Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3052 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 februari 2021

Overeenkomstig de bestaande afspraken ontvangt u hierbij 6 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche: Verordening inzake Digitale Markten (Digital Markets Act) (Kamerstuk 22 112, nr. 3049)
Fiche: Verordening inzake digitale diensten en wijziging Richtlijn 2000/31/EG (Digital Services Act) (Kamerstuk 22 112, nr. 3050)
Fiche: Verordening betreffende trans-Europese energie-infrastructuur (TEN-E) (Kamerstuk 22 112, nr. 3051)
Fiche: Gezamenlijke Mededeling EU-strategie inzake cyberbeveiliging
Fiche: Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn) (Kamerstuk 22 112, nr. 3053)
Fiche: Richtlijn veerkracht kritieke entiteiten (Kamerstuk 22 112, nr. 3054)

De Minister van Buitenlandse Zaken,
S.A. Blok

kst-22112-3052
ISSN 0921 - 7371
's-Gravenhage 2021

Fiche: Gezamenlijke Mededeling EU-strategie inzake cyberbeveiliging

1. Algemene gegevens

a) *Titel voorstel*
Gezamenlijke Mededeling aan het Europees Parlement en de Raad: De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk
b) *Datum ontvangst Commissiedocument*
december 2020
c) *Nr. Commissiedocument*
COM (2020) 18
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52020JC0018
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

2. Essentie voorstel

Op 16 december 2020 hebben de Commissie en de Hoge Vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid gezamenlijk de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk (hierna: «de strategie»») gepubliceerd. Tegelijkertijd presenteerde de Commissie een voorstel tot herziening van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIB-richtlijn)[1] en de richtlijn voor de veerkracht van kritische entiteiten (CER)[2], waarover separaat BNC-fiches worden opgesteld en gelijktijdig aan uw Kamer worden verzonden.

De strategie vormt een reactie op de toegenomen digitale dreiging tegen de EU en haar economieën, democratische vrijheden en waarden, en bouwt voort op de resultaten van de EU Cyberstrategie uit 2013[3] en de mededeling over cyberbeveiliging uit 2017[4]. De strategie richt zich op de volgende drie pijlers.
Ten eerste de pijler veerkracht, technologische soevereiniteit en leiderschap. In dit kader wordt onder meer een herziene NIB-richtlijn als speerpunt genoemd. Er wordt voorgesteld om een Europees cyberschild te ontwikkelen, via een EU-netwerk van beveiligingsoperaties centra (*Security Operations Centers/SOC's)* [5]. Ook betreft deze pijler de verdere uitvoering op nationaal niveau van maatregelen uit en het vervolg op de *toolbox* voor 5G-cyberbeveiliging[6] en mogelijk nieuwe wetgeving ter versterking van een veilig internet van dingen (*IoT*). Middels investeringen via het voorgestelde kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en netwerk van nationale coördinatiecentra (*Cybersecurity Competence Centre and Network/CCCN*) dient het CCCN een sleutelrol te spelen in de ontwikkeling van de

[1] COM (2020) 823
[2] COM (2020) 829
[3] JOIN (2016) 1 Cybersecurity Strategie van de Europese Unie: een open vrij en veilig cyberspace
[4] JOIN (2017) 450 Mededeling Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU
[5] Afdeling of team dat informatiesystemen controleert of bewaakt. Dit doen zij voor de eigen organisatie of voor klanten.
[6] COM (2020) 50; Kamerstuk 22 112, nr. 2854

technologische soevereiniteit van de EU[7]. Door middel van de ontwikkeling van een EU-dienst voor *Domain Name System*(DNS)-resolutie[8] moet een veilig en open alternatief worden geboden om toegang te krijgen tot het internet.

Ten tweede de pijler die zich richt op de opbouw van operationele capaciteit om te voorkomen, af te schrikken en te reageren. Om het Europees kader voor crisisbeheersing inzake cyberbeveiliging te versterken, pleit de Commissie voor het opzetten van een gezamenlijke cybereenheid (*Joint Cyber Unit/JCU)*. Ten behoeve van de aanpak van cybercriminaliteit beoogt de Commissie verdere uitvoering van de agenda voor cybercriminaliteit in het kader van de Veiligheidsuniestrategie[9] en het vergroten van digitale capaciteiten van opsporingsdiensten. Tevens noemt de Commissie het versterken van het instrumentarium voor cyberdiplomatie van de EU (*EU cyberdiplomacy toolbox*)[10]. Daarnaast moedigt de Hoge Vertegenwoordiger de totstandbrenging van een werkgroep cyberinlichtingen binnen het inlichtingen- en situatiecentrum van de EU (EU *intelligence and situation centre/EU INTCEN*) aan[11]. Ook doet de Commissie voorstellen ten behoeve van het vergroten van cyberdefensiecapaciteiten binnen de Unie.

Ten derde de pijler inzake het bevorderen van een mondiale, open *cyberspace.* Met het oog op het versterken van EU-leiderschap inzake standaarden en normen in cyberspace, stelt de Commissie voor om een set van doelstellingen in internationale standaardisatieprocessen[12] vast te leggen en deze op internationaal niveau te bevorderen. Daarbij wil de Commissie zich inzetten voor veiligheid en stabiliteit in het cyberdomein. Tevens wordt ingezet op het versterken van samenwerking met derde landen, regionale en internationale organisaties en de *multistakeholder*gemeenschap. Ook doet de Commissie voorstellen ten behoeve van wereldwijde cybercapaciteitsopbouw.

Tot slot stelt de Commissie voor om het cyberbeveiligingsniveau van EU-instellingen, -organen en -agentschappen te verhogen door middel van wetgeving. Daarbij wordt het versterken van het mandaat en financiering van het EU *Computer Emergency Response Team (*CERT-EU)[13] benoemd.

---

[7] COM (2018) 630; Kamerstuk 22 112, nr. 2705

[8] Het DNS is een van de belangrijkste protocollen van het internet. Wanneer een gebruiker in een webbrowser wil navigeren naar een bestemming, bijvoorbeeld de website van de rijksoverheid, dan typt hij niet het IP-adres van de rijksoverheid in, maar de URL www.rijksoverheid.nl. Op het moment dat via de webbrowser het «verzoek» wordt ingediend om naar dat adres te navigeren, dient de webbrowser doorgaans via het besturingssysteem een DNS-verzoek in bij de internet serviceprovider om deze te laten vertellen welk IP-adres bij het opgevraagde domein hoort (dit proces van vertaling van IP-adressen naar domeinnamen heet DNS-resolutie).

[9] COM (2020) 605

[10] Dit kader biedt de EU en haar lidstaten beschikking over alle GBVB-maatregelen om kwaadwillige cyberactiviteiten tegen de EU en haar lidstaten te voorkomen, te ontmoedigen, te bestrijden en erop te reageren.

[11] De voorgestelde werkgroep zou de strategische samenwerking inzake inlichtingen over cyberdreigingen en -activiteiten tussen de lidstaten moeten bevorderen.

[12] Enkele voorbeelden zijn de Internationale Organisatie voor Standaardisatie (ISO), de Internationale Unie voor Telecommunicatie (ITU), het Europees Comité voor Standaardisatie (CEN), het Europees Comité voor elektrotechnische standaardisatie (CENELEC), en de Internet Engineering Task Force (IETF).

[13] CERT-EU fungeert sinds 11 september 2012 als CERT voor EU-instellingen, agentschappen en organen en bestaat uit IT-beveiligingsexperts van de belangrijkste EU-instellingen (Europese Commissie, secretariaat-generaal van de Raad, Europees Parlement, Comité van de Regio's, Economisch en Sociaal Comité).

3. Nederlandse positie ten aanzien van de mededeling/aanbeveling

a) Essentie Nederlands beleid op dit terrein

Het versterken van de digitale weerbaarheid is voor het kabinet een prioriteit. De uitwerking van de Nederlandse cyberbeveiligingsaanpak is vastgelegd in de Nederlandse Cyber Security Agenda (NCSA) uit 2018, waarin het weerbaar maken van Nederland tegen digitale dreigingen op geïntegreerde wijze wordt geadresseerd[14]. De NCSA omvat zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen. Over de voortgang van de NCSA wordt uw Kamer jaarlijks geïnformeerd[15].

Nederland is als open en internationaal georiënteerde economie gebaat bij een stabiel, veilig en vrij toegankelijk cyberdomein. Het kabinet zet zich hier samen met zijn internationale partners voor in, waarbij de kansen die digitalisering onze economie en samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. Ook in de Nederlandse Digitaliseringsstrategie[16] en NL DIGIbeter[17] is het versterken van weerbaarheid een prioriteit.

Dreigingsbeelden[18] van de afgelopen jaren tonen aan dat de digitale risico's voor Nederland onverminderd groot zijn. Gezien het inherente grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging staan Europese en internationale samenwerking voor het kabinet centraal. Het kabinet zet zich dan ook via de EU in om de ambities uit de NCSA te realiseren, onder meer via de NIB Samenwerkingsgroep[19], het EU *Computer Security Incident Response Teams* (CSIRT's) Netwerk en de Raadswerkgroep Cyber. Ook blijft het kabinet zich in Europees verband inzetten voor het verhogen van de cybersecurity van ICT-producten en diensten, inclusief IoT, op basis van de Roadmap Digitaal Veilige Hard- en Software[20]. Nederland blijft zich hard maken voor Europees verplichte cybersecuritycertificering van op het internet aangesloten apparaten[21] en samenwerking ten behoeve van veilige 5G-telecommunicatienetwerken[22]. De integrale kabinetsaanpak cybercrime richt zich onder andere op preventie, waar capaciteit en het ontwikkelen van vaardigheden en middelen onderdeel van zijn. Dit geldt ook voor de versterking van internationale juridische kaders in de rechtshandhaving.[23]

Het kabinet zet in op versterking van de internationale vrede en veiligheid en het bestendigen van de internationale rechtsorde in het digitale domein[24], zoals onder meer uitgewerkt in de Geïntegreerde Buitenland-

---

[14] Kamerstuk 26 643, nr. 536
[15] Kamerstuk 26 643, nr. 695
[16] Nederlandse Digitaliseringsstrategie 2020, Kamerstukken II 2019–2020, 26 643, nr. 709
[17] Kamerstuk 26 643, nr.700
[18] Cybersecuritybeeld Nederland 2019, Kamerstuk 26 643, nr. 614; Cybersecuritybeeld Nederland 2020, Kamerstuk 26 643, nr. 695
[19] In de Netwerk- en Informatiebeveiliging (NIB) Samenwerkingsgroep zitten vertegenwoordigers van de lidstaten samen met de Commissie en het Europese Agentschap voor Netwerk- en Informatiebeveiliging (Enisa).
[20] Kamerstuk 26 643, nr. 735
[21] Conform Motie van het lid Paternotte c.s. (Kamerstuk 21 501-30, nr. 422)
[22] Conform Motie van het lid Weverling c.s. (Kamerstuk 21 501-33, nr. 734) en motie van het lid Van den Berg c.s. (Kamerstuk 21 501-33, nr. 747)
[23] Kamerstuk 26 643, nr. 696
[24] Kamerstuk 26 643, nr. 614

en Veiligheidsstrategie (GBVS)[25] en de Internationale Cyberstrategie[26]. Over de voortgang van de versterking van de internationale rechtsorde is uw Kamer november jl. geïnformeerd.[27] Nederland en de EU beschikken over meerdere diplomatieke instrumenten om het normatief kader in het digitale domein te bestendigen en de kosten van norm overschrijdend gedrag te verhogen.[28]

b) Beoordeling + inzet ten aanzien van dit voorstel

De noodzaak tot versterking van de inzet op cyberbeveiligingsgebied, zowel door de lidstaten zelf als op Europees niveau, wordt door het kabinet ondersteund met oog op de toegenomen digitalisering en het permanente karakter van de digitale dreiging. Een integrale Europese aanpak is nodig waarbij zowel de risico's als de kansen van cyberbeveiliging geadresseerd worden. Het kabinet heeft waardering voor de brede aanpak die deze strategie voorstaat. Daarbij acht het kabinet het van essentieel belang dat cyberbeveiliging binnen alle beleidsdomeinen en niveaus van de EU wordt geïntegreerd. Het kabinet zal in de beoordeling van plannen nadrukkelijk aandacht besteden aan de verhouding met de verdragsrechtelijke bepaling over de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid (artikel 4, lid 2, VEU). Ook zal er nadrukkelijk worden gelet op het voorkomen van duplicatie en het bewaken van samenhang met reeds bestaande organisaties, netwerken en initiatieven.

Het kabinet verwelkomt het feit dat de Commissie het onderwerp van 5G-veiligheid actief blijft adresseren in gezamenlijkheid met de lidstaten. Ook ziet het kabinet het voorstel om de cybersecurity van IoT te verhogen door middel van eventuele regelgeving, aanvullend op bestaande en reeds voorgenomen maatregelen[29], met belangstelling tegemoet. Deze koers is in lijn met het Nederlandse beleid en de raadsconclusies van de Telecomraad van 7 december 2020.[30] Het kabinet onderstreept de urgentie van de voorstellen inzake de beschikbaarheid van elektronisch bewijs en het verbeteren van capaciteit, vaardigheden en middelen bij de aanpak van cybercriminaliteit en kijkt uit naar het aangekondigde actieplan. Tevens ondersteunt het kabinet de inzet op de internationale juridische kaders in de rechtshandhaving, zoals het Verdrag van Boedapest.[31] Het kabinet acht het positief dat de Commissie een hoog cyberbeveiligingsniveau van EU-instellingen wil bereiken. Met inachtneming van de eigen verantwoordelijkheid die de Commissie hiervoor heeft, kijkt het kabinet met belangstelling naar de concrete invulling van de voorgestelde wetgeving en de samenhangende budgettaire impact. Verder zal het kabinet in EU-verband aandacht blijven vragen voor het belang van (het ontwikkelen van) cybervaardigheden en cyber *professionals*.

Verder ziet het kabinet graag verduidelijking van de plannen van de Commissie omtrent een Europees cyberschild en de samenwerking van SOC's in Europees verband. Het kabinet heeft hiertoe onder meer vragen over de haalbaarheid, toegevoegde waarde, dwarsverbanden met en betrokkenheid van CSIRT's en de rol van de private sector. Ook over het voorstel van de Commissie voor de uitrol van beveiligde kwantumcommunicatie-infrastructuur (*kwantum communication infrastructure/*

[25] Kamerstuk 33 694, nr. 12
[26] Kamerstuk 26 643, nr. 447
[27] Kamerstuk 33 694, nr. 60
[28] O.a. de EU cyberdiplomacy toolbox (9916/17) en het EU-cybersanctieregime (7299/19)
[29] Zoals certificering onder de Cyber Security Act (COM (2019)/881) en wettelijke minimumeisen voor verbonden apparaten onder de Radio Equipment Directive (COM (2014)/53)
[30] Kamerstuk 21 501–33, nr. 838
[31] ETS (2001) 185

QCI)[32] behoeft het kabinet meer verduidelijking inzake de kosten, de technische beveiligingswaarden en het toepassingsgebied van dit systeem. Het voorstel voor een EU-dienst voor DNS-resolutie ontvangt het kabinet met belangstelling. Het kabinet wenst daarbij wel verdere uitwerking van de Commissie te ontvangen met betrekking tot nut, noodzaak en uitvoerbaarheid. In de praktijk wordt op dit moment door de Nederlandse internetproviders zelf op hun *resolvers* DNS resolutie gedaan.[33] [34]

Het kabinet steunt in beginsel de ambitie om het situationeel bewustzijn ten aanzien van (potentiële) cyberdreigingen te vergroten. In hoeverre het opzetten van een JCU kan bijdragen aan versterking van de samenwerking tussen verschillende cyberbeveiligingsgemeenschappen in de EU, behoeft nadere onderbouwing door de Commissie voordat er een goed oordeel over gegeven kan worden. Het kabinet stelt alvast met instemming vast dat de strategie vermeldt dat de JCU geen op zichzelf staand orgaan zal zijn. Het kabinet kijkt uit naar het nadere voorstel, dat wordt verwacht in het eerste kwartaal van 2021. Hierbij zal het kabinet scherp zijn op samenhang met bestaande netwerken en initiatieven, de uitsluitende verantwoordelijkheid van lidstaten inzake bescherming van nationale veiligheid, alsmede de aansturing.

Het kabinet verwelkomt de voorstellen voor het gebruik van de *cyberdiplomacy toolbox* bij cyberaanvallen op de vitale infrastructuur, democratische processen en toeleveringsketens. Het kijkt daarbij uit naar het voorstel om de houding van de EU tegen cyberafschrikking verder te definiëren. Het kabinet is voorstander van besluitvorming onder stemming bij gekwalificeerde meerderheid en verwelkomt daarom het initiatief deze optie onder het cybersanctieregime te onderzoeken. Ook verwelkomt het kabinet het voorstel om synergie te zoeken tussen de *cyberdiplomacy toolbox* en inspanningen gericht op het tegengaan van hybride dreigingen, desinformatie en buitenlandse inmenging. Daarnaast verwelkomt het kabinet de voorgestelde intensivering van de inzet op het internationale standaardisatieproces. Tevens onderschrijft het kabinet het belang om proactief bij te dragen in norm-discussies, middels bestaande en nieuwe initiatieven zoals het actieprogramma[35] waarvan Nederland cosponsor is, en het belang van de ontwikkeling van standpunten rondom de toepassing van internationaal recht in cyberspace, daar waar het kabinet proactief tot heeft opgeroepen in internationale discussies. Voorts verwelkomt het kabinet het voorstel om begeleiding te bieden bij de toepassing van mensenrechten en fundamentele vrijheden in het cyberdomein.

Tevens onderschrijft het kabinet het belang om versterkt in te zetten op capaciteitsopbouw en de voorgestelde externe agenda voor de opbouw van cybercapaciteit en een EU-raad voor de opbouw van cybercapaciteit. Het kabinet benadrukt dat deze voorstellen primair moeten helpen om de coördinatie binnen de EU te verbeteren; externe coördinatie moet zich

---

[32] De QCI zal in potentie een gloednieuwe manier bieden om vertrouwelijke informatie door te geven met behulp van een uitstekend beveiligde vorm van versleuteling om cyberaanvallen af te wenden. Deze infrastructuur zal twee belangrijke componenten omvatten: de bestaande terrestrische glasvezelcommunicatienetwerken en onderling verbonden satellieten in de ruimte die de gehele EU bestrijken, met inbegrip van de overzeese gebieden.

[33] Dit zou kunnen veranderen als door niet-EU partijen het DNS over HTTPS (DoH) protocol wordt toegepast/ingebouwd in de door hen aangeboden webbrowsers en er mogelijk alleen resolutie buiten de EU plaatsheeft.

[34] Kamerstuk 26 643, nr. 703

[35] Actieprogramma ter bevordering van verantwoord gedrag van de staat in cyberspace, voor te leggen aan de Verenigde Naties, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

volgens het kabinet voltrekken in bestaande gemeenschappen, zoals het *Global Forum on Cyber Expertise* (GFCE).

Met betrekking tot de nieuwe wettelijke basis met als doel het mandaat en de financiering van CERT-EU te versterken, rijst de vraag waartoe de voorgestelde mandaat wijziging zou dienen. Het kabinet acht het huidige mandaat voldoende voor CERT-EU om haar CERT-taak voor de EU-instellingen uit te voeren. Voor wat betreft het aanmoedigen van en faciliteren door de Hoge Vertegenwoordiger van de totstandbrenging van een werkgroep cyberinlichtingen binnen EU INTCEN acht het kabinet het van belang dat er kritisch wordt gekeken naar doel en ratio, en waar kan worden aangesloten bij reeds bestaande initiatieven en structuren, zoals de *Hybrid Fusion Cell*.

c) Eerste inschatting van krachtenveld

Naar verwachting zal een grote meerderheid van de EU-lidstaten de strategie ondersteunen. In algemene zin onderschrijven alle lidstaten het belang van het waarborgen van cyberbeveiliging in de EU. De verwachting is dat lidstaten, net als Nederland, behoefte hebben aan meer uitleg over de manier van implementatie van de strategie en bijbehorende prioritering. Veel lidstaten, net als Nederland, zullen bijvoorbeeld kritisch zijn op plannen van de Commissie die (potentiële) raakvlakken met nationale veiligheid kennen, zoals de JCU en de cyberintelligence werkgroep binnen EU INTCEN. Naar verwachting zal de strategie op steun kunnen rekenen van het Europees Parlement.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen op het gebied van regeldruk en administratieve lasten

a) Bevoegdheid

De grondhouding van het kabinet ten aanzien van de bevoegdheid is positief. De gezamenlijke mededeling van de Commissie en de Hoge Vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid ziet met name op de bescherming van de Europese Unie tegen digitale aanvallen. De plannen passen volgens het kabinet op hoofdlijnen binnen de bevoegdheden van de EU op de terreinen interne markt (Artikel 4, tweede lid, onder a, VWEU), gemeenschappelijk buitenlands en veiligheidsbeleid (Artikel 24 VEU; artikel 2, vierde lid, VWEU) en de ruimte van vrijheid, veiligheid en recht (Artikel 4, tweede lid, onder j, VWEU).

Hoewel de Commissie en de Hoge Vertegenwoordiger in de gezamenlijke mededeling vermelden dat lidstaten verantwoordelijk blijven voor nationale veiligheid, stellen zij dat vanwege het grensoverschrijdende karakter van de digitale dreigingen ook de EU hierin een faciliterende rol heeft. Het kabinet zal er bij de in de strategie voorgestelde plannen nauwgezet op toezien dat de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van nationale veiligheid (Artikel 4, tweede lid, VEU) gewaarborgd blijft. In het bijzonder zal het kabinet met betrekking tot het voornemen tot aanmoedigen en faciliteren door de Hoge Vertegenwoordiger van de totstandbrenging van een werkgroep cyberinlichtingen binnen EU INTCEN en de uitwerking van dit voornemen, steeds toetsen of niet wordt getreden in voornoemde uitsluitende verantwoordelijkheid van de lidstaten.

b) Subsidiariteit

Het kabinet heeft een positieve grondhouding ten opzichte van de subsidiariteit van de gezamenlijke mededeling. Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging kunnen de gestelde doelstellingen in het algemeen volgens het kabinet beter worden verwezenlijkt op EU-niveau. Het kabinet steunt gelet daarop, onder meer optreden op EU-niveau ten behoeve van de versterking van de samenwerking tussen EU-lidstaten, en de ondersteuning daarvan door EU-instellingen, -organen en -agentschappen, om de digitale weerbaarheid van de EU te vergroten.

c) Proportionaliteit

De grondhouding van het kabinet ten aanzien van de proportionaliteit van de mededeling is positief, onder meer omdat het hierin aangekondigde optreden de cyberveiligheid van de EU op een effectieve en evenredige wijze naar een hoger niveau zal brengen, waardoor het optreden geschikt is om de digitale weerbaarheid binnen de EU te vergroten. Dit geldt bijvoorbeeld voor de voorgestelde intensivering van de EU-inzet op het internationale standaardisatieproces en de inzet op normen en raamwerken in cyberspace, waaronder het Verdrag van Boedapest. Een groot gedeelte van het aangekondigde optreden in de strategie gaat niet verder dan noodzakelijk en biedt in de uitvoering voldoende ruimte voor lidstaten. Zo laten het voorgestelde CCCN en het vervolg op de *toolbox* voor 5G-cyberbeveiliging voldoende ruimte voor de verdere uitvoering van maatregelen op nationaal niveau. Op basis van de mededeling is het vermoeden dat onder meer het voorstel voor een JCU mogelijk niet proportioneel is, en nadere uitleg en uitwerking behoeft alvorens dit te kunnen bepalen.

d) Financiële gevolgen

Als onderdeel van het nieuwe technologie- en industriebeleid en de agenda voor herstel kondigt de Commissie aan de strategie de komende zeven jaar te ondersteunen via investeringen in de digitale transitie van de EU.[36] Daarnaast kondigt de Commissie het voorstel van € 4,5 miljard aan publieke en particuliere investeringen aan in de periode van 2021–2027, via het CCCN (met name via het programma Digitaal Europa, Horizon Europa en de herstelfaciliteit). Het is nog niet helemaal duidelijk hoe de eventuele budgettaire impact van de voorstellen inzake het verhogen van de weerbaarheid van EU-instellingen wordt opgevangen door de Commissie. Het kabinet is van mening dat de financiële middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van het MFK 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting van de EU. Eventuele budgettaire gevolgen voor de nationale begroting zullen worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels inzake budgetdiscipline.

---

[36] Investeringen in de gehele toeleveringsketen voor digitale technologie, die bijdragen aan de digitale transitie of aan oplossingen voor de uitdagingen die eruit voortvloeien, dienen ten minste 20% uit te maken – € 134,5 miljard – van de faciliteit voor herstel en veerkracht, die € 672,5 miljard aan subsidies en leningen omvat. In het meerjarig financieel kader voor 2021–2027 is voorzien in EU-financiering voor cyberbeveiliging in het kader van het programma Digitaal Europa, en voor onderzoek naar cyberbeveiliging in het kader van Horizon Europa, waarbij bijzondere aandacht wordt geschonken aan steun voor kleine of middelgrote ondernemingen. De totale financiering zou kunnen oplopen tot € 2 miljard, plus investeringen door de lidstaten en door het bedrijfsleven.

e) Gevolgen voor regeldruk, administratieve lasten en concurrentiekracht

De mededeling zelf bevat geen nieuwe wettelijke maatregelen waarbij gevolgen te verwachten zijn op regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers. Bij het bekend worden van nieuwe ontwerp-regelgeving volgend op deze strategie zal worden bezien of en in hoeverre dit gevolgen heeft voor de regeldruk, administratieve lasten en concurrentiekracht en hoe dat moet worden beoordeeld. De uiteindelijke regeldruk en administratieve lasten van beleidsmaatregelen zijn afhankelijk van de specifieke invulling daarvan. Het is niet uit te sluiten dat zowel de uitvoering van afzonderlijke beleidsmaatregelen als de uitvoering van de beleidsmaatregelen in onderling verband bezien aanleiding geven tot nieuwe regels of verhoging van de uitvoeringslasten. Bij de uitwerking van eventuele maatregelen zal het kabinet zich inspannen om onwenselijke gevolgen voor de regeldruk, administratieve lasten en andere uitvoeringslasten te voorkomen of te mitigeren. Daarbij dient ook rekening gehouden te worden met eventuele gevolgen voor lokale overheden.