26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1349 Brief van de minister en staatssecretaris van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 juni 2025

Hierbij ontvangt u, mede namens de minister van Asiel en Migratie, de antwoorden op de door uw Kamer gestelde schriftelijke vragen over het Jaarverslag en Slotwet van het ministerie van Justitie en Veiligheid 2023 (Kamerstuk 36 740-VI, nr. 1,3 en 4) en het rapport Resultaten verantwoordingsonderzoek 2023 bij het ministerie van Justitie en Veiligheid (Kamerstuk 36 740-VI, nr. 2).

Het betreft hierbij de antwoorden op de vragen die zijn gesteld door de Commissie Justitie en Veiligheid, door de commissie Digitale Zaken en de vragen die gesteld zijn door de V100.

De minister van Justitie en Veiligheid,
D.M. van Weel

De staatssecretaris van Justitie en Veiligheid,
T.H.D. Struycken

V-100 (26 mei 2025) – Vragen over het National Cyber Security Center (NCSC)

Aan de minister van Justitie en Veiligheid

Vraag (1):
Kunt u aangeven wat u ziet als de taken van het NCSC? Welke zijn af te leiden uit de Cyberbeveiligingswet (Cbw)? En welke komen uit beleidsbrieven dan wel de Nederlandse Cybersecuritystrategie (NLCS)? En welke zijn afkomstig van een andere bron? Kan u hiervan een limitatieve opsomming geven?

Antwoord:
In het kader van de Nederlandse Cybersecurity Strategie (NLCS) en het onderliggende actieplan voert het NCSC verschillende taken uit waaronder, maar niet uitsluitend, de oprichting van het publiek-private informatiedelingsplatform Cyclotron en het ontwikkelen van het Cyberweerbaarheidsnetwerk.
Als uitvoeringscoördinator werkt het NCSC aan een Nederlands cybersecuritystelsel dat optimaal functioneert. Met een brede set (publieke en private) partners werkt het NCSC gecoördineerd samen met als doel alle organisaties in Nederland in staat te stellen om hun weerbaarheidsniveau en digitale slagkracht te verhogen.
Op dit moment regelt de Wet beveiliging netwerk- en informatiesystemen (Wbni) de wettelijke taken van het NCSC op het terrein van cybersecurity. Per 1 januari 2026 zal het NCSC voor de minister van Economische Zaken ook de wettelijke taken op grond van de Wet bevordering digitale weerbaarheid bedrijven uitvoeren. Op het moment dat de Cyberbeveiligingswet (Cbw) in werking treedt zal de Wbni worden ingetrokken en zal het NCSC de taken uit de Cbw uitvoeren.

Vraag (2):
Kunt u aangeven hoeveel fte voor alle taken, inclusief de wettelijke taak, uit de Cbw beschikbaar is per onderdeel en activiteit, en welke budgetten uit welke begrotingen daaraan gekoppeld zijn?

Antwoord:
Bij het NCSC werken momenteel ruim 500 medewerkers. Dat zijn medewerkers in vaste dienst, met een tijdelijk contract, en extern ingehuurde medewerkers. Alle medewerkers dragen direct of indirect bij aan de wettelijke taken en de maatschappelijke opgave van het NCSC. Vanwege de samenhang van de werkzaamheden is het onmogelijk om een onderscheid te maken op het niveau van individuele taken of activiteiten.
Het NCSC wordt voor een belangrijk deel gefinancierd uit de begroting van JenV. Daarnaast dragen andere departementen als opdrachtgevers van overige (wettelijke) taken (zie ook antwoord op vraag 3) bij aan de financiering van het NCSC.

Vraag (3):
Kunt u inzicht geven in wie de opdrachtgevers van NCSC zijn, welke opdrachten er jaarlijks verstrekt worden, en uit welke begrotingen dit betaald wordt? Kunt u een meerjarig overzicht geven vanaf 2022 (ingangsdatum NLCS)?

Antwoord:
De situatie rondom de aansturing van het NCSC verloopt sinds het huidige jaar (2025) middels het ‘meervoudig opdrachtgeverschap’.
Dit betekent dat meerdere ministeries op hun eigen beleidsterrein een opdracht

verlenen aan het NCSC. Voorheen was *het Ministerie van Justitie en Veiligheid* via de *Nationaal Coördinator Terrorismebestrijding en Veiligheid* (NCTV) de enige opdrachtgever. Sinds 2025 is het 'Ministerie van Justitie en Veiligheid' via de *Nationaal Coördinator Terrorismebestrijding en Veiligheid* (NCTV) 'coördinerend opdrachtgever' en zijn de ministeries van: '*Financiën', 'Binnenlandse zaken en Koninkrijksrelaties', 'Economische Zaken', 'Landbouw, Visserij, Voedselzekerheid en Natuur', 'Infrastructuur en Waterstaat'* en *'Klimaat en Groene Groei'* mede-opdrachtgevers voor het NCSC.
De opdrachtgevers formuleren jaarlijks gezamenlijk een opdracht aan het NCSC (de jaarplanaanschrijving) waarin staat wat ze van het NCSC verwachten. De uitvoering van deze opdrachten wordt betaald vanuit de begroting van het NCSC die bestaat uit de financiële middelen die de opdrachtgevers aan het NCSC verstrekken voor het uitvoeren van de gegeven opdracht.

Vraag (4):
Kunt u uitleggen waarom er niet voor gekozen is het NCSC aan te wijzen als wettelijke nationale Computer Security Incident Response Team (CSIRT)?

Antwoord:
Juridisch gezien kent de NIS-2 richtlijn, en daarmee de Cyberbeveiligingswet (cbw), de term nationale CSIRT niet. Het NCSC vervult wel een rol die beleidsmatig gezien kan worden als de nationale CSIRT, zo is het operationeel coördinerend over het cybersecuritystelsel, bevordert en faciliteert samenwerking, coördineert de afhandeling van (bijna) incidenten en kwetsbaarheden op nationaal niveau. Ook is er het voornemen om het NCSC, onder de Cbw, de taak van coördinator voor de bekenmaking van kwetsbaarheden te laten uitvoeren. Daarnaast zijn er CSIRTS die onder andere sectorspecifieke kennis met zich meebrengen, en naar waarschijnlijkheid onder de Cbw, voor die specifieke sectoren de CSIRT taak uitvoeren.

Vraag (5):
Hoe zorgt u ervoor dat het NCSC voldoende is toegerust (in capaciteit en middelen) om voornoemde taken te kunnen uitvoeren en de toegenomen doelgroepen te kunnen blijven bedienen?

Antwoord:
Het NCSC krijgt naar aanleiding van de uitbreiding van de doelgroepen onder de Cbw een opdracht van verschillende departementen de benodigde middelen om deze opdracht uit te voeren. Met deze middelen kan het NCSC haar taak om Nederland digitaal veilig te houden voor haar doelgroepen uitvoeren. Daarnaast zal het vernieuwde NCSC, na de integratie van het NCSC en het Digital Trust Center, de taken uit de Wet bevordering digitale weerbaarheid gaan uitvoeren (de verantwoordelijkheid blijft bij de minister van Economische Zaken) waarmee de doelgroep verder wordt uitgebreid naar de niet vitale bedrijven.

Vraag (6):
Kunt u reflecteren op de omslag van cybersecurity naar digitale weerbaarheid? En wat de gevolgen daarvan zijn voor de taakopvatting van het NCSC?

Antwoord:
Met de publicatie van de Nederlandse Cybersecuritystrategie in 2022 wordt gekeken naar digitale veiligheid in het brede ecosysteem. Het NCSC vergroot de digitale weerbaarheid door te begrijpen, verbinden en voorkomen. Daarnaast

beogen de genoemde integratie en de Cbw de slagkracht van het vernieuwde NCSC te verhogen en zo de digitale weerbaarheid van alle organisaties in Nederland te versterken.

Vraag (7):
Kunt u aangeven met welke stakeholders het NCSC en het Digital Trust Center (DTC) in contact zijn, onder andere via de relatiemanagers, zoals brancheorganisaties, samenwerkingsverbanden, medeoverheden en private organisaties? En blijft dit netwerk intact of wordt dit netwerk vergroot na de invoering van de Cbw?

Antwoord:
Samenwerking tussen publieke en private organisaties is essentieel in het vergroten van de digitale weerbaarheid. De verwachting is dat dit netwerk de komende jaren, mede vanwege de ambities van het kabinet zoals beschreven in de Nederlandse Cybersecurity Strategie (NLCS), verder zal groeien. Het NCSC heeft hierin de rol als uitvoeringscoördinator en zorgt hiermee voor de groei van het netwerk en de juiste randvoorwaarden en binnen de beschikbare financiële middelen. Met betrekking tot de Cbw is er een publiek-privaat NIS2-overleg actief met vertegenwoordigers uit de overheid en diverse brancheorganisaties. Ieder vakdepartement en uitvoeringsorganisatie is verantwoordelijk voor het informeren en activeren van hun eigen sector en achterban.

Vraag (8):
Kunt u aangeven op welke wijze stakeholders input kunnen geven op de beleidsbrieven?

Antwoord:
Om in te kunnen spelen op trends, actuele dreigingen en risico’s kan het actieplan van de Nederlandse Cybersecuritystrategie (NLCS) jaarlijks worden geactualiseerd. Mogelijke aanleidingen voor de bijstelling van het actieplan is bijvoorbeeld het jaarlijkse Cybersecuritybeeld Nederland (CSBN) wat een actueel beeld geeft van de digitale dreiging in Nederland. Daarnaast kunnen inzichten van publieke, private- en wetenschapspartijen ook reden zijn voor bijsturing. Zij worden jaarlijks betrokken bij een toets of zij ontwikkelingen zien die aanleiding kunnen vormen voor bijstelling. Dit kan daarnaast verwoord zijn in nationale dan wel internationale rapporten of adviezen die gedurende de looptijd van de NLCS worden uitgebracht. Tot slot wordt de Cyber Security Raad (CSR) jaarlijks om advies gevraagd over strategische ontwikkelingen die volgens hen meegewogen moeten worden.

Vraag (9):
Kunt u aangeven hoe de kwaliteit van de dienstverlening van het NCSC zich heeft ontwikkeld? En moet gaan ontwikkelen onder de Cbw? Welke lessen trekt u daaruit?

Antwoord:
De dienstverlening van het NCSC ontwikkelt zich doorlopend. Daarbij speelt wetgeving, zoals Cbw, een belangrijke rol. Bijvoorbeeld omdat het aantal organisaties waarvoor het NCSC-producten en diensten levert een vlucht neemt door nieuwe wetgeving. Het NCSC werkt daarom aan producten en diensten die schaalbaar zijn en beter aansluiten op de meer diverse behoeften van organisaties. Denk hierbij aan het maken van andere producten voor een grootbedrijf met een volwassen eigen cybersecurityafdeling en aan de andere kant

een mkb-bedrijf dat afhankelijk is van lokale of regionale leveranciers. Dit doet zij waar mogelijk ook samen met het Digital Trust Center. In toenemende mate gebruikt het NCSC-input van zijn doelgroepen om producten en diensten verder te ontwikkelen. Zoals benoemt zet het NCSC in op schaalbare dienstverlening en uitbreiding van capaciteit.

Vraag (10):
Hoe kan de NCSC wendbaarder aangestuurd worden op basis van prangende vraagstukken zoals rond het thema digitale autonomie?

Antwoord:
De opdrachtgevers van het NCSC schrijven jaarlijks gezamenlijk een opdracht aan het NCSC, middels een jaarplanaanschrijving, waarin staat wat ze van het NCSC verwachten. Met deze jaarplanaanschrijving wordt het NCSC in staat gesteld om de taken en opgave waar de organisatie voor staat adequaat te kunnen uitvoeren. Regelmatig wordt daarnaast tussen opdrachtgevers en het NCSC gesproken over deze opdracht in de zogenoemde opdrachtgevers-opdrachtnemersoverleggen. Zowel via de jaarplanaanschrijving als via de opdrachtgever- en opdrachtnemeroverleggen kan het NCSC worden (bij)gestuurd op prangende vraagstukken.

Vraag (11):
Hoe ondersteunt u het NCSC bij het toegankelijk houden van haar dienstverlening richting alle doelgroepen, met name richting het mkb en de kleine ondernemer?

Antwoord:
Na het samenvoegen van het Nationaal Cyber Security Centrum, het Digital Trust Center en het Cyber Security Incident Response Team voor digitale diensten (CSIRT-DSP) is het informeren, adviseren en ondersteunen van alle organisaties in Nederland - groot of klein, publiek of privaat en vitaal of niet-vitaal- een integraal onderdeel van de dienstverlening van het vernieuwde NCSC. Daarbij staat het bereiken van impact bij de verschillende doelgroepen van het NCSC voorop, ook richting mkb en kleine ondernemers.

Vraag (12):
Hoe ondersteunt u de wens uit het veld om één loket te hebben voor het melden en oplossen van digitale incidenten?

Antwoord:
De NLCS is het strategisch kader waarbinnen het Nederlandse cybersecuritystelsel wordt ingericht. Daarin is opgenomen dat het NCSC zich zal zich doorontwikkelen tot het nationaal Cyber Security Incident Response Team (CSIRT). Het Nationaal Cyber Security Centrum, het Digital Trust Center en het Cyber Security Incident Response Team voor digitale diensten (CSIRT-DSP) worden samengevoegd tot één nationale cyberautoriteit.
Daarnaast wordt er meer samenhang gecreëerd tussen bestaande schakelorganisaties door integratie, waar nuttig, te stimuleren. Voor alle bestaande sectorale Computer Emergency Response Teams (CERT’s) en CSIRT’s wordt daarom door de Rijksoverheid verkend in hoeverre meer samenwerking, samenhang of samenvoeging met het NCSC toegevoegde waarde heeft. Nieuwe CSIRT’s ontstaan in principe alleen daar waar dit toegevoegde waarde heeft en waarvoor financiële middelen beschikbaar zijn.

Vraag (13):
Hoe ondersteunt u de wens uit het veld voor nazorg na een incident?

Antwoord:
Het NCSC biedt ondersteuning bij het herstel van cyberincidenten, onder meer door middel van het actief delen van *lessons learned*, richtlijnen en informatie. Het NCSC deelt breed toegankelijke kennis- en adviesproducten, zoals de publicaties ‘Herstel van een cyberincident’ en ‘Continuïteit van diensten’.

Vraag (14):
Kunt u aangeven of de uitbreiding van het mandaat van het NCSC voldoende is om informatie te delen met niet-NIS2 geregistreerde partijen?

Antwoord:
Met de Cyberbeveiligingswet krijgen alle CSIRT’s, waaronder het NCSC, de juridische grondslag om informatie te delen met relevante partijen. Dit hoeven geen NIS-2 partijen te zijn. De aard van de informatie bepaald mede of een partij relevant is.

Vraag (15):
Op welke wijze gaat u de wildgroei aan partijen die pretenderen een keurmerk te zijn te lijf?

Antwoord:
Zelfregulering kan onder de juiste randvoorwaarden bijdragen aan het behalen van een maatschappelijk doel, maar een keurmerk heeft geen zelfstandige status in relatie tot het voldoen aan de wettelijke vereisten. Iedereen kan een keurmerk starten, hierin zijn ook verschillende gradaties. Maar het is aan de toezichthouder om te bezien of een entiteit aan de wet voldoet. Er wordt vanuit de overheid geen uitspraak gedaan over dit soort initiatieven. Organisaties blijven zelf verantwoordelijk voor het implementeren van de Cyberbeveiligingswet en het staat het vrij een externe partij hiervoor in te huren. Vanuit de overheid worden voorafgaand aan de inwerkingtreding van de Cyberbeveiligingswet wel verschillende handreikingen opgesteld die partijen kunnen helpen bij het voldoen aan de vereisten uit (de zorgplicht) van de Cyberbeveiligingswet. Deze handreikingen hebben geen juridische status en zijn bedoeld als hulpmiddel.

Vraag (16):
Hoe waarborgt u dat de toetsende instanties in staat worden gesteld om de onafhankelijkheid van keurmerken te waarborgen?

Antwoord:
De toezichthoudende instanties zullen de implementatie van de Cyberbeveiligingswet bij entiteiten beoordelen, en zullen daarbij de vereisten uit de wet nalopen en beoordelen. De toezichthouder kan bij zijn oordeel of een entiteit aan de wet voldoet al dan niet rekening houden met een keurmerk, maar een keurmerk heeft geen zelfstandige status in relatie tot het voldoen aan de wettelijke vereisten.