Fiche 2: Verordening cyberbeveiliging van instellingen, organen en instanties van de Europese Unie

1. Algemene gegevens

a) Titel voorstel

Voorstel voor een verordening van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie

b) Datum ontvangst Commissiedocument

22 maart 2022

c) Nr. Commissiedocument

COM(2022) 122

d) *EUR-lex*

EUR-Lex - 52022PC0122 - EN - EUR-Lex (europa.eu)

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

Niet opgesteld

f) Behandelingstraject Raad

Raad Algemene Zaken

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid

h) Rechtsbasis

Artikel 106bis van het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie (Euratom-verdrag)
Artikel 298 van het Verdrag betreffende de werking van de Europese Unie (VWEU)

i) Besluitvormingsprocedure Raad

Gekwalificeerde meerderheid

j) Rol Europees Parlement

Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 22 maart 2022 heeft de Commissie een voorstel gepubliceerd voor een verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en

instanties van de Europese Unie (hierna: EU IAO's) (hierna: het voorstel). Dit voorstel bouwt voort op de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[1].

Met dit voorstel wordt een kader ingericht voor gemeenschappelijke voorschriften en maatregelen voor cyberbeveiliging binnen de EU IOA's. Het voorstel beoogt de digitale weerbaarheid van alle EU IOA's te verhogen en incidentbestrijdingscapaciteiten te versterken. De Commissie constateert dat er grote verschillen zijn in de mate van cyberbeveiliging tussen de verschillende EU IOA's. Tegelijkertijd bestaat er momenteel nog geen Uniewetgeving gericht op de cyberbeveiliging van de EU IOA's en het aanpakken van de dreigingen op het gebied van cyberbeveiliging en de uit de digitalisering voortvloeiende nieuwe ICT-risico's. Dit voorstel beoogt daaraan tegemoet te komen.

Het voorstel richt zich ten eerste op verplichtingen voor de EU IOA's tot het opzetten van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's; ten tweede op verplichtingen voor de EU IOA's inzake risicobeheer en rapportage op het gebied van cyberbeveiliging; en als laatste op voorschriften inzake de organisatie en werking van het cyberbeveiligingscentrum voor de EU IOA's (Computer Emergency Response Team voor EU IOA's, hierna: CERT-EU) en een interinstitutionele raad voor cyberbeveiliging (IICB).

In het voorstel wordt gespecificeerd aan welke eisen op gebied van cyberbeveiliging de EU IOA's moeten voldoen. Zij worden onder andere verplicht tot het opstellen van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's, met supervisie van het hoogste managementniveau en passende financiële dekking. Ook moeten de EU IOA's een eigen basisniveau voor cyberbeveiliging vaststellen met een aantal concrete domeinen en maatregelen waar in het voorstel naar wordt verwezen. Daarnaast moeten de EU IOA's ten minste om de drie jaar een maturiteitsbeoordeling[2] van hun cyberbeveiliging uitvoeren. Op basis daarvan moeten maatregelen worden genomen die worden neergelegd in een cyberbeveiligingsplan.

Daarnaast ziet het voorstel op de oprichting en taken van het IICB. De IICB zal verantwoordelijk zijn voor: het toezicht op de uitvoering van deze verordening door de EU IOA's; het toezicht op de uitvoering van de algemene prioriteiten en doelstellingen door CERT-EU en het geven van strategische leiding aan CERT-EU. De IICB kan in het kader van het toezicht op de naleving van de verordening door de EU IOA's niet-bindende waarschuwingen geven en audits aanbevelen, indien blijkt EU IOA's het voorstel of hetgeen daaruit voortvloeit niet doeltreffend toepassen.

Het voorstel vormt CERT-EU om van computercrisisteam tot het autonome IICB voor de EU IOA's, conform de ontwikkelingen in de lidstaten en wereldwijd, waar veel CERT's worden omgedoopt tot

[1] BNC-fiche Gezamenlijke Mededeling EU-strategie inzake cyberbeveiliging, Kamerstuk 22 112, nr. 3052.

[2] De maturiteitsbeoordeling zal het volwassenheidsniveau van de EU IOA toetsen en daarbij onder andere aandacht besteden aan de IT-omgeving ter plekke, uitbestede activa en diensten gehost door derden, mobiele apparatuur, bedrijfsnetwerken, zakelijk netwerken die niet met het internet verbonden zijn en de met de IT-omgeving verbonden apparaten.

cyberbeveiligingscentra; de korte naam 'CERT-EU' blijft vanwege de herkenbaarheid evenwel behouden. Bepaald wordt dat CERT-EU voor EU IOA's met de volgende taken zal worden belast: ten eerste het ondersteunen van EU IOA's bij de uitvoering van de verordening en het bijdragen aan de coördinatie van de toepassing van de verordening; ten tweede ondersteuning van EU IOA's met het aanbieden van zogenaamde basisniveaudiensten; ten derde het onderhouden van een relevant internationaal netwerk; ten vierde het bij de IICB onder de aandacht brengen van kwesties betreffende de uitvoering van de verordening en van de uitvoering van richtsnoeren, aanbevelingen en oproepen tot actie; en ten vijfde het uitbrengen van verslag over de cyberdreigingen waaraan de EU IOA's blootstaan. Voorts krijgt CERT-EU onder andere de bevoegdheid tot het delen van informatie met nationale instanties van lidstaten en tot het samenwerken met derde landen.

Tot slot stelt het voorstel kaders voor samenwerking en verslagleggingsverplichtingen voor CERT-EU en de EU IOA's. Voor de EU IOA's komt onder meer de verplichting te gelden om significante cyberdreigingen[3], kwetsbaarheden of incidenten binnen 24 uur na ontdekking hiervan te delen met CERT-EU. In gerechtvaardigde gevallen en in overeenstemming met CERT-EU kunnen de EU IOA's van die termijn afwijken. Laatstgenoemde instantie dient maandelijks een verslag in bij het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA)[4]. Ook wordt bepaald dat CERT-EU de respons coördineert tussen de EU IOA's in geval van grootschalige cyberaanvallen, door het faciliteren van informatie-uitwisseling over dreigingen, kwetsbaarheden en incidenten, om zo bij te dragen aan consequente externe communicatie, wederzijdse bijstand, optimaal gebruik en efficiëntie bij het inzetten van operationele middelen en de coördinatie met andere crisisresponsmechanismen op Unieniveau. Voorts wordt onder andere de eis gesteld dat alle contacten met CERT-EU die door nationale veiligheids- en inlichtingendiensten worden geïnitieerd of beoogd, onverwijld aan de Commissie en de voorzitter van de IICB worden meegedeeld. Tot slot wordt de mogelijkheid gecreëerd dat deskundigen in dienst van de EU IOA's lidstaten bijstaan in geval van een grootschalige aanval.

Parallel aan dit voorstel heeft de Commissie het voorstel gepubliceerd genaamd het Voorstel voor een verordening van het Europees Parlement en de Raad betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie. Het kabinet informeert de Tweede Kamer hierover in een apart BNC-fiche.

[3] Volgens de definitie van artikel 3, elfde lid van het voorstel is een 'significante cyberdreiging' een 'cyberdreiging met de bedoeling, de gelegenheid en het vermogen om een significant incident te veroorzaken'.
[4] ENISA heeft krachtens de Verordening tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging onder andere tot taak het verzamelen van relevante informatie met het oog op de analyse van bestaande en nieuwe risico's en, in het bijzonder op Europees niveau, risico's die gevolgen hebben voor de veerkracht en de beschikbaarheid van elektronische-communicatienetwerken en voor de authenticiteit, integriteit en vertrouwelijkheid van de informatie die via deze netwerken toegankelijk wordt gemaakt en wordt verzonden.

b) Impact assessment Commissie

Het onderhavige voorstel heeft gevolgen voor de EU IOA's. Aangezien het voorstel enkel van toepassing is op EU IOA's en niet direct van toepassing is op de lidstaten, heeft geen specifieke effectbeoordeling plaatsgevonden. Het kabinet kan zich hier in vinden.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het versterken van de digitale weerbaarheid is een prioriteit voor het kabinet. De uitwerking van de Nederlandse cyberbeveiligingsaanpak is vastgelegd in de Nederlandse Cyber Security Agenda (NCSA[5]). Momenteel werkt het kabinet aan een herziening hiervan in de vorm van een nieuwe Nederlandse Cybersecuritystrategie (NLCS). Nederland heeft als open en internationaal georiënteerde economie belang bij een stabiel, veilig en vrij toegankelijk cyberdomein en een hoog niveau van digitale weerbaarheid in Nederland, de EU en breder internationaal. Het kabinet zet zich hier samen met haar internationale partners voor in, waarbij de kansen die digitalisering onze economie en samenleving biedt volop worden benut, dreigingen het hoofd wordt geboden, cybercriminaliteit wordt bestreden en fundamentele rechten en waarden worden beschermd.

Het Cybersecuritybeeld Nederland 2021[6] laat zien dat de digitale risico's onverminderd groot zijn. Gezien het inherente grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging is Europese en internationale samenwerking voor het kabinet van groot belang. Het kabinet zet zich daarom actief in bij de verschillende Europese gremia[7] die tot doel hebben de digitale weerbaarheid in de EU te vergroten.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet herkent het door de Commissie geschetste beeld dat de digitale dreiging de laatste jaren alleen maar is toegenomen. Dit beeld is mede bevestigd door de hack op het in Nederland gevestigde Europese Geneesmiddelenbureau in 2020.[8] Ook de Europese Rekenkamer concludeert in een verslag van maart 2022 dat het paraatheidsniveau van de EU IOA's over het algemeen niet in verhouding staat tot de dreiging.[9] Het kabinet onderschrijft dan ook de door de Commissie geschetste noodzaak tot het verbeteren van de weerbaarheid en de responscapaciteit bij incidenten van de EU IOA's en verwelkomt de aandacht van de Commissie voor de cyberbeveiliging van de EU IOA's.

Een hoog niveau van cyberbeveiliging van de EU IOA's is ook voor Nederland zelf van direct belang. De burger, het bedrijfsleven en de Nederlandse overheid moeten er ten eerste van op aan kunnen dat de netwerk- en informatiesystemen van de verschillende EU IOA's voldoende beveiligd

[5] Nationale Cybersecurity Agenda, 2018, Kamerstuk 26 643 nr. 536

[6] Cybersecuritybeeld Nederland 2021, Kamerstuk 26 643, nr. 767

[7] Bijvoorbeeld in het Europese netwerk voor 'Cyber Security Incident Response Teams': het CSIRTs-netwerk.

[8] Zie ook vermelding hiervan in het Cybersecuritybeeld Nederland 2021, Kamerstuk 26 643, nr. 767

[9] Europese Rekenkamer, Speciaal verslag, 'Cyberbeveiliging van EU-instellingen, -organen en -agentschappen, Paraatheidsniveau staat over het algemeen niet in verhouding tot dreigingen' (2022).

zijn en dat daarmee de vertrouwelijkheid van de daarin opgeslagen gegevens, bijvoorbeeld die uit Nederland zijn ontvangen, voldoende wordt gewaarborgd en die gegevens niet door kwaadwillenden kunnen worden ontvreemd. Daarnaast zijn er EU IOA's waarvan de werkzaamheden direct het functioneren van de Nederlandse maatschappij raken, bijvoorbeeld de Europese Centrale Bank (ECB) in het kader van het betalingsverkeer, of Eurocontrol voor wat betreft het vliegverkeer, en waarvan het dus van belang is dat de netwerk- en informatiesystemen zodanig beveiligd zijn dat de continuïteit van hun werkzaamheden niet onnodig in gevaar komt.

Om die redenen verwelkomt het kabinet het voorliggende voorstel. Tegelijkertijd stelt het kabinet de kritische vraag of het voorstel wel verreikend genoeg is: wat digitale weerbaarheid betreft geldt voor het kabinet dat de vrijblijvendheid voorbij is. Het kabinet zal de Commissie daarop bevragen en erop inzetten dat dit in voldoende mate wordt gewaarborgd in het vervolgtraject.

Het kabinet onderschrijft de doelstellingen van de verordening. Het kabinet vindt het van belang dat bij het formuleren daarvan zo veel mogelijk aansluiting wordt gezocht bij de bestaande richtlijn Netwerk- en Informatiebeveiliging (NIB)[10] en het voorstel voor herziening daarvan waarover momenteel in EU-verband wordt onderhandeld (NIB2).[11] Dit geldt ook voor de elders in het voorstel beschreven maatregelen, zowel qua terminologie als qua niveau van de gestelde eisen. Het kabinet zal het belang hiervan bij de Commissie benadrukken.

Het kabinet ondersteunt in algemene zin de verplichtingen tot het opzetten van een intern kader, een basisniveau en maturiteitsbeoordeling met betrekking tot de cyberbeveiliging van de EU IOA's en de daarbij behorende cyberbeveiligingsplannen. De verwachting is dat de voorgestelde maatregelen zullen bijdragen aan een hoger niveau van cyberbeveiliging. Wel zal het kabinet de Commissie bevragen over bijvoorbeeld de eis dat alle EU IOA's een eigen kader opstellen voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's. De Commissie benadrukt de institutionele autonomie van de EU IOA's, maar de vraag is gerechtvaardigd of en in hoeverre hiermee de huidige verschillen in beveiliging van EU IOA's voldoende worden weggenomen. Om een gezamenlijk niveau van cyberbeveiliging te bewerkstelligen kunnen meer geharmoniseerde kaders of richtsnoeren zinvol zijn.

Het voornemen tot oprichting van het IICB beziet het kabinet positief. Dit zal naar verwachting bijdragen aan een hoger en gemeenschappelijker niveau van de digitale weerbaarheid van de EU IOA's. Wel vraagt het kabinet zich daarbij af of de IICB daartoe voldoende bevoegdheden zal krijgen, aangezien de IICB krachtens dit voorstel, indien blijkt van niet doeltreffende toepassing van de verordening door de EU IOA's, enkel niet-bindende waarschuwingen kan geven en audits kan aanbevelen. Het kabinet zal met de Commissie in gesprek gaan over de wenselijkheid en mogelijkheid om de IICB meer bevoegdheden te geven, in lijn met de voorgestelde verdergaande instrumenten voor toezicht en handhaving als in het NIB2-voorstel. Ook vraagt het kabinet zich af

[10] BNC-fiche Richtlijn netwerk- en informatiebeveiliging, Kamerstuk 22 112, nr. 1587.
[11] BNC-fiche: Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn), Kamerstuk 22 112, nr. 3053.

in hoeverre de EU-lidstaten voldoende vertegenwoordigd zijn in de IICB, aangezien de veiligheid van de EU IOA's ook de belangen van de lidstaten raakt. Tijdens de onderhandelingen over het voorstel zal het kabinet erop inzetten dat dit goed wordt geborgd.

Het voorstel tot versteviging van de taken van CERT-EU wordt door het kabinet gesteund. Naar verwachting kan er zo een meer centraal geregelde ondersteuning van de digitale weerbaarheid van de EU IOA's worden gerealiseerd. Dit kan niet alleen leiden tot een verbetering van de digitale weerbaarheid van EU IOA's, maar ook tot grotere uniformiteit en daarmee vergemakkelijking van respons in geval van (grootschalige) incidenten. Wat betreft het delen van informatie over dreigingen, kwetsbaarheden en incidenten met lidstaten, zal het kabinet met de Commissie in gesprek gaan over de nadere invulling daarvan. Uitgangspunt voor het kabinet is dat relevante informatie waar mogelijk proactief wordt gedeeld met de lidstaten. Over samenwerking door CERT-EU met nationale entiteiten van buiten de EU zal het kabinet in de onderhandelingen het uitgangspunt uitdragen dat het primaat hiertoe bij de lidstaten blijft. Het kabinet onderschrijft het belang om CERT-EU een rol te geven bij de verdere ontwikkeling van een Joint Cyber Unit, maar vindt het daarbij van belang dat deze activiteiten niet afleiden van de hoofdtaak van CERT-EU, namelijk het verhogen van het cyberbeveiligingsniveau van de EU IOA's.

In algemene zin steunt het kabinet de maatregelen die samenwerking en verslagleggingsverplichtingen betreffen. Bij het voorkomen en bestrijden van incidenten in het digitale domein is samenwerking immers essentieel. De samenwerking tussen CERT-EU en de EU IOA's zoals die in het voorstel wordt vormgegeven beziet het kabinet dan ook positief. Het kabinet zal bij de Commissie om toelichting vragen over de nadere invulling van de uitzonderingsgrond bij de plicht voor EU IOA's om significante cyberdreigingen, kwetsbaarheden of incidenten binnen 24 uur na ontdekking hiervan te delen met CERT-EU. Daarnaast vraagt het kabinet zich af hoe de communicatie en rolverdeling wordt vormgegeven met de Cyber Rapid Response Teams (CRRT's) in het kader van Permanente Gestructureerde Samenwerking (PESCO) van de EU en zal de Commissie oproepen zoveel mogelijk geleerde lessen van dit PESCO-project toe te passen. Het kabinet is terughoudend voor wat betreft de voorgestelde eis dat alle door nationale veiligheids- en inlichtingendiensten geïnitieerde of beoogde contacten met CERT-EU dienen te worden meegedeeld aan de Commissie en de voorzitter van de IICB. De maatregel brengt het risico met zich mee dat inlichtingen- en veiligheidsdiensten minder met de EU IOA's kunnen delen, waardoor het kabinet betwijfelt of het bijdraagt aan het doel de veiligheid van de EU IOA's te vergroten. Uitgangspunt moet zijn dat de inlichtingen- en veiligheidsdiensten zelf per casus een afweging kunnen maken wie van welke informatie op de hoogte moet zijn. Wat betreft de mogelijkheid tot het verlenen van bijstand aan lidstaten door deskundigen in dienst van de EU IOA's is het standpunt van het kabinet dat hiervan uitsluitend sprake kan zijn op verzoek van die lidstaat.

c) Eerste inschatting van krachtenveld

Naar verwachting zal een meerderheid van de EU-lidstaten de algehele doelstelling van de verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU IOA's steunen. Desondanks is het de verwachting van het kabinet dat, naast Nederland,

diverse lidstaten aandacht zullen vragen voor de rol en mate van invloed van de lidstaten, de rol van het IICB en de rol van de CERT-EU.

Naar verwachting zal het Europees Parlement positief staan tegenover het voorstel. De grootste politieke groeperingen in het Europees Parlement hebben het verbeteren van de digitale veiligheid binnen de EU en haar lidstaten opgenomen in de politieke programma's. Om deze reden is het aannemelijk dat een meerderheid van het Europees Parlement positief zal staan tegenover het voorstel en het beoogde doel ervan.

4. Beoordeling bevoegdheid, subsidiariteit, proportionaliteit

a) Bevoegdheid

Het oordeel van het kabinet ten aanzien van de bevoegdheid is positief. Het voorstel is gebaseerd op artikel 298 VWEU en artikel 106bis Euratom-verdrag. Artikel 298, eerste lid, VWEU bepaalt dat de EU IOA's bij de vervulling van hun taken steunen op een open, doeltreffend en onafhankelijk Europees ambtenarenapparaat. Artikel 298, tweede lid, VWEU geeft de EU de bevoegdheid, met inachtneming van het statuut en de regeling vastgesteld op grond van artikel 336 VWEU bepalingen daartoe vast te stellen. In artikel 106bis Euratom-verdrag wordt artikel 298 VWEU van toepassing verklaard op het Euratom-verdrag. Het kabinet kan zich vinden in de rechtsgrondslag.

Aangezien het voorstel in hoofdzaak ziet op het treffen van maatregelen ten behoeve van een hoog gezamenlijk niveau van cyberbeveiliging voor de EU IOA's, wat buiten de in de artikelen 3 en 6 VWEU bedoelde artikelen valt, is sprake van een gedeelde bevoegdheid van de EU en de lidstaten (artikel 4, eerste lid, VWEU).

b) Subsidiariteit

Het oordeel van het kabinet is positief. De verordening heeft tot doel een hoog niveau van cyberbeveiliging voor de EU IOA's te bereiken. Aangezien het gaat om regels voor de EU-instellingen, ligt het voor de hand dat dit op EU-niveau geregeld wordt. Dit zou niet door de lidstaten kunnen worden verwezenlijkt. Optreden op EU-niveau is daarom gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet is positief. De verordening heeft tot doel om het basisniveau van cyberbeveiliging van de EU IOA's te verhogen. Deze verordening wordt door het kabinet als geschikt geacht om deze doelstelling te bereiken, gezien onder andere de minimumeisen op het terrein van cyberbeveiliging waar de EU IOA's aan dienen te voldoen. Zo worden de EU IOA's onder andere verplicht tot het opstellen van een intern kader voor het beheer, de governance en de controle met betrekking tot cyberbeveiligingsrisico's, met onder meer passende financiële dekking. Daarnaast voorziet het voorstel door middel van de oprichting van de IICB, de verstevigde rol van CERT-EU en de verplichte maturiteitsbeoordeling in het opzetten van systemen en stelt het vereisten om cyberbeveiliging te waarborgen. Deze systemen en vereisten dragen volgens het kabinet bij aan de verbetering van de cyberbeveiliging van de EU IOA's, waardoor het voorstel geschikt is om de doelstellingen ervan te verwezenlijken. Gelet op de mogelijkheid voor EU IOA's om eigen kaders vast te stellen en omdat de bepalingen enkel de EU IOA's betreffen en

geen nieuwe verplichtingen opleggen aan de lidstaten, gaat het voorstel bovendien niet verder dan noodzakelijk. Het voorstel zou wat het kabinet betreft zelfs verstrekkender mogen worden, bijvoorbeeld door de IICB meer toezichtsbevoegdheden te geven.

Een aandachtspunt is de bepaling waarin de eis wordt gesteld dat alle contacten met CERT-EU die door nationale veiligheids- en inlichtingendiensten worden geïnitieerd of beoogd, onverwijld aan de Commissie en de voorzitter van de IICB moeten worden meegedeeld. Het kabinet hecht waarde aan de mogelijkheid van de inlichtingen- en veiligheidsdiensten om op basis van vertrouwelijkheid te kunnen communiceren met CERT-EU. Een verplichting om ieder contact te delen met de Commissie ziet het kabinet als een belemmering van de goede samenwerking. Het kabinet betwijfelt de geschiktheid en noodzakelijkheid van deze verplichting en zal hierover het gesprek aangaan met de Commissie.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

De totale kosten van de verordening schat de Commissie op €68,3 miljoen tot het einde van het huidige Meerjarig Financieel Kader (MFK) in 2027. Voor de financiering wordt beroep gedaan op hoofdstukken 1 t/m 6 (budget voor Unie contributies aan gedecentraliseerde lichamen en agentschappen) en hoofdstuk 7 (budget voor o.a. personeelsvergoedingen) van het MFK. Het overige bedrag wordt gefinancierd door zelf-gefinancierde Europese instituties, lichamen en agentschappen. Onder deze kosten vallen de salariskosten voor 21 extra fulltime-equivalent (fte) die aangenomen worden tot het einde van het huidige Meerjarig Financieel Kader (MFK) in 2027. De 21 extra fte bestaan uit 20 permanente posten binnen CERT-EU en 1 post op contractbasis bij het Directoraat-Generaal voor Informatie van de Commissie. Hier staat tegenover dat er 12 fte op contractbasis binnen CERT-EU zullen verdwijnen. De Commissie stelt dat de budgettaire gevolgen van het voorstel binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 passen. Nederland is van mening dat de middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

Daarnaast moet de ontwikkeling van de administratieve uitgaven in lijn zijn met de conclusies van de Europese Raad van juli 2020 over het MFK-akkoord. Het kabinet is kritisch over de stijging van het aantal werknemers.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of medeoverheden

Er worden geen financiële consequenties verwacht voor de rijksoverheid en/of medeoverheden, omdat de verordening uitsluitend verplichtingen oplegt aan EU IOA's. Eventuele budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger
Er worden geen financiële consequenties of gevolgen voor regeldruk verwacht voor de bedrijfsleven en burger, omdat de verordening uitsluitend verplichtingen oplegt aan EU IOA's.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten
Er worden geen gevolgen verwacht voor de concurrentiekracht van Nederland of de EU, aangezien het hier om een interne aangelegenheid van de EU IOA's gaat. Deze EU IOA's hebben geen concurrentiepositie vis-à-vis de private sector.

Gezien het door de Commissie geschetste beeld, waar het steeds vaker doelwit wordt van statelijke actoren, zal deze verordening naar verwachting leiden tot een beperking van incidenten en een effectievere respons wanneer incidenten zich voordoen. De verwachting is dat dit de geopolitieke positie van de EU versterkt doordat spionage en sabotage worden bemoeilijkt.

6. Implicaties juridisch
a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)
Er worden geen consequenties verwacht voor nationale en decentrale regelgeving en/of sanctionering beleid.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan
Niet van toepassing.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid
De verordening is beoogd in werking te treden op de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie. De verordening wordt van toepassing twee jaar na deze datum. Het kabinet acht dit haalbaar.

d) Wenselijkheid evaluatie-/horizonbepaling
Het voorstel luidt dat de Commissie niet eerder dan vijf jaar na de inwerkingtreding de werking van deze verordening evalueert daarover verslag uitbrengt aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's. Gezien het continu veranderende dreigingslandschap zal het kabinet met de Commissie in gesprek gaan over de vraag in hoeverre een eerdere evaluatie wenselijk is.

e) Constitutionele toets
Niet van toepassing.

7. Implicaties voor uitvoering en/of handhaving
Geen implicaties voor uitvoering of handhaving.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden.