoorbeeld ook de antwoorden op de vragen 58 en 60. Met toezichthouders wordt ook samengewerkt bij het opstellen van de benodigde uitvoeringswetgeving. Wanneer er meerdere toezichthouders in aanmerking komen voor bepaalde toezichtstaken wordt met de relevante toezichthouders gesproken om te kunnen beoordelen welke toezichthouder het meest geschikt is om toezicht te houden en hoe dat op de meest effectieve wijze kan worden belegd. Daarbij is ook aandacht voor de uitvoerbaarheid, de middelen die nodig zijn om effectief toezicht te houden, en hoe de samenhang in het toezicht op alle EU-wetgevingsinitiatieven kan worden verzorgd. Verder worden toezichthouders op EU-niveau via netwerken als ECN en BEREC ook al betrokken bij de voorbereidingen op het toezicht.

185
Welk deel van de begrotingen van de digitale toezichthouders worden ingezet voor de implementatie van nieuwe EU regelgeving, zoals de AI Act, DSA, DMA en DGA?

Antwoord
Ten behoeve van de nieuwe toezichtstaken is het uitgangspunt dat er aanvullende middelen ter beschikking worden gesteld als dat nodig blijkt. Er moet bijvoorbeeld worden bekeken of er mogelijke synergie is met bestaande toezichtstaken, of dat het nieuwe taken betreft. Daarbij geldt dat de nieuwe toezichtstaken in principe niet ten koste van bestaande toezichtstaken mogen gaan. Ook wordt rekening gehouden met het feit dat de verschillende wetgevingsprocedures zich in verschillende stadia

bevinden. Dit wordt na overleg met de betrokken toezichthouders bepaald.
Voor de DSA, DGA en de DMA geldt dat de termijn waarop de wetgeving van kracht wordt bekend is. Voor deze wetgeving is daarom voor 2023 al budget beschikbaar gesteld. Voor de Data Act en de AI Act geldt dat ze zich nog volop in het Europese wetgevingsproces bevinden, waarbij zowel de termijn waarop deze verordeningen van kracht worden als ook de inhoud nog aan verandering onderhevig zijn. Om die reden geldt voor deze wetgeving dat er voor 2023 nog geen budget beschikbaar wordt gesteld. Voor de DGA, DSA en DMA is voor 2023 budget ter beschikking gesteld van € 2.286.500. Dit bedrag wordt toegevoegd aan de bestaande begroting van de relevante toezichthouders.

186
In hoeverre worden de digitale toezichthouders met een mogelijk prominente rol in het toezicht op de nieuwe EU verordening (zoals de DSA, DGA, DMA en AI Act) betrokken bij de uitwerking van het toezicht hierop?

Antwoord
Zie het antwoord op vraag 184.

187
Waarom is de budgetverantwoordelijkheid voor de algoritmetoezichthouder toebedeeld aan JenV, maar de beleidsverantwoordelijkheid bij BZK?

Antwoord
In het coalitieakkoord staat vermeld dat er een algoritmetoezichthouder komt die regelt dat algoritmen gecontroleerd worden op transparantie, discriminatie en willekeur. In de budgettaire bijlage staan hiervoor vanaf 2023 middelen toegewezen aan de Autoriteit Persoonsgegevens. De AP is een onafhankelijke toezichthouder die zich – conform de Algemene verordening gegevensbescherming (AVG) – richt op het toezicht houden op de bescherming van persoonsgegevens. Een groot deel van de algoritmen die een risico met zich meebrengen wat betreft impact op grondrechten en fundamentele vrijheden (zoals non-discriminatie) bevat persoonsgegevens. Voor algoritmen die geen persoonsgegevens bevatten is een goede samenwerking met alle betrokken toezichthouders van groot belang. Het bestaande toezicht blijft daarbij intact.
Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) stuurt -gezien de coördinerende rol van de Staatssecretaris op het digitaliseringsdomein. Hier valt ook de (beleidsmatige) inrichting van de algoritmetoezichthouder, en de bijbehorende taken, bevoegdheden en instrumenten, onder. De begroting van de AP valt onder de budgetverantwoordelijkheid van het Ministerie van Justitie en Veiligheid (JenV). Dit volgt uit de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), waarin staat vastgelegd dat de Minister voor Rechtsbescherming jaarlijks aan de AP een budget toekent ten laste van de rijksbegroting (artikel 11 UAVG).

188
Hoeveel extern advies is er ingewonnen over digitale zaken? Kan dit worden uitgesplitst naar ministerie? Hoeveel hebben deze adviezen gekost en wie heeft dit advies uitgebracht?

Antwoord
Het kabinet vindt het belangrijk om de Kamer adequaat te informeren over rijksbrede ICT-ontwikkelingen, digitale zaken in den brede en de bijbehorende kosten en ook om daarbij het inhoudelijke debat te voeren. Zoals

aangeven in antwoord 14 en in de kabinetsreactie (Kamerstuk 26 643, nr. 794) inzake «ICT-investeringen door de overheid» is het bieden van een overzicht van alle investeringen per departement nu niet mogelijk. Wel wordt in de antwoorden op de vragen 97 en 107 inzicht geboden in de betrokken instanties waarmee samengewerkt wordt en waar extern advies van verkregen wordt.

189
Hoeveel geld komt er totaal extra bij op cybersecuritygebied bij alle begrotingen bij elkaar opgesteld? Kunt u dit afzetten tegen voorgaande jaren?

Antwoord
Dit kabinet heeft evenals het vorige kabinet structurele middelen vrijgemaakt die specifiek zijn gelabeld voor het verhogen van de digitale weerbaarheid. Het vorige kabinet heeft € 95 miljoen structureel geïnvesteerd in de versterking van digitale weerbaarheid. Dit kabinet investeert een extra € 111 miljoen euro structureel in cybersecurity, de verdeling per departement is hieronder weergegeven.

Ministerie	2022	2023	2024	2025	2026	2027 e.v.
EZK	2,1	6,6	13,5	13,5	13,5	16,1
IenW	0,5	1,1	2,3	2,3	2,3	2,8
JenV	8,7	14,8	29,5	29,5	29,5	35,5
Waarvan NCSC	6,6	13,7	27,5	27,5	27,5	33
BZK	5,9	13,5	27,2	27,2	27,2	32,6
Waarvan AIVD	3,8	7,9	15,9	15,9	15,9	19,1
BZ	0,5	0,5	0,5	0,5	0,5	0,7
Def.	3,4	7,1	14,2	14,2	14,2	17
Waarvan MIVD	3,4	7,1	14,2	14,2	14,2	17
OCW	0,5	1,3	2,7	2,7	2,7	3,2
VWS	0,5	1,3	2,7	2,7	2,7	3,2
TOTAAL	22,1	46,2	92,6	92,6	92,6	111

Deze middelen maken deel uit van een bredere structurele investering van € 300 miljoen waarmee onder andere de AIVD en MIVD worden versterkt en investeringen worden gedaan op het gebied van economische veiligheid en de vitale infrastructuur. De structurele investering van € 111 miljoen draagt bij aan het uitvoeren van de verschillende acties uit die de departementen ondernemen ten behoeve van de realisatie van de doelen uit de NLCS. Daarnaast is digitale weerbaarheid onderdeel van andere investingen die dit kabinet doet onder andere in digitalisering in brede zin, de versterking van de eigen ICT-infrastructuur of investeringen op specifieke beleidsterreinen. Voorbeelden hiervan zijn de versterking van het postennetwerk, hier zitten bijvoorbeeld ook cyberdiplomaten bij of de versterking van Defensie waarvan een deel ook geïnvesteerd zal worden in cybercapaciteit. Waar geen additionele investeringen mogelijk zijn en toch een opgave ligt zal herprioritering binnen de eigen begrotingen plaatsvinden. Tenslotte wordt er nog gekeken naar de mogelijkheid om aanvullende activiteiten te financieren via de Europese digitaliseringsfondsen. Daarnaast kunnen generieke nationale fondsen zoals het groeifonds ook ingezet worden voor digitale weerbaarheid. Naast middelen zijn er ook andere kritieke randvoorwaarden waaraan moet worden voldaan voor het realiseren van de acties. Hierbij behoeft voldoende capaciteit op de arbeidsmarkt met name de aandacht.

Ministerie	Structurele investering	Structureel in
Cybersecurity (bovenop € 26 mln Miljoenennota)	49	2021
waarvan JenV	16	2021
waarvan BZK	12	2021
waarvan BZ	2	2020
waarvan EZK	9	2021
waarvan IenW	7	2021
waarvan Defensie	20	2021
waarvan AZ	3	2018

Deze investeringen komen boven op de al bestaande structurele investeringen in cybersecurity.

190
Hoeveel kostte de ontwikkeling van de coronamelder?

Antwoord
De totale kosten voor CoronaMelder in 2020, 2021 en 2022 bedragen naar verwachting ongeveer 24 miljoen euro. Dit is op basis van de realisatie in 2020 en 2021 en inclusief de verwachte lopende kosten voor dit jaar. Het gaat daarbij om in totaal 16,6 miljoen euro voor de ontwikkeling, doorontwikkeling en beheer van de app, waarvan ongeveer 9 miljoen euro aan beheer en hosting door het CIBG en DICTU. De ontwikkeling heeft daarbij in 2020 plaatsgevonden. Overige kosten zijn 3,3 miljoen euro voor communicatie (waaronder ook de massamediale publiekscampagne), en 4,1 miljoen euro voor kosten die gemaakt zijn voor de helpdesk, beleidsmatig advies, (wetenschappelijk) onderzoek en adoptie, privacy en juridisch advies en de begeleidingscommissie DOBC en taskforces DOBC en Gedragswetenschappen.

191
Hoeveel is er in totaal uitgegeven voor het project Open Overheid?

Antwoord
Het kabinet heeft begin 2021 in totaal € 1.357 mln. vrijgemaakt voor Open Overheid (2021–2026). Voor 2021–2022 gaat dit in totaal om een bedrag van € 336 mln.
Dit totaalbedrag voor 2021 en 2022 valt uiteen in drie posten: (1) verbetering rijksbrede informatiehuishouding en actieve openbaarmaking (2021–2022); (2) implementatie Wet open overheid Rijk (2022); (3) implementatie Wet open overheid medeoverheden (2022).
In 2021 is in totaal € 104 mln. vrijgemaakt voor de verbetering van de rijksbrede informatiehuishouding en actieve openbaarmaking. Gezien het moment van toekenning in het jaar is hiervan € 84 mln. uitgekeerd. De mate van uitputting verschilt per ministerie. In de departementale jaarverslagen hebben zij zich hierover verantwoord.
In 2022 is in totaal € 151 mln. uitgekeerd aan de ministeries en stelselpartijen. Naar verwachting wordt dit budget vrijwel volledig uitgegeven.
Voor de implementatie van de Wet open overheid is in 2022 in totaal € 81 mln. vrijgemaakt. Voor deze implementatie en het bieden van ondersteuning daarbij is hiervan € 52 mln. toegekend aan de medeoverheden en bijhorende koepels. De overige € 29 mln. is toegekend aan de ministeries en de landelijke uitvoeringsorganisaties.

192
Wat behelst en is de toegevoegde waarde van een visie op het gegevensbeschermingsrecht in Nederland?

Antwoord
De visie waaraan gerefereerd wordt, behelst het door Nederland in te nemen standpunt bij de eerstvolgende (tweede) evaluatie van de AVG. Het kabinet vindt het belangrijk dat de Nederlandse gezichtspunten daarin worden meegenomen. De exacte standpunten zullen de komende tijd worden uitgewerkt. Het zal gaan om voorstellen ter verbetering, verduidelijking en aanscherping van de AVG.

193
In de verticale toelichting van de Miljoenennota staat: «Daarnaast betreft het o.a een bijdrage van het Ministerie van Justitie en Veiligheid aan Defensie voor de uitvoering van activiteiten voor de Bijzondere Opsporingsdiensten (BOD) tegen ondermijning.» Kunt u uiteenzetten waarvoor het geld van Justitie en Veiligheid naar Defensie gaat?

Antwoord
De Koninklijke Marechaussee (KMar) valt als krijgsmachtonderdeel onder het Ministerie van Defensie en is vanuit haar taakstelling (art. 4 PW) een partner in de coalitie voor de (inter)nationale aanpak van ondermijnende criminaliteit. De KMar ontvangt vanuit het Ministerie van Justitie en Veiligheid middelen die beschikbaar zijn gesteld vanuit de middelen uit de Prinsjesdaggelden 2021. De gehele aanpak waarbinnen deze investeringen worden gedaan, wordt geschetst in de volgende brief: Extra investeringen in het breed offensief tegen ondermijnende criminaliteit (Tweede Kamer, vergaderjaar 2021–2022, 29 911, nr. 329).
Voor de post «Bijzondere Opsporingsdiensten en landelijke organisaties» ontvangt de KMar structurele middelen. Deze worden ingezet voor het versterken van de informatiepositie in de keten, een specialistische bijdrage ten aanzien van bestrijding van identiteitsfraude en het realiseren van flexibele capaciteit teneinde ondermijnende criminaliteit op de mainports te bestrijden. Daarnaast wordt geïnvesteerd in het realiseren van een programmatische aanpak van ondermijnende criminaliteit vanuit de KMar, alsmede de inrichting van een Team Bijzondere Getuigen met als doel de aangiftebereidheid te vergroten.