Actieplan Nederlandse Cybersecuritystrategie 2022-2028

Ambities en acties voor een digitaal veilige samenleving

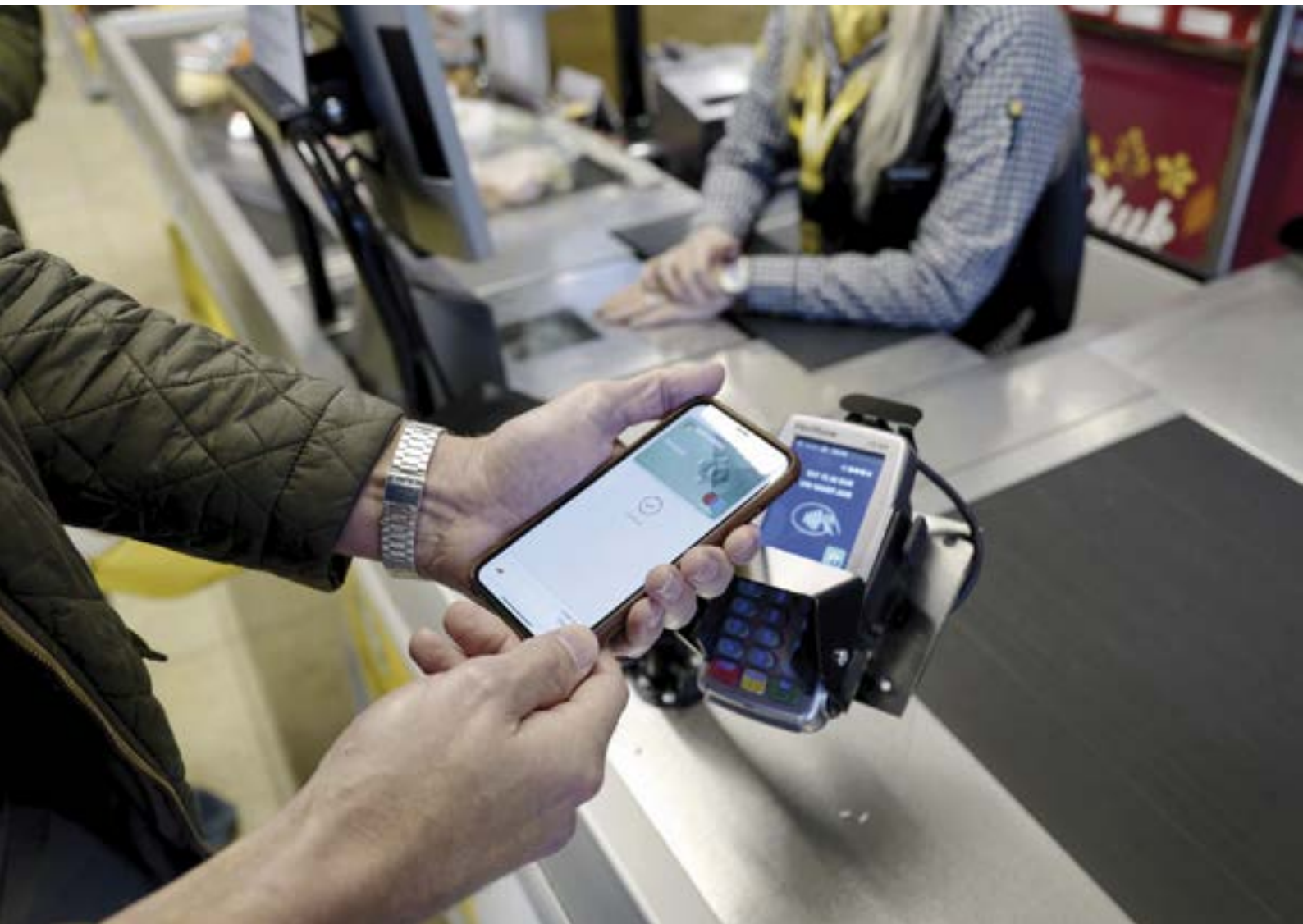

Foto omslag: We gebruiken steeds minder contant geld. Tegenwoordig gebeurt 81% van de betalingen aan de kassa zelfs contactloos. Dat maakt het nog belangrijker dat ons betalingsverkeer veilig en betrouwbaar is en blijft.

De Nederlandse Cybersecuritystrategie (NLCS) is tot stand gekomen met een brede betrokkenheid van publieke, private en maatschappelijke organisaties, onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het Cybersecurity Beeld Nederland 2022 (CSBN) vormt het uitgangspunt voor de pijlers en doelstellingen van de NLCS.

Actieplan Nederlandse Cybersecuritystrategie 2022-2028

Ambities en acties voor een digitaal veilige samenleving

Inhoud

Pijler I
Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Pijler II
Veilige en innovatieve digitale producten en diensten

Pijler III
Tegengaan van digitale dreigingen van staten en criminelen

Pijler IV
Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Digitalisering is een belangrijke stap om zorg voor iedereen toegankelijk te houden en de druk op zorgprofessionals te verminderen. Het maakt het mogelijk om zorg op afstand te verlenen, maar biedt ook sneller toegang tot informatie.

Pijler I
Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Doel I.1: Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.

I.1.1 Herziening van het stelsel

I.1.1.1	Actie samenvatting Het NCSC, DTC en CSIRT-DSP worden samengevoegd tot één nationale cyber-security autoriteit (CSIRT).	Tijdlijn 2022-2026	Eigenaar JenV, EZK Betrokken NCSC, DTC, CSIRT-DSP
I.1.1.2	Actie samenvatting Voor de overheidsschakelorganisaties binnen het cybersecurity informatiede-lingsstelsel wordt beoordeeld welke van hun taken centraal (bij de nationale cybersecurity autoriteit) of sectoraal moeten worden belegd.	Tijdlijn 2022-2023	Eigenaar JenV, EZK Betrokken VWS, BZK, DEF, OCW, IenW
I.1.1.3	Actie samenvatting Samen met het bedrijfsleven wordt een routekaart opgesteld voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling. De basis voor dit traject is het opgeleverde Cyclo-tronrapport.	Tijdlijn 2022-2023	Eigenaar JenV Betrokken NCSC, DTC, AIVD, MIVD, politie, OM, private partners, medeoverheden
I.1.1.4	Actie samenvatting Het NCSC verkent met partners de haal-baarheid van een centrale landelijke campus/locatie ter bevordering van samenwerking, informatiedeling, ken-nisontwikkeling en onderzoek tussen publieke en private partijen.	Tijdlijn 2022-2023	Eigenaar JenV Betrokken NCSC, DTC, AIVD, MIVD, politie

I.1.2 Versterken Landelijk Dekkend Stelsel van cybersecuritysamenwerkingsverbanden (LDS)

I.1.2.1	Actie samenvatting Het wettelijk kader wordt gewijzigd zodat organisaties binnen het LDS in staat worden gesteld om informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen. Voorbeelden hiervan zijn de aankomende wijziging van de Wbni die dit najaar in de Kamer wordt behandeld en het wetsvoorstel bevordering digitale weerbaarheid bedrijven.	Tijdlijn 2022-2026	Eigenaar JenV, EZK Betrokken DTC, NCSC
I.1.2.2	Actie samenvatting In interdepartementaal verband worden eisen voor aansluiting op het LDS geformuleerd. Deze zullen verplichtend zijn voor overheidsschakelorganisaties en als richtinggevende leidraden gelden voor private schakelorganisaties. Private partners worden betrokken bij de uitwerking van deze leidraden.	Tijdlijn 2023-2024	Eigenaar JenV Betrokken EZK, VWS, IenW, DTC, NCSC
I.1.2.3	Actie samenvatting Het kabinet gaat schakelorganisaties ondersteunen met financieringsmodellen waardoor zij in staat worden gesteld om duurzame financiering te borgen.	Tijdlijn 2023-2026	Eigenaar JenV Betrokken NCSC, DTC
I.1.2.4	Actie samenvatting Er wordt een communicatieplan LDS opgeleverd aan de hand waarvan organisaties wegwijs kunnen worden binnen het stelsel. Onderdeel hiervan is te komen tot heldere aanspreekpunten.	Tijdlijn 2023-2025	Eigenaar JenV Betrokken BZK, EZK, NCSC, DTC

I.1.3 Uitbreiden schakelorganisaties binnen het LDS

I.1.3.1	Actie samenvatting In samenwerking met private partners wordt een LDS-bouwplan opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven de dekkingsgraad van het LDS te verhogen. Onderdeel van dit bouwplan is een overzicht van de huidige staat van het LDS om inzicht te creëren in alle initiatieven die reeds zijn ontwikkeld en de huidige leemtes in het LDS.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken EZK, OCW, VWS, IenW, BZK, NCSC, DTC, medeoverheden en private partners
I.1.3.2	Actie samenvatting Met een financiële bijdrage van BZK gaan de provincies, onder regie van het IPO, verder met het inrichten van interprovinciaal informatieknooppunt als schakelorganisatie binnen het LDS.	Tijdlijn 2022-2023	Eigenaar BZK Betrokken IPO
I.1.3.3	Actie samenvatting OCW richt een CERT op voor het primair en voortgezet onderwijs.	Tijdlijn 2022-2023	Eigenaar OCW Betrokken OCW en SURFcert
I.1.3.4	Actie samenvatting IenW versterkt het CERT Watermanagement.	Tijdlijn 2022-2023	Eigenaar IenW Betrokken RWS

I.1.4 Nationaal Detectie Netwerk (NDN)

I.1.4.1	Actie samenvatting Alle nog niet aangesloten Rijksoverheidsorganisaties worden aangesloten op het Nationaal Detectie Netwerk.	Tijdlijn 2023	Eigenaar BZK Betrokken JenV, CIO-Rijk, NCSC
I.1.4.2	Actie samenvatting De samenwerking en informatiedeling tussen de partners in het Nationaal Detectie Netwerk (AIVD, MIVD, NCSC) en de dienstverlening richting aangesloten organisaties wordt versterkt door geïntensiveerde onderlinge kennisuitwisseling.	Tijdlijn 2023-2026	Eigenaar JenV Betrokken AIVD, MIVD, NCSC, CIO-Rijk

I.1.5 Slachtoffernotificatie

I.1.5.1	Actie samenvatting Er komt een onderzoek om vast te stellen op welke manier bedrijven en burgers die doelwit dreigen te worden of slachtoffer zijn van digitale incidenten, geïnformeerd kunnen worden. De NCTV en NCSC onderzoeken hierbij specifiek hoe slachtoffernotificatie uit niet-strafrechtelijke bron verder kan worden vormgegeven.	Tijdlijn 2022-2023	Eigenaar JenV Betrokken NCSC, AIVD, MIVD en private partners
I.1.5.2	Actie samenvatting De politie en het OM verkennen op welke manier het notificeren van slachtoffers die blijken uit strafrechtelijke onderzoeken verder vorm kan krijgen.	Tijdlijn 2022-2025	Eigenaar JenV Betrokken OM, Politie, NCTV, NCSC

Doel I.2: Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee.

I.2.1 Digitale weerbaarheid vitale infrastructuur

I.2.1.1	Actie samenvatting De vernieuwde EU NIB-richtlijn (NIB2) zal in 2024 via de Wbni in Nederland worden geïmplementeerd.	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK, LNV, MIVD, AIVD en NCSC
I.2.1.2	Actie samenvatting Om de lasten voor bedrijven zoveel mogelijk te beperken, zal sectorale wetgeving, zoals de DORA en de Network Code en aanpalende wetgeving zoals de CER-richtlijn in nauwe samenhang met de NIB2 worden geïmplementeerd.	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken FIN, EZK, OCW, BZK, IenW, VWS en LNV
I.2.1.3	Actie samenvatting Het kabinet start in 2023 met uitgebreide voorlichtingscampagnes om organisaties die onder de nieuwe wet komen te vallen te informeren over voor hun geldende rechten en plichten, en hen actief te begeleiden bij de implementatie.	Tijdlijn 2023-2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK en LNV
I.2.1.4	Actie samenvatting Om kwaliteit en consistentie van het toezicht op de Wbni na de implementatie van de NIB2 te verzekeren, wordt het *Samenhangend Inspectiebeeld Cybersecurity Vitale Processen* en de bijhorende governance doorontwikkeld. Op deze manier wordt de samenhang in en transparantie over de aanpak van informatiegestuurd en risicogericht toezicht geborgd.	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK en LNV

I.2.1.5	Actie samenvatting Verkenning naar het opzetten van één centraal meldloket waarmee meldingen voor NIB2 laagdrempelig en gelijktijdig kunnen worden gedaan bij het CSIRT en de toezichthouder. Bij deze verkenning worden ook meldingen uit gerelateerde wetgeving betrokken (AVG, DORA, Network Code).	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK en LNV
I.2.1.6	Actie samenvatting Evalueren van de huidige methode voor het vaststellen van drempelwaarden meldplicht voor cyberincidenten onder de Wbni. Deze uitkomsten worden in ieder geval betrokken bij het bepalen van drempelwaarden voor nieuw aangewezen aanbieders.	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK en LNV
I.2.1.7	Actie samenvatting Het NCSC zal gezien de toename van doelgroeporganisaties, schaalbare technische voorzieningen voor digitale en geautomatiseerde informatiedeling met en tussen doelgroepen en partners realiseren en implementeren.	Tijdlijn 2022- 2024	Eigenaar JenV Betrokken NCSC
I.2.1.8	Actie samenvatting De NIB2-eisen hebben raakvlakken met de Baseline Informatiebeveiliging Overheid (BIO) en worden waar van toepassing daarin opgenomen zodat de verbinding met de basisbeveiliging voor de overheid herkenbaar blijft.	Tijdlijn 2022-2024	Eigenaar BZK Betrokken
I.2.1.9	Actie samenvatting Er wordt gestart met een verkenning naar de benodigde stappen voor het verhogen van de digitale weerbaarheid van de vitale infrastructuur in Caribisch Nederland.	Tijdlijn 2022-2024	Eigenaar JenV Betrokken BZK

I.2.1.10	Actie samenvatting Het kabinet start een Versterkte Aanpak Vitaal om de bescherming van de Nederlandse vitale infrastructuur te verbreden. Onderdeel van deze aanpak is een herziening van het vitaalbeleid en bijbehorende wetgeving, mede in het licht van de CER- en NIB2-richtlijnen. Vitale aanbieders zullen begin 2023 over het nieuwe stelsel worden geconsulteerd. De versterkte aanpak voorziet daarnaast in een structurele samenwerking met een deel van de vitale sectoren, een verbeterd beleidsinstrumentarium om sectorale risico's en afhankelijkheden beter in beeld te krijgen en in een doorontwikkeling van informatiedeling over kwetsbaarheden en dreigingen. Cybersecurity maakt hier integraal deel van uit.	Tijdlijn 2022-2024	Eigenaar JenV Betrokken OCW, BZK, IenW, VWS, FIN, EZK, LNV, NCSC, AIVD en MIVD

I.2.2 Digitale weerbaarheid MKB en bedrijfsleven

I.2.2.1	Actie samenvatting NCSC en DTC ontwikkelen nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity in het risicomanagementproces; crisispreparatie; incidentrespons en thematische advisering. Deze gedifferentieerde en datagedreven informatie- en kennisproducten en -diensten worden gezamenlijk en laagdrempelig beschikbaar gesteld ten behoeve van organisaties op een manier die past bij het volwassenheidsniveau.	Tijdlijn 2022-2024	Eigenaar JenV, EZK Betrokken NCSC, DTC
I.2.2.2	Actie samenvatting Realisatie van eerste versie van centrale registers voor cybersecurity gerelateerde informatie (i.e. type ransomware, kwetsbaarheden).	Tijdlijn 2023	Eigenaar JenV Betrokken NCSC
I.2.2.3	Actie samenvatting Het gebruik van tools, zoals risicoscans, en producten en beveiligingsadviezen incl. handelingsperspectief, stimuleren onder het MKB onder andere via brancheorganisaties, zoals bij het publiek-private platform Samen Digitaal Veilig.	Tijdlijn 2022-2024	Eigenaar EZK, JenV Betrokken DTC, NCSC, VNO-NCW, MKB-Nederland
I.2.2.4	Actie samenvatting Er wordt één set aan basismaatregelen vanuit de overheid geformuleerd en gepromoot voor vrijwillig gebruik door organisaties.	Tijdlijn 2023 - 2024	Eigenaar JenV Betrokken EZK, BZK, NCSC, DTC, AIVD, MIVD

I.2.3 Digitale weerbaarheid onderwijs

I.2.3.1	Actie samenvatting Er wordt een normenkader informatiebeveiliging en privacy geïmplementeerd voor het primair en voortgezet onderwijs, incl. periodieke monitors en benchmarks om te volgen of schoolbesturen voldoen aan de norm.	Tijdlijn 2022-2024	Eigenaar OCW
I.2.3.2	Actie samenvatting Schoolbesturen in het primair en voortgezet onderwijs besteden in hun jaarverslag verplicht expliciet aandacht aan informatiebeveiliging en privacy.	Tijdlijn 2022-2024	Eigenaar OCW
I.2.3.3	Actie samenvatting In het primair onderwijs, voortgezet onderwijs, MBO en hoger onderwijs wordt gewerkt aan bewustzijn van digitale risico's en maatregelen bij studenten, medewerkers en bestuurders door middel van campagnes, crisisoefening en speciale werkgroepen.	Tijdlijn 2022-2024	Eigenaar OCW
I.2.3.4	Actie samenvatting De instellingen in het hoger en middelbaar beroepsonderwijs gebruiken voor hun audits het NBA volwassenheidsmodel en afgeleid hiervan het Toetsingskader Informatiebeveiliging Hoger Onderwijs van SURF.	Tijdlijn 2022-2024	Eigenaar OCW Betrokken SURF

I.2.4 Digitale weerbaarheid zorginstellingen

I.2.4.1	Actie samenvatting Er wordt een herziene versie van de NEN 7510[1] gepubliceerd. Hierbij worden implementatietools ontwikkeld die bijdragen aan een verbeterde implementatiegraad van de NEN 7510.	Tijdlijn 2025	Eigenaar VWS Betrokken
I.2.4.2	Actie samenvatting De Kwetsbaarheden Analyse Tool (KAT) is open-source beschikbaar gemaakt zodat alle zorgorganisaties dit kunnen gebruiken om actief te scannen op kwetsbaarheden in hun eigen systemen. VWS en Z-CERT stimuleren zorgorganisaties om dit structureel doen. De tool wordt ook breder beschikbaar gesteld.	Tijdlijn 2022-2023	Eigenaar VWS Betrokken Z-CERT
I.2.4.3	Actie samenvatting De bijstand bij incidenten binnen de zorgsector wordt uitgebreid door gefaseerd nieuwe subsectoren aan te sluiten op dienstverlening van Z-CERT. Voor 2023 sluiten eerstelijnszorgsector, zoals huisartsen en apotheken aan. In de loop van 2023 en 2024 worden de volgende sectoren aangesloten: Gehandicaptenzorg, Verpleging, verzorging en thuiszorg en Revalidatiezorg.	Tijdlijn 2023-2024	Eigenaar VWS Betrokken Z-CERT
I.2.4.4	Actie samenvatting Het programma Informatieveilig gedrag in de zorg voorziet zorginstellingen van manieren om informatieveilig gedrag te bevorderen.	Tijdlijn 2022-2023	Eigenaar VWS Betrokken ECP, Z-CERT

1 Een norm voor informatiebeveiliging voor de zorgsector in Nederland. Zorgaanbieders zijn op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) verplicht om te voldoen aan de NEN-7510.

I.2.4.5	Actie samenvatting In het kader van preventie en detectie zal Z-CERT oefen- en testactiviteiten organiseren samen met aangesloten zorginstellingen en best practices ontwikkelen in relatie tot de vigerende, zorgsector specifieke, informatiebeveiligingsnorm NEN7510.	Tijdlijn 2023	Eigenaar VWS Betrokken Z-CERT

I.2.5 Digitale weerbaarheid sectoren infrastructuur en waterstaat

I.2.5.1	Actie samenvatting De versterking van de digitale weerbaarheid van sectoren waarvoor IenW een systeemverantwoordelijk heeft, zoals drinkwater, keren en beheren, luchtvaart, maritiem, nucleair, spoorwegen en plaats- en tijdbepaling Global Navigation Satelite System (GNSS). Onder andere door: • Het organiseren van bestuurlijk overleg met sectoren om kennis en ervaring uit te wisselen en te bespreken op welke manier kan worden samengewerkt om digitale risico's te kunnen beheersen. • Ontwikkelen van sectorale kennisproducten zoals periodieke cybersecuritydreigingsbeelden per sector die o.a. bijdragen aan integraal risicomanagement; tegengaan van ransomware en inzicht in ketenrisico's. • Faciliteren van organisaties bij opleiding, testen, trainen en oefenen zodat zij beter in staat zijn snel te reageren op en te herstellen na een cyberincident, passend bij de behoefte van de sector.	Tijdlijn 2022-2026	Eigenaar IenW Betrokken NCSC, AIVD, MIVD, CERT Watermanagement

I.2.6 Digitale weerbaarheid rijksoverheid

I.2.6.1

Actie samenvatting
De ambitie van BZK op dit onderwerp wordt uiteengezet in de I-strategie Rijk en de routekaarten, zoals die op 15 juli 2022 met de Kamer is gedeeld.[2] Voorbeelden van concrete acties zijn:

- In 2022 wordt gestart met de projectaanpak 'redteaming' gericht op drie sporen: risicogericht testen, kennisdeling (binnen Rijksoverheid), opvolging van bevindingen.
- Er komt een verplichte basistraining digitale weerbaarheid voor rijkoverheidsmedewerkers vanaf 2024.
- Daarnaast wordt, met facilitering vanuit CIO-Rijk, parallel gewerkt aan beleid voor een aantal activiteiten: handreikingen bij het in augustus 2022 herziene rijksbrede cloudbeleid, aanpak risico's quantum computing, rijksbrede voorzieningen voor hoog gerubriceerde informatie, en versterken van het SOC-stelsel Rijk.
- Het rijksbrede programma I-Partnerschap richt zich aanvullend aan dcypher op de samenwerking tussen de Rijkoverheid en hoger onderwijs op I-gebied, waaronder cybersecurity. Een van de onderdelen hiervan is het I-doctoraatsprogramma. Dit levert kenniswerkers en draagt met onderzoek en innovatie bij aan de versterking van de kennispositie en de digitale uitdagingen van het Rijk.

Tijdlijn
2022-2025

Eigenaar
BZK

Betrokken
NCSC, Rijks-CIO's, AIVD, MIVD

2 Kamerbrief routekaarten I-strategie Rijk 2022-2025 | Kamerstuk | Rijksoverheid.nl

I.2.7 Digitale weerbaarheid overheid

I.2.7.1

Actie samenvatting
Er wordt een bestuurlijk convenant opgesteld met de VNG ten aanzien van digitale veiligheid waarin de gezamenlijke inzet op het gebied van cybersecurity voor gemeenten nader zal worden uitgewerkt.

Tijdlijn
2022

Eigenaar
BZK

Betrokken
VNG

I.2.7.2

Actie samenvatting
In 2023 vindt de doorontwikkeling van en monitoring op de Baseline Informatiebeveiliging Overheid (BIO) plaats incl. de wettelijke verankering hiervan in de Wet Digitale Overheid.

Tijdlijn
2023

Eigenaar
BZK

Betrokken

I.2.7.3

Actie samenvatting
Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) verlengt en actualiseert de uitvoering van het ondersteuningsprogramma BIO voor de gehele overheid. Hiermee worden organisaties bijgestaan bij de implementatie en toepassing van de BIO.

Tijdlijn
2022-2027

Eigenaar
BZK

Betrokken
CIP

I.2.7.4

Actie samenvatting
Het CIP verlengt en actualiseert de uitbreiding en doorontwikkeling van de service Informatiebeveiliging en Privacy. Overheden krijgen maatwerkadvisering van professionals bij de overheid over digitale veiligheid en privacy. Organisaties met onvoldoende kennis op gebied van informatieveiligheid worden op deze manier laagdrempelig geholpen door organisaties met specifieke expertise.

Tijdlijn
2022-2027

Eigenaar
BZK

Betrokken
CIP

I.2.7.5	Actie samenvatting Doorontwikkeling van verantwoordings-systematiek ENSIA (Eenduidige Normatief Single Information Audit). Door horizontaal en verticaal toezicht te organiseren met de BIO als basis werken gemeenten aan betere informatieveiligheid en wordt de democratische verantwoording over IB gefaciliteerd.	Tijdlijn 2022-2025	Eigenaar BZK Betrokken VNG

2.8 Digitale weerbaarheid sectoren met operationele technologie- en procesautomatiseringssystemen

I.2.8.1	Actie samenvatting De aanpak om de beveiliging van Industrial Automation and Control Systems (IACS) te verhogen wordt versterkt door middel van een coalitie. Voorbeelden van acties binnen de coalitie zijn: • De ontwikkeling en implementatie van een (significante en realistische) IACS component in landelijke oefeningen, trainingen en opleidingen. • De versterking van kennisopbouw en de realisatie van instrumenten, bijvoorbeeld handreikingen en best practices om publieke en private organisaties te helpen om voor IACS de juiste maatregelen te implementeren en de juiste risico's te definiëren en aan te pakken. • Het delen van deze kennisproducten en instrumenten via een collectieve kennis hub IACS.	Tijdlijn 2022-2024	Eigenaar IenW Betrokken NCSC, EZK, (private) partners

2.9 Zicht op digitale weerbaarheid van overheid en bedrijfsleven

I.2.9.1	Actie samenvatting Er worden pilots uitgevoerd waarbinnen de toegevoegde waarde van een IT-verslag en een IT-auditverklaring binnen de overheid wordt onderzocht. Vergelijkbaar met het gangbare financiële jaarverslag. De verkenning sluit aan op pilots uit het bedrijfsleven.	Tijdlijn 2023	Eigenaar BZK Betrokken ADR
I.2.9.2	Actie samenvatting Er wordt samen met het brede cybersecurityveld een monitoringssystematiek voor de digitale weerbaarheid van Nederland opgezet. Een eerste rapportage wordt 2024 verwacht.	Tijdlijn 2024-2026	Eigenaar JenV Betrokken BZK, EZK, NCSC, DTC
I.2.9.3	Actie samenvatting Het Centrum voor Informatiebeveiliging en Privacy (CIP) beheert en ontwikkelt de website basisbeveiliging.nl waarop op basis van verschillende indicatoren, scores op veiligheidsgebied van overheidsorganisaties worden gemeten en getoond.	Tijdlijn 2023	Eigenaar BZK Betrokken CIP
I.2.9.4	Actie samenvatting In het kader van de corporate governance code wordt met het bedrijfsleven overlegd op welke manier zij kunnen samenwerken voor het beheersen van cybersecurityrisico's bij beursgenoteerde bedrijven.	Tijdlijn 2022	Eigenaar EZK
I.2.9.5	Actie samenvatting Met verzekeraars wordt verkend welke rol zij zouden kunnen spelen in het kader van gevolgschade van cyberincidenten.	Tijdlijn 2022-2023	Eigenaar JenV Betrokken EZK, FIN

Doel I.3: Organisaties reageren, herstellen en leren snel en adequaat op en van cyber- incidenten en –crises.

I.3.1 Incident- en crisispreparatie

I.3.1.1	Actie samenvatting Het geactualiseerde Landelijk Crisisplan Digitaal (LCP-Digitaal) wordt gelanceerd en in gebruik genomen. Dit plan biedt de basis voor de digitale crisisaanpak.	Tijdlijn 2022	Eigenaar JenV Betrokken NCP-partners
I.3.1.2	Actie samenvatting Departementen zorgen voor aansluiting van departementale crisisplannen op het Landelijk Crisisplan Digitaal en kunnen aantonen dat incident-, continuïteit- en herstelplannen zijn getest, door middel van bijvoorbeeld een oefening of audit. Ook geven departementen opvolging aan (oefen)evaluaties en bevindingen.	Tijdlijn 2022-2024	Eigenaar JenV Betrokken Departementen
I.3.1.3	Actie samenvatting Als aanvulling op het LCP digitaal wordt onderzocht of het huidige wettelijke crisis instrumentarium (incl. noodwetgeving) voor ingrijpen bij nationale crises voldoende is voor nationale crises met digitale elementen. Hierbij zal ook aandacht zijn voor een verdringingsreeks.	Tijdlijn 2022-2024	Eigenaar JenV
I.3.1.4	Actie samenvatting Relevante regionale crisisplannen worden aangesloten op het Landelijk Crisisplan Digitaal.	Tijdlijn 2022-2023	Eigenaar JenV Betrokken Veiligheidsregio's

I.3.1.5	Actie samenvatting Nederland neemt een actieve rol in de doorontwikkeling van internationale crisisnetwerken.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken DEF, BZ
I. 3.1.6	Actie samenvatting Doorontwikkeling van het Nationaal Response Netwerk (NRN) tot nationaal incident responsnetwerk. Onder andere door beschikbaar maken en houden van defensiecybercapaciteiten voor militaire bijstand en steunverlening. Verhogen inzet door het strategisch detacheren van cyberexperts tussen (Rijks)overheidsorganisaties. Uitbreiden publiek-private samenwerking. In kaart brengen beschikbare responscapaciteit.	Tijdlijn 2022-2025	Eigenaar JenV, DEF Betrokken NRN partners
I. 3.1.7	Actie samenvatting Ontwikkeling van kennisproducten/ diensten om organisaties te adviseren over hun incidentresponsprocessen (factsheets, whitepapers, runbooks etc.).	Tijdlijn 2022-2024	Eigenaar JenV Betrokken NCSC, DTC
I. 3.1.8	Actie samenvatting Inlichtingengebaseerde incidentcoördinatie vanuit de AIVD en MIVD wordt verder uitgebouwd, onder andere via samenwerking in de CIIC.	Tijdlijn 2022-2026	Eigenaar BZK, DEF, Betrokken NCSC, CIIC
I. 3.1.9	Actie samenvatting Defensie investeert in personele en technische capaciteit in de gehele keten bij Defensie om het delen van informatie sneller en veiliger te laten plaatsvinden en de reactiesnelheid bij kwetsbaarheden en incidenten te verhogen. Voor verdere uitwerking, zie bijlage 2 van de Defensienota 2022.	Tijdlijn 2023-2026	Eigenaar DEF

I.3.2 Oefenen

I.3.2.1	Actie samenvatting Na de publicatie van de Rijksbrede Risicoanalyse en de Rijksbrede Veiligheidsstrategie zal een interdepartementale oefenagenda worden opgesteld, waarin ook de planning van cyber- en hybride-oefeningen wordt meegenomen.	Tijdlijn 2023-2024	Eigenaar JenV Betrokken Alle departementen
I.3.2.2	Actie samenvatting De nationale oefening ISIDOOR wordt georganiseerd. De deelnemers worden in aanloop hiernaartoe gestimuleerd dat organisaties eigen plannen en procedures hebben vastgelegd en hun medewerkers hiervoor zijn opgeleid en getraind.	Tijdlijn 2023	Eigenaar JenV Betrokken NCSC, politie, AIVD, MIVD en private partners.
I.3.2.3	Actie samenvatting Als aanvulling op ISIDOOR worden diverse sectorale en lokale oefeningen georganiseerd. Voorbeelden hiervan zijn het symposium met crisissimulatie dat VWS organiseert voor ongeveer 200 deelnemers uit alle lagen van de zorgsector; het jaarlijks georganiseerde overheidsbrede cyberprogramma waarvan oefeningen deel uitmaken en lokale oefeningen, zoals 'Hack the Hague'.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken Departementen, overheden, operationele partners en private partners.
I.3.2.4	Actie samenvatting Jaarlijks oefenen overheden (Rijksoverheid, provincies, gemeenten en waterschappen) aan de hand van een gesimuleerde hackaanval. Tevens zijn er gedurende het gehele jaar Webinars waarbij organisaties binnen en buiten de overheid kennis delen.	Tijdlijn 2022-2026	Eigenaar BZK Betrokken Medeoverheden

I.3.2.5	Actie samenvatting Defensie gaat frequenter cyberoefeningen organiseren, waarbij ook de verbinding wordt gezocht met nationale en internationale partners.	Tijdlijn 2022-2026	Eigenaar DEF
I.3.2.6	Actie samenvatting Nederland doet mee aan internationale NAVO- en EU-oefeningen, waaronder edities van *PACE*, *CMX* en *BlueOLEx*, en streeft naar een intensievere jaarlijkse deelname.	Tijdlijn 2022-2026	Eigenaar JenV, DEF Betrokken AIVD, MIVD, NCSC

Het einde van de OV-chipkaart is nabij. Binnenkort is inchecken met een betaalplas of smartphone mogelijk in het openbaar vervoer. Dit moet zorgen voor meer reis- en betalingsgemak. Een dergelijke verandering is een behoorlijke operatie. Ruim 60.000 poortjes en kaartlezers moeten worden omgebouwd.

Pijler II
Veilige en innovatieve digitale producten en diensten

Doel II.1: Digitale producten en diensten zijn veiliger.

II.1.1 Europese wetgeving voor digitale producten en diensten

	Actie samenvatting	Tijdlijn	Eigenaar / Betrokken
II.1.1.1	Het kabinet maakt zich in de onderhandelingen voor de *Europese Cyber Resilience Act* (CRA) hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, inclusief bijbehorende standaarden en toezicht. Deze zorgplicht moet gedurende de hele levenscyclus blijven gelden.	2022-2024	Eigenaar: EZK Betrokken: JenV, BZK, private partners
II. 1.1.2	Het kabinet zet zich in om de samenhang tussen regelgeving voor producten en diensten te bevorderen onder meer door in te zetten op goede aansluiting van de CRA op sectorspecifieke cybersecurity-eisen in Europese regelgeving (zoals voor medische hulpmiddelen en auto's) en generieke wetgeving zoals de Richtlijn voor Algemene Productveiligheid en de Richtlijn voor aansprakelijkheid voor producten met gebreken.	2022-2024	Eigenaar: EZK Betrokken: JenV, VWS, IenW, private partners
II. 1.1.3	Het kabinet draagt samen met private partijen via het Nederlandse normalisatie-instituut NEN bij aan de totstandkoming van Europese geharmoniseerde normen voor cybersecurity-eisen onder de Richtlijn Radioapparatuur.	2022-2024	Eigenaar: EZK Betrokken: NEN, private partners

II.1.2 Toezicht en handhaving op digitale producten en diensten

II. 1.2.1	Actie samenvatting Consumenten en ondernemers worden voorgelicht over de richtlijnen verkoop goederen en levering digitale inhoud, op grond waarvan consumenten recht hebben op (veiligheids)updates zolang zij die redelijkerwijs mogen verwachten.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken ACM
II. 1.2.2	Actie samenvatting Agentschap Telecom versterkt haar toezicht op de cybersecurity markttoegangseisen voor draadloos verbonden apparaten onder de Radio Equipment Directive onder meer door onderzoeken via het Internet of Things Testlab en versterking van capaciteit.	Tijdlijn 2022-2024	Eigenaar EZK Betrokken AT
II. 1.2.3	Actie samenvatting Agentschap Telecom houdt in Nederland als Nationale Cybersecurity Certificeringsautoriteit (NCCA) toezicht op de certificeringschema's in Nederland en autoriseert de uitgifte van certificaten met het certificeringsniveau 'hoog'. Daarbij werkt zij samen met het Nationaal Bureau Verbindingsbeveiliging van de AIVD.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken AT, AIVD
II. 1.2.4	Actie samenvatting Autoriteit Consument en Markt houdt toezicht op de verkopers van producten die verplicht zijn informatie te geven aan consumenten over hoe lang (veiligheids)updates beschikbaar zijn.	Tijdlijn 2022-2024	Eigenaar EZK Betrokken ACM

II. 1.2.5	Actie samenvatting Agentschap Telecom en de Autoriteit Consument en Markt gaan intensiever samenwerken om handhaving en toezicht op het gebied van veilige producten en diensten te verbeteren onder meer door het opstellen van een gezamenlijke oefenagenda.	Tijdlijn 2022-2024	Eigenaar EZK Betrokken AT, ACM

II.1.3 Certificering en standaarden

II. 1.3.1	Actie samenvatting Het kabinet draagt in samenwerking met private partijen bij aan de ontwikkeling en adoptie van Europese cybersecurity certificeringschema's voor ICT-producten, diensten en processen, zoals voor clouddiensten, 5G technologie en *Common Criteria*.	Tijdlijn 2023	Eigenaar EZK Betrokken BZK, JenV, private partijen
II. 1.3.2	Actie samenvatting Het kabinet zet in op de ontwikkeling van Europese certificeringschema's voor veilige software en cybersecurity diensten.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken JenV, BZK, private partijen
II. 1.3.3	Actie samenvatting EZK stimuleert de bewustwording en implementatie van certificeringsschema's onder de Cyber Security Act.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken AT

II.1.3.4	Actie samenvatting De Baseline Security Product Assessment wordt doorontwikkeld, zodat het overeenkomt met vergelijkbare Europese evaluatiestandaarden om uitwisselbaarheid van (veilige) Europese producten te bevorderen. Daarnaast werkt de AIVD samen met Agentschap Telecom aan een transitie van het op common criteria gebaseerde nationale schema NSCIB naar het Europese schema zodra de Cyber Security Act in werking treedt.	Tijdlijn 2022-2023	Eigenaar BZK Betrokken AIVD, EZK
II. 1.3.5	Actie samenvatting Het kabinet stimuleert contacten met gelijkgezinde derde landen over aansluiting van internationale standaarden op Europese standaarden en omgekeerd de ontwikkeling van vergelijkbare wet- en regelgeving en standaarden in die landen.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken JenV, BZ, private partijen
II. 1.3.6	Actie samenvatting Er wordt verkend hoe organisaties beter in staat kunnen worden gesteld om duidelijke afspraken te maken over cybersecurity met hun afnemers middels onderzoek naar de contractrechtpraktijk en best practices in business-to-business relaties tussen aanbieders van ICT-producten en -diensten en afnemers.	Tijdlijn 2023	Eigenaar EZK Betrokken DTC, private partijen

II.1.4 Algemene beveiligingseisen rijksoverheid (ABRO) en overheidsinkoopbeleid

II. 1.4.1	Actie samenvatting Er worden Algemene Beveiligingseisen opgesteld voor de Rijksoverheid (ABRO), op basis van doorontwikkeling van het bestaande regime Algemene beveiligingseisen Defensieopdrachten (ABDO), waaraan bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen moeten voldoen.	Tijdlijn 2022-2023	Eigenaar BZK Betrokken DEF, JenV AIVD, MIVD
II. 1.4.2	Actie samenvatting De tool inkoopeisen cybersecurity overheid (ICO) wordt doorontwikkeld, verbreed en geïmplementeerd. Inclusief verdere ontwikkeling van overheidsbrede eisensets. Dit zal indirect de markt positief beïnvloeden om veilige producten en diensten te leveren	Tijdlijn 2022-2023	Eigenaar BZK Betrokken CIP, EZK, medeoverheden
II. 1.4.3	Actie samenvatting BZK voert samen met de VNG een verkenning uit naar wat er nodig is om het leveranciersmanagement voor medeoverheden naar een hoger niveau te brengen met aandacht voor integreren van dienstverlening in de inkoopondersteuning en het organiseren van effectief toezicht op leveranciers.	Tijdlijn 2022-2023	Eigenaar BZK Betrokken CIP, EZK, medeoverheden
II.1.4.4	Actie samenvatting Het Centrum voor Informatiebeveiliging en Privacy (CIP) ontwikkelt een pakket aan cybersecurity-eisen en een tool die overheidsorganisaties ondersteunt bij de inkoop van ICT-producten en -diensten. Deze tool wordt verder ontwikkeld en de toepassing wordt bij de overheid gestimuleerd. Tevens zal middels wetgeving worden geborgd dat de normensets voor veilig inkopen ook verplicht worden toegepast door overheden.	Tijdlijn 2022-2026	Eigenaar EZK, BZK Betrokken medeoverheden

Doel II.2: Nederland heeft een sterke cybersecuritykennis- en innovatieketen

II.2.1 Veilige cryptografie

II.2.1.1	Actie samenvatting De productontwikkeling voor high assurance producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid, zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen. Dat gebeurt in nauwe samenwerking met de Nederlandse cryptografische-industrie.	Tijdlijn 2022-2026	Eigenaar BZK Betrokken AIVD, JenV, DEF, EZK, OCW, IenW, privaat, kennis-instellingen.
II.2.1.2	Actie samenvatting In samenwerking met bedrijven en wetenschappelijke instellingen wordt onderzoek uitgevoerd naar de ontwikkeling van moderne en hoogwaardige beveiligingsproducten.	Tijdlijn 2022-2026	Eigenaar BZK Betrokken AIVD, JenV, DEF, EZK, OCW, IenW, private partijen, kennisinstellingen.
II.2.1.3	Actie samenvatting Het kabinet zet meerjarige thematische routekaarten op aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet middels het platform dcypher. Dit is inclusief een routekaart op cryptocommunicatie en voor geautomatiseerd kwetsbaarhedenonderzoek.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken JenV, BZK, DEF, OCW, IenW, private partijen, kennis-instellingen.

II.2.2 Nationale samenwerking kennis- en innovatie-onderzoekssamenwerking

II.2.2.1	Actie samenvatting De interdepartementale cybersecurity kennis- en innovatiebehoefte wordt jaarlijks geïnventariseerd en inzichtelijk gemaakt. Indien nodig wordt hierbinnen geprioriteerd.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken BZK, JenV, OCW, DEF, IenW
II.2.2.2	Actie samenvatting Defensie versterkt de *Cyber Innovation Hub* (CIH) om het innovatieportfolio uit te breiden en de landelijke positie in cybersecurity kennis- en innovatienetwerken te versterken.	Tijdlijn 2022-2024	Eigenaar DEF Betrokken
II.2.2.3	Actie samenvatting NCSC voert onderzoeksactiviteiten uit onder een meerjarige agenda in samenwerking met diverse (kennis)instellingen op diverse domeinen gerelateerd aan de rol van het NCSC en haar doelgroep(en).	Tijdlijn 2022-2026	Eigenaar JenV Betrokken NCSC
II.2.2.4	Actie samenvatting De cybersecurity kennis-en innovatiebehoefte van het bedrijfsleven en kennisinstellingen wordt onderdeel van het Nederlandse Topsectoren Programma.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken Private partijen

II.2.3 Europese onderzoekssamenwerking en fondsen

II.2.3.1

Actie samenvatting
Bij de RVO wordt een Nationaal Coördinatie Centrum (NCC-NL) opgericht als onderdeel van het Europese Netwerk van Cyber Competence Centers (ECCCN).

Tijdlijn
2022-2026

Eigenaar
EZK

Betrokken
BZK, DEF, JenV, OCW, IenW

II.2.3.2

Actie samenvatting
Organisaties uit het dcypher-netwerk worden ondersteund via het Nationaal Coördinatie Centrum (NCC-NL) in de voorbereiding en uitvoering van projecten uit Europese initiatieven en fondsen zoals Digital Europe en Horizon 2020.

Tijdlijn
2022-2026

Eigenaar
EZK

II.2.3.3

Actie samenvatting
Er wordt actief gestuurd op het opnemen van de onderzoeksbehoeften van Nederlandse organisaties in nieuwe werkprogramma's van onder andere Digital Europe en Horizon 2020, hierbij gebruik makend van Nederlandse cybersecurity expertise en innovatiekracht.

Tijdlijn
2022-2026

Eigenaar
EZK

Betrokken
OCW, JenV, BZK, DEF, IenW

Luchthavens proberen zich niet meer enkel te onderscheiden met service en aanbod. Ook digitalisering en data zijn terreinen waarop ze zich snel ontwikkelen. Zowel voor passagiers- als goederenverkeer betekent dit ook dat de afhankelijkheid en mogelijke kwetsbaarheid groeit.

Pijler III
Tegengaan van digitale dreigingen van staten en criminelen

Doel III.1: Nederland heeft zicht op digitale dreigingen van staten en criminelen

III.1.1 Zicht op statelijke actoren

	Actie samenvatting	Tijdlijn	Eigenaar / Betrokken
III.1.1.1	De onderzoekscapaciteit wordt versterkt ten behoeve van inlichtingenmatig-diepteonderzoek waarmee breder zicht ontstaat op de huidige en voorstelbare digitale dreiging.	2022-2026	Eigenaar: BZK, DEF Betrokken: AIVD, MIVD
III.1.1.2	De unieke inlichtingen worden vertaald naar specifiek handelingsperspectief waarmee afnemers zich beter kunnen weren.	2022-2026	Eigenaar: BZK, DEF Betrokken: AIVD, MIVD
III.1.1.3	De mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden voor onderzoeken naar landen met een offensief cyberprogramma worden vergroot. Hiertoe wordt een wetsvoorstel ingediend bij Tweede Kamer.	2022-2026	Eigenaar: BZK, DEF Betrokken: AIVD, MIVD

III.1.2 Onderzoeks- en opsporingscapaciteit cybercriminelen

III.1.2.1	Actie samenvatting Politie en OM zetten, naast strafrechtelijke interventies, met lokaal bestuur en private partners in op het ontwikkelen van niet-strafrechtelijke interventies ter bestrijding van cybercrime, waaronder ransomware.	Tijdlijn 2023-2026	Eigenaar JenV Betrokken Politie, OM, BZK, medeoverheden, BZ
III.1.2.2	Actie samenvatting Er wordt ingezet op het vergroten van kennis en kunde van cybersecurityfenomenen binnen het OM.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken OM
III.1.2.3	Actie samenvatting De KMar en de politie verkennen de mogelijkheden tot verdere samenwerking op het bestrijden van (grensoverschrijdende) cybercriminaliteit.	Tijdlijn 2022-2024	Eigenaar JenV, DEF Betrokken KMar, politie
III.1.2.4	Actie samenvatting Het OM voert een verkenning uit naar de mogelijkheid om middels een ‘fasttrack’ cyberzaken versneld af te doen.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken OM
III.1.2.5	Actie samenvatting De politie stelt jaarlijks een veiligheidsbeeld over cybercrime en gedigitaliseerde criminaliteit op, waarin de belangrijkste criminele fenomenen, werkwijzen en het risico hiervan voor de samenleving geschetst worden. De beelden geven richting aan de keuze van de politie en het OM voor de fenomenen waarop wordt ingezet en de onderzoeken die worden geprioriteerd.	Tijdlijn 2022-2026	Eigenaar JenV Betrokken Politie, OM

III.1.3 Versterken diplomatiek netwerk

III.1.3.1	Actie samenvatting Het aantal cyberdiplomaten en hun taken worden uitgebreid ten behoeve van een versterkte informatiepositie over digitale dreigingen en ontwikkelingen middels gerichte en proactieve rapportages op basis van diplomatieke contacten in derde landen.	Tijdlijn 2022-2026	Eigenaar BZ Betrokken DEF, BZK, JenV
III.1.3.2	Actie samenvatting Versterken van cybercompetentie en -kennis binnen het postennetwerk om cybersecurity beter te integreren in regulier diplomatiek contact en in aanpalende beleidsthema’s.	Tijdlijn 2022-2026	Eigenaar BZ Betrokken DEF, BZK, JenV
III.1.3.3	Actie samenvatting BZ stimuleert in EU- en NAVO-verband betere internationale informatiedeling en gezamenlijke analyse en initieert waar nodig kleinere coalities om het situationeel beeld van digitale dreigingen te versterken.	Tijdlijn 2022-2026	Eigenaar BZ Betrokken DEF, BZK, JenV, NCSC
III.1.3.4	Actie samenvatting Het NCSC start met de uitvoering van het capaciteitsopbouwprogramma internationaal o.a. door het ontwerp van trainingsactiviteiten.	Tijdlijn 2022-2024	Eigenaar JenV Betrokken BZ, NCSC
III.1.3.5	Actie samenvatting Deelnemen van Defensie aan initiatieven op het gebied van cyber, onder meer binnen het Europees Defensiefonds en via PESCO-projecten en het innemen van een conceptueel leidende rol binnen de EU en de NAVO. Internationaal oefenen wordt de norm.	Tijdlijn 2022-2026	Eigenaar DEF Betrokken BZ

Doel III.2: Nederland heeft grip op digitale dreigingen van staten en criminelen

2.1 Attributie en respons

	Actie samenvatting	Tijdlijn	Eigenaar / Betrokken
III.2.1.1	Samen met internationale partners worden nieuwe en effectievere opties voor diplomatieke respons op cyberdreigingen ontwikkeld. Bestaande kaders en instrumenten, zoals het interdepartementale diplomatiek responskader bij cyberincienten, de *EU Cyber Diplomacy Toolbox* en de *NATO Guide* worden doorontwikkeld. Dit vindt plaats in samenhang met het Rijksbreed Responskader voor Statelijke Dreigingen.	2022-2026	Eigenaar: BZ Betrokken: DEF, BZK, JenV, AIVD, MIVD, NCSC
III.2.1.2	Nederland neemt het initiatief voor kleinere landencoalities om specifieke incidenten of dreigingen te adresseren en beleidsvorming binnen de EU en NAVO op het gebied van (diplomatieke) respons en attributie te stimuleren.	2022-2026	Eigenaar: BZ Betrokken: DEF, BZK, JenV, NCSC

III.2.2 Defensieve en offensieve cybercapaciteiten

	Actie samenvatting	Tijdlijn	Eigenaar / Betrokken
III.2.2.1	Defensie investeert in zijn gehele keten van cybercapaciteiten, onder meer via het structureel borgen en vergroten van *Cyber Rapid Respons Teams* (CRRT's) en *Cyber Missie Teams* (CMT's) en het vergroten van de personele gereedheid via opleiding, training en oefening.	2022-2026	Eigenaar: DEF Betrokken: BZ
III.2.2.2	Defensie breidt bijstandsconstructies uit om andere organisaties te kunnen helpen bij grootschalige incidenten. Onder andere via het Nationaal Response Netwerk (NRN).	2022-2026	Eigenaar: DEF Betrokken: JenV
III.2.2.3	Verkenning naar de mogelijkheden, en implementatie van actieve cyberverdedigingsmaatregelen in het kader van implementatie van NIB2 en het (tijdelijk) laten blokkeren van malafide verkeer door Nederlandse Internet Service Providers met de benodigde juridische waarborgen in het kader van nationale risicomitigatie, tegengaan van meer slachtoffers en dreiging te verminderen.	2023-2024	Eigenaar: JenV Betrokken: EZK, BZK, DEF, NCSC, AIVD, MIVD, BZ

Doel III.3: Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte

III.3.1 Normatief kader

III.3.1.1	Actie samenvatting Het VN normatief kader in cyberspace wordt verstevigd en bestendigd binnen onderhandelingen in multilaterale fora middels effectieve inzet op Nederlandse prioriteiten, waaronder bescherming van de kernfunctionaliteit van het internet en het multi-stakeholdermodel voor het beheer van het internet.	Tijdlijn 2022-2026	Eigenaar BZ Betrokken DEF, EZK, JenV, BZK
III.3.1.2	Actie samenvatting De naleving en uitvoering van het VN normatief kader wordt bevorderd door bij te dragen aan de totstandkoming van het Program of Action als implementatiemechanisme. Het kabinet is transparant over de implementatie van het normatief kader in Nederland.	Tijdlijn 2022-2026	Eigenaar BZ Betrokken DEF, JenV, EZK, BZK

III.3.2 Internet governance

III.3.2.1	Actie samenvatting Deelname van de Nederlandse multi-stakeholdergemeenschap aan het internationale debat wordt bevorderd (incl. een vergelijkbare inzet van de EU voor de Europese multi-stakeholdergemeenschap) om met een sterker geluid een open, vrij en veilig internet te bepleiten.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken BZ
III.3.2.2	Actie samenvatting Er vindt actieve deelname plaats aan de internationale discussies over technische internetstandaarden en andere technische standaarden die van invloed zijn op de openheid, vrijheid en veiligheid van het internet door standpunten te coördineren op EU-niveau en met gelijkgezinde landen.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken BZ
III.3.2.3	Actie samenvatting Multistakeholder organisaties dienen effectiever te worden in het erkennen en adresseren van maatschappelijke en technische uitdagingen met betrekking tot internet governance. Zodat sneller tot een consensus of beslissing gekomen wordt ten aanzien van oplossingen van deze uitdagingen. Het kabinet wil dit bevorderen door zelf actief deel te nemen aan de discussie, gelijkgestemde landen stimuleren hun presentie te vergroten en door de uitkomsten van de discussies binnen ICANN in het Internet Governance Forum en de EU te agenderen.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken BZ

Toenemende digitalisering biedt het onderwijs veel kansen, bijvoorbeeld door het aanbieden van online colleges en voor het ontsluiten van kennis. Tegelijkertijd brengt deze grotere afhankelijkheid van technologie risico's met zich mee. Verschillende universiteiten zijn de laatste jaren doelwit van ransomware geweest.

Pijler IV
Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Doel IV.1: Burgers zijn goed beschermd tegen digitale risico's.

IV.1.1 Voorlichtingscampagnes

	Actie samenvatting	Tijdlijn	Eigenaar / Betrokken
IV.1.1.1	JenV, EZK, BZK organiseren doelgroepspecifieke voorlichtingscampagneprogramma's cyberveiligheid gericht op de cybersecurity basismaatregelen. Er vindt een effectmeting plaats na elke campagne. De campagnes worden georganiseerd in samenwerking met gemeenten voor optimale inzet van de beschikbare gemeentelijke communicatiekanalen.	2022-2026	Eigenaar JenV, EZK, BZK Betrokken Medeoverheden
IV.1.1.2	In het kader van de City Deal Cybercrime[3] worden pilotprojecten uitgevoerd met als doel de weerbaarheid van burgers en bedrijven tegen cybercrime te vergroten. De pilots zijn gericht op meer integraliteit om lokale best practices beter en breder te benutten zodat kan worden toegewerkt naar een landelijk dekkend ondersteuningsaanbod.	2022- 2023	Eigenaar BZK, JenV Betrokken Medeoverheden
IV.1.1.3	De jaarlijkse cybersecurity bewustwordingsmaand Alert Online met het partnernetwerk wordt structureel georganiseerd in oktober.	2022	Eigenaar EZK, JenV Betrokken BZK

3 Samenwerking tussen J&V en gemeenten op het gebied van cybercrime.

IV.1.2 Beveiligingsadvies burgers

IV.1.2.1	Actie samenvatting De Informatiepunten Digitale Overheid worden gefaciliteerd om hulpvragen van burgers op het terrein van cyberveiligheid te beantwoorden en waar nodig door te verwijzen naar bestaande steunpunten, informatieloketten en lokale ondersteuningsinitiatieven van private partners.	Tijdlijn 2022	Eigenaar BZK Betrokken
IV.1.2.2	Actie samenvatting Het publiek-private veiliginternetten.nl wordt doorontwikkeld en verbreed als de centrale vindplaats voor cybersecurity-informatie en handelingsperspectief voor burgers.	Tijdlijn 2022-2023	Eigenaar EZK Betrokken BZK
IV.1.2.3	Actie samenvatting Het cyberweerbericht wordt periodiek opgesteld en gepubliceerd. Na twee jaar vindt een effectiviteitsevaluatie plaats.	Tijdlijn 2022-2024	Eigenaar JenV Betrokken EZK

IV.1.3 Betrouwbaarheid digitale overheidsvoorzieningen

IV.1.3.1	Actie samenvatting De overheid zet in op een uniforme domeinnaamextensie, zodat burgers gemakkelijk kunnen herkennen of zij online echt te maken hebben met een overheid of niet. Dit helpt online fraude als phishing tegen te gaan.	Tijdlijn 2022-2026	Eigenaar BZK
IV.1.3.2	Actie samenvatting Ter verbetering van de herkenbaarheid van de overheid op het internet wordt gewerkt aan de ontwikkeling van een “register internetdomeinen overheid”, zodat burgers via dit register een snelle check kunnen doen of internetdomeinen van de overheid zijn of niet. Bij onduidelijkheden over de echtheid van websites kunnen burgers terecht bij een contactpunt.	Tijdlijn 2022-2023	Eigenaar BZK

Doel 2: Burgers reageren snel en adequaat op cyberincidenten.

IV.2.1 Melding of aangifte doen van cybercrime fenomenen

IV.2.1.1	Actie samenvatting De politie maakt vanaf 2023 voor meer cybercrime fenomenen het mogelijk om online melding of aangifte te doen.	Tijdlijn 2023	Eigenaar JenV Betrokken Politie

Doel IV.3: Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid.

IV.3.1 Curriculum

	Actie samenvatting	Tijdlijn	Eigenaar
IV.3.1.1	Stichting Leerplan Ontwikkeling (SLO) heeft de opdracht gekregen om samen met het onderwijsveld concrete kerndoelen voor de basisvaardigheden te ontwikkelen waarvan digitale veiligheid deel uitmaakt. Deze opdracht voeren ze uit voor zowel het PO als het VO. De aangescherpte kerndoelen voor het PO en het VO in 2025 in een wetsvoorstel aan de Tweede Kamer voorgelegd.	2022-2025	OCW
IV.3.1.2	Het 'masterplan basisvaardigheden' wordt opgezet dat ervoor moet zorgen dat de leraar goed toegerust is om het beste onderwijs te geven in taal, rekenen/wiskunde, burgerschap en digitale geletterdheid. Met de ingang van het schooljaar 2022-2023 zullen de eerste scholen hiermee beginnen.	2022- 2026	OCW

Doel IV.4: De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts.

IV.4.1 Cybersecurity arbeidsmarkt

	Actie samenvatting	Tijdlijn	Eigenaar
IV.4.1.1	Onderwijsinstellingen werken aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Daartoe werken zij samen met het bedrijfsleven en andere relevante partijen. Hierbij worden o.a. knelpunten en beperkingen in die samenwerking voortvloeiend uit regelgeving geïnventariseerd en bezien welke oplossingen daarvoor nodig zijn.	2022-2026	OCW Betrokken OCW, onderwijsinstellingen en werkgevers
IV.4.1.2	Er wordt geïnvesteerd in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zij-instroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt. Het doel van deze maatregel is om de arbeidsmarkttekorten in te perken.	2023-2029	OCW Betrokken Hogescholen

IV.4.1.3	Actie samenvatting Afhankelijk van definitief advies van een onafhankelijke commissie waarover eind september/begin oktober 2022 uitsluitsel zal komen, wordt voor een aantal specifieke onderwerpen in het WO vanuit de sectorplannen geïnvesteerd in cybersecurity. Het doel van deze middelen is om samenwerking te stimuleren. Universiteiten maken per sector/domein een analyse waarin zij de kansen en knelpunten op gebied van onderzoek en onderwijs in kaart brengen, en voorstellen doen voor maatregelen om hierop in te spelen. In het ingediende sectorplan Techniek wordt ook aandacht besteed aan cybersecurity. Via deze weg zullen ook de universitaire cybersecurity opleidingen profiteren.	Tijdlijn 2023-2026	Eigenaar OCW Betrokken Universiteiten
IV.4.1.4	Actie samenvatting De kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt worden onderzocht, inclusief aanbevelingen hoe deze tekorten aan te pakken.	Tijdlijn 2023	Eigenaar EZK Betrokken OCW, JenV, werkgevers, CBS, Universitaire Commissie voor Wetenschapsbeoefening.
IV.4.1.5	Actie samenvatting Verkend wordt of de initiatieven voor inzicht in ICT- brede tekorten en de ontwikkeling van een onderwijs en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity specialisten.	Tijdlijn 2023-2024	Eigenaar EZK Betrokken OCW, SZW, BZK

IV.4.1.6	Actie samenvatting Het kabinet zet zich via de *Human Capital Agenda ICT* in om de instroom van cybersecurityspecialistenICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken
IV.4.1.7	Actie samenvatting Via thematische routekaarten en communities worden gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.	Tijdlijn 2022-2026	Eigenaar EZK Betrokken Dcypher

Oktober 2022

Deze publicatie is een uitgave van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) namens de Rijksoverheid.
info@nctv.minjenv.nl