Ministerie van Financiën

TER INFORMATIE
Aan
de minister

Directie Financiële Markten

5.1.2e
5.1.2e

5.1.2e

5.1.2e

nota

Beleid digitale euro

Datum
2 februari 2022

Notanummer
2022-0000047157

Bijlagen
geen

Aanleiding

Via deze nota informeren we u graag over de ontwikkelingen en mogelijke beleidsinzet op het gebied van de digitale euro. Wij zijn voornemens om u binnenkort voorstellen te doen voor een 'agenda financiele sector', waarin u uw beleidsvoornemens op het brede terrein van de financiele sector met de Kamer kunt delen. De inzet op de digitale euro komt daar vanzelfsprekend ook in terug. Deze notitie neemt daar vast een voorschot op.

Kern

- De digitale euro is een digitale vorm van contant geld. De digitale euro is, in tegenstelling tot een giraal banktegoed, net als contant geld inwisselbaar bij de centrale bank. De digitale euro kan bijdragen aan innovatie, autonomie en het behoud van publiek geld in Europa.
- Zowel in ECB-verband als in Eurogroep-verband staat de digitale euro hoog op de agenda, waaronder tijdens de Eurogroepvergadering van 25 februari.
- Uw voorganger heeft de TK toegezegd een brief met een visie op de politieke keuzes bij de digitale euro te sturen. We adviseren u om dit voor de zomer te doen.
- De belangrijkste politieke vragen bij de digitale euro die wij momenteel zien zijn:
    1. Wat wordt de rol van de digitale euro in het financieel systeem?
    2. Wie bepaalt of de digitale euro er komt en hoe die eruit dient te zien?
    3. Hoe groot mag de rol van de ECB worden in het financiële stelsel?
    4. Wat wordt de balans tussen privacy voor gebruikers en het tegengaan van witwassen/belastingontduiking?
- In deze notitie beschrijven wij mogelijke Nederlandse prioriteiten bij de ontwikkeling van de digitale euro. Die kunnen we desgewenst nader met u bespreken. Sowieso leggen we deze ook nog aan u voor in het kader van de agenda financiele sector.

Toelichting

Wat is de digitale euro?

- Er bestaan verschillende vormen van geld. De bekendste zijn contant geld (publiek, chartaal geld) en banktegoeden (privaat, giraal geld).
- Contant geld is een claim op de centrale bank; een banktegoed is een claim op een commerciële bank. Een digitale euro is een nieuwe digitale vorm van contant geld: een digitale claim op de centrale bank. In de praktijk betekent

dit dat je een bankrekening kan aanhouden bij de centrale bank. Consumenten en bedrijven kunnen met deze digitale euro betalingen doen, en mogelijk ook sparen.

- De vraag is welke voordelen een digitale euro in Europa kan bieden ten opzichte van het bestaande geld. Banktegoeden zijn al veilig dankzij bankregelgeving en het depositogarantiestelsel (spaartegoeden tot EUR 100.000 worden gegarandeerd). Consumenten kunnen ook al veilig, snel en efficiënt betalen met hun bankrekening.
- De mogelijke introductie van de digitale euro moet gezien worden in de context van een snel veranderend banken- en betalingslandschap. Betalingen vinden in toenemende mate digitaal plaats. Het gevaar bestaat dat er dominante niet-publieke partijen ontstaan op de betalingsmarkt, zoals kaartmaatschappijen Visa en Mastercard of *bigtech*-bedrijven (Facebook, Apple, e.d.). Ook de opkomst van stablecoins, die de potentie hebben om tot een snel en efficiënt betaalmiddel met groot bereik uit te groeien, is hierbij van belang[1]. Het betalingsverkeer vervult belangrijke maatschappelijke functies. Een sterke concentratie en afhankelijkheid van buitenlandse partijen kan risico's met zich meebrengen voor de toegankelijkheid, financiële stabiliteit en digitale weerbaarheid.
- Een digitale euro moet breder gezien worden dan enkel een digitale vorm van geld die gebruikt kan worden als betaal- of spaarmiddel. De digitale euro kan dienen als open, publieke infrastructuur voor het betalingsverkeer, dat andere systemen verbindt. Die infrastructuur kan als basis dienen voor dienstverlening en innovaties door private partijen, zoals banken en *fintechs*.
- Tot slot zijn er partijen als de ECB die wijzen op het belang van het gebruik van publiek geld (geld als directe claim op een centrale bank) als fundering van het financiële systeem. Banktegoeden worden gebruikt met de verwachting dat het 1-op-1 inwisselbaar is met publiek geld. De ECB vraagt zich af of deze inwisselbaarheid gewaarborgd is als contant geld in de toekomst steeds beperkter wordt gebruikt.
- Een digitale euro kan dus:
    - de machtspositie van buitenlandse en/of private partijen in de financiële infrastructuur verminderen en daarmee bijdragen aan de autonomie van de euro(zone);
    - bijdragen aan innovatie en diversiteit in de financiële sector;
    - burgers en bedrijven een alternatief digitaal publiek betaalmiddel geven in de context van afnemend gebruik van contant geld.

Waar staan we in het proces?

- De ECB heeft in 2021 een "onderzoeksfase" van twee jaar aangekondigd (tot oktober 2023). De ECB verdiept zich in het ontwerp van de digitale euro, het uitwerken van *use cases*, het vormgeven van waarborgen (voor privacy, financiële stabiliteit, etc.) en een analyse van het wettelijk kader.
- De digitale euro staat de komende maanden vaak op het werkprogramma van de Eurogroep. In de Eurogroep wordt politieke sturing gegeven aan de vormgeving van de digitale euro. In november 2021 heeft een eerste inhoudelijke bijeenkomst plaatsgevonden over de beleidsdoelstellingen van de digitale euro. Het programma voor de komende maanden is:

[1] Hier vindt overigens ook regulering plaats, zie notitie FM 39576 over crypto's

Wanneer	Onderwerp
Februari	De digitale euro als digitaal betaalmiddel
April	Trade-offs in het design van de digitale euro tussen privacy en andere beleidsdoelen van de EU
Juni	De potentiële impact van de digitale euro op het financiële systeem en cashgebruik

- De verwachting is dat deze kabinetsperiode belangrijke keuzes zullen worden gemaakt over (het ontwerp van) de digitale euro en of deze zal worden ingevoerd.
- In 2023 loopt de onderzoeksperiode van de ECB af. Een volgende fase zou een fase van ontwikkeling en echte experimenten zijn. De huidige inschatting is dat die fase drie jaar zou kunnen duren (dus tot 2026).[2]
- Parallel zal er (Europese) regelgeving voor een sluitend juridisch kader ontwikkeld moeten worden, voor het uitgeven, beheren en toezichthouden op de digitale euro.

Hoe ziet de Tweede Kamer de digitale euro?

- In Nederland is het debat over de digitale euro op gang gekomen na het WRR-rapport Geld en Schuld, waarbij de digitale euro als alternatief genoemd wordt voor het bankieren bij "commerciële banken".
- De TK heeft tot nu toe vooral aangegeven dat er debat moet komen over de digitale euro, zonder al te veel richting te geven over de vormgeving hiervan. De TK is van mening dat het ontwikkelen van een digitale euro niet alleen een technocratische discussie (lees: een besluit van de ECB) moet zijn, maar juist politieke sturing vraagt.
- Het lid Alkaya (SP) is rapporteur voor de digitale euro, samen met het lid Heinen (VVD) – die het rapporteurschap heeft overgenomen van Aukje de Vries (VVD). De rapporteurs hebben in februari 2021 een eerste rapport uitgebracht. Met name het lid Alkaya vraagt aandacht voor de noodzaak voor het voeren van een politiek debat over de euro, en heeft aangekondigd om binnenkort een boek over dit onderwerp te publiceren.
- In november 2021 heeft uw ambtsvoorganger een debat over de digitale euro gehad met de vaste commissie Financiën. Daarin heeft hij toegezegd om "de contourenschets van de keuzes in het onderzoek naar de digitale euro, dat thans loopt, aan de Kamer toesturen. [...] Dat hoeft niet per se over drie maanden, maar wel binnen een afzienbare tijd en als het juiste moment daar is."
- In het regeerakkoord wordt niet ingegaan op de Nederlandse positie t.a.v. de digitale euro.

Hoe ziet het internationale speelveld er uit?

- China is in een verder gevorderd stadium ten aanzien van de ontwikkeling van een digitale munt (e-CNY). In een pilot wordt de e-CNY al gebruikt als betaalmiddel, bijvoorbeeld tijdens de olympische winterspelen. Het aandeel

[2] Dit blijkt uit de FAQ van ECB over mogelijke fase na onderzoeksfase.

van e-CNY-gebruikers nadert nu 10% van de bevolking (van bijna anderhalf miljard).

- Binnen Europa loopt Zweden voorop. Zij zijn bezig met de ontwikkeling van de E-krona. In Zweden is het dalende gebruik van contant geld aanleiding geweest om hier onderzoek naar te gaan doen.
- De VS loopt juist iets achter. Met een discussiepaper heeft de FED afgelopen maand het debat over een digitale munt op gang gebracht.
- Canada heeft na een onderzoeksproject te hebben uitgevoerd, besloten dat er momenteel geen noodzaak is voor het invoeren van een digitale munt, gezien de huidige staat van het Canadese betalingssysteem.

Wat zijn de belangrijkste politieke kwesties bij de digitale euro?

- We verwachten dat de belangrijkste politieke kwesties in dit dossier zullen zijn:
  1. Wat wordt de rol van de digitale euro in het financieel systeem? De belangrijkste vraag is waar een digitale euro voor kan worden gebruikt. Wordt het een betaalmiddel, of ook een spaarmiddel? En mogen alleen particulieren er gebruik van maken, of ook bedrijven? Hierbij moet worden nagedacht over welke rol de digitale euro speelt t.a.v. reguliere banktegoeden, en wat de impact van een digitale euro kan zijn op het reguliere bankenlandschap en de rest van de financiële sector.
  2. Wie bepaalt of de digitale euro er komt en hoe die er uit komt te zien? Dit gaat onder andere over de vraag of het bestaande mandaat van de ECB toereikend is om een digitale euro te kunnen invoeren. Ook na de invoering zal er een goede rolverdeling gevonden moeten worden tussen de ECB en de politiek.
  3. Hoe groot mag de rol van de ECB worden in het financiële stelsel? Het risico bestaat dat de ECB private partijen en innovatie wegduwt, door als machtige publieke partij deel te nemen aan een concurrerende markt. De ECB kan ook met een "pettenprobleem" komen te zitten als het zowel toezichthouder als marktpartij wordt. Daarnaast kan de balans en daarmee de rol van de ECB in de economie groter worden bij invoering van een digitale euro.
  4. Wat wordt de balans tussen privacy voor gebruikers en het tegengaan van witwassen/belastingontduiking? Privacy is een belangrijk aspect bij dit thema. Tegelijkertijd is het lastig voorstelbaar dat publiek geld niet aan hoge standaarden voldoet op het gebied van het tegengaan van witwassen, terrorismefinanciering en belastingontduiking. Dat zijn twee belangen die kunnen schuren.
- De belangrijkste technische ontwerpkeuzes beschrijven we nader in bijlage 1.

Wat zijn Nederlandse prioriteiten bij de digitale euro?

- We zien voor Nederland een actieve rol in het digitale euro-dossier. Nederland loopt voor wat betreft digitalisering en innovatie in het betalingsverkeer en de bredere economie, en heeft een relatief grote financiële sector.
- Hieronder schetsen we aan aantal mogelijke prioriteiten (ter bespreking) van Nederland bij de digitale euro. Aan de hand van deze prioriteiten kunnen we toetsen of invoering van de digitale euro wenselijk is en kunnen we onze inzet bepalen in Europa.

Prioriteit	Toelichting
Toekomstgericht en innovatief	- Op dit moment behoort ons betalingsverkeer tot de top van de wereld, de digitale euro kan helpen om dat in de toekomst te blijven. - De digitale euro moet bijdragen aan verdere digitalisering van de economie. De digitale euro moet met nieuwe toepassingsmogelijkheden verdere innovatie aanjagen.
Autonomie en borgen maatschappelijk belang	- In een wereld waarbij de geopolitieke scheidslijnen sterker naar voren komen, dient de digitale euro te helpen de Europese autonomie te vergroten. - Het is van belang dat kritieke (financiële) infrastructuur in publieke handen komt/blijft. - Het is van belang dat iedereen met een publiek betaalmiddel moet kunnen blijven betalen, ook als betalingen steeds vaker digitaal plaatsvinden.
Meerwaarde	- De digitale euro moet vanuit gebruikersperspectief (de potentie) een duidelijke meerwaarde hebben ten opzichte van bestaande alternatieven. - Meerwaarde kan zitten in kosten voor gebruikers, veiligheid en gebruiksmogelijkheden.
Financiële stabiliteit	- De digitale euro mag niet ten koste gaan van de financiële stabiliteit. - Tegelijkertijd is het bredere maatschappelijk belang leidend, niet de gevestigde positie van banken en bedrijven.
Privacy	- De digitale euro moet voldoen aan de hoogste privacystandaarden. Hiermee kan de EU deze standaarden "exporteren" voor andere CBDC's - De digitale euro dient niet ten koste te gaan van AML/terrorismefinanciering.
Democratische legitimiteit en goede governance	- Het primaat voor het besluit tot invoering moet liggen bij de politiek. - Tegelijkertijd moeten we uitvoeringsbeslissingen delegeren aan de ECB. De ECB moet impopulaire beslissingen kunnen nemen in de context van haar mandaat (zoals prijs- en financiële stabiliteit). - In de governance moeten belangenconflicten bij de ECB in haar rol als toezichthouder en uitgever van de digitale euro zoveel mogelijk worden voorkomen.

Vervolgstappen
Wij zullen u separaat adviseren over de thema's die besproken worden in de bijeenkomsten van de Eurogroep later dit jaar. Tevens zullen we werken aan de voorbereiding van de aan de vaste commissie Financiën door uw ambtsvoorganger toegezegde 'contourenschets van de keuzes in het onderzoek naar de digitale euro'.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.

Bijlage 1. Belangrijkste technische keuzes tav digitale euro

Onderwerp	**Toelichting**
Beschikbaarheid en gebruik online en offline	Het gaat hier om de vraag of je de digitale euro ook offline (vergelijkbaar met bijvoorbeeld destijds de chipknip) moet kunnen gebruiken.
Gebaseerd op een account of op een draaginstrument	De vraag is of gebruikers een rekening moeten aanhouden bij de centrale bank (zoals je nu ook een bankrekening hebt), of dat de waarde in de drager van het instrument verwerkt wordt (zoals contant geld).
Middelen om te voorkomen dat bankruns plaatsvinden	Het gevaar bestaat dat mensen, zeker in tijden van stress, in korte periode veel geld weghalen van hun bank door deze in te wisselen voor digitale euro's. Dat kan leiden tot financiële instabiliteit. Mogelijk kan dit voorkomen worden door een limiet te zetten op de hoeveel geld die aangehouden kan worden, een limiet te zetten op de totale waarde van transacties op één dag of het aanhouden van grotere bedragen via rente erg onaantrekkelijk te maken.
Ontwerpkeuzes op het gebied van privacy	Dit vraagstuk gaat over de herleidbaarheid van informatie naar het individu en de mate waarin de overheid mag bepalen welke betalingen wel en niet mogen plaatsvinden. De vraag is hoeveel informatie je van gebruikers wilt hebben zowel bij het aanmaken van een account, als bij het doen van transacties, en hoe deze informatie wordt beveiligd en opgeslagen. Daarbij valt een onderscheid te maken tussen de ECB en private intermediairs als de partij die de gegevens ontvangt. Private partijen kunnen immers een commercieel belang hebben bij het ontvangen van transactiedata van individuele gebruikers. Daarnaast dient privacy afgewogen te worden tegen voldoende waarborgen om bijvoorbeeld witwassen tegen te gaan.
Hoe de digitale euro onder de motorkap werkt	Hierover is nog weinig bekend. Het Eurosysteem verkent de opties en sluit nog geen technieken uit. Zogenaamde *Distributed Ledger Technology* (DLT), zoals bijvoorbeeld Blockchain, wordt bijvoorbeeld ook onderzocht.
Rol van intermediairs in dienstverlening	De vraag is of consumenten voor de digitale euro rechtstreeks hun saldo zouden moeten kunnen beheren bij de centrale banken, of dat private intermediairs hun eerste aanspreekpunt zijn voor de afwikkeling van transacties. De ECB heeft al het signaal afgegeven dat ze opteren voor een model met een sterke rol voor private intermediairs.
Programmeerbaarheid en andere functionaliteiten	De vraag is of de digitale euro de optie dient te hebben om transacties te programmeren, toegesneden op specifieke situaties of omstandigheden. Daarnaast komt de vraag op of er nog andere functionaliteiten nodig of behulpzaam zijn bij de eventuele introductie van de digitale euro.
Grensoverschrijdend gebruik	Hier is van belang of, en in welke mate, de digitale euro gebruikt zou moeten kunnen worden voor de afwikkeling van transacties buiten de Eurozone.

Ministerie van Financiën

TER INFORMATIE
Aan
5.1.2e

Directie Financiële Markten
5.1.2e

nota

Overzicht beleid t.a.v. veiligheid van de financiële sector

Datum
17 oktober 2023

Notanummer
2023-0000234423

Bijlagen
Lijst vitale financiële instellingen

Aanleiding

FM is beleidsverantwoordelijk voor de veiligheid van vitale financiële instellingen in Nederland. N.a.v. een eerder verzoek van u, 5.1.2e wordt in deze nota specifiek stilgestaan bij de wet Vifo. Voor u, 5.1.2e maakt onderscheid op drie terreinen: cyberveiligheid, fysieke veiligheid en economische veiligheid. In deze nota een overzicht van de beleidsacties die FM op dit gebied onderneemt en waar door capaciteitsgebrek is gekozen voor mindere inzet.

Kernpunten

- In Nederland is het betaal- en effectenverkeer als vitale infrastructuur aangemerkt. 20 instellingen zijn als vitale aanbieder aangewezen (Bijlage I). Dit betekent dat deze instellingen bij (dreigende) uitval bijstand kunnen vragen van het Nationaal Cyber Security Centrum.
- Sinds 1 juni 2023 is de Wet Vifo van kracht in Nederland. De wet introduceert een veiligheidstoets voor investeringen, fusies en overnames die de nationale veiligheid kunnen bedreigen. Deze toets geldt voor vitale aanbieders en bedrijven met gevoelige technologie, die veranderingen in zeggenschap moeten melden bij het Bureau toetsing en investeringen (BTI). Het BTI beoordeelt het veiligheidsrisico en kan indien nodig voorwaarden aan de investering koppelen (in uiterst geval blokkeren of terugdraaien).
- FM is beleidsverantwoordelijk voor de nu 20 financiële instellingen die als vitaal zijn aangemerkt en onder Vifo vallen (zie bijlage I voor lijst).

Toelichting

Wet Vifo en Bureau Toetsing Investeringen

- De Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) introduceert een veiligheidstoets voor investeringen, fusies en overnames die een risico kunnen zijn voor de nationale veiligheid. Het gaat hierbij om investeringen die leiden tot significante zeggenschap in het betreffende bedrijf. De veiligheidstoets geldt voor twee soorten bedrijven in Nederland: vitale aanbieders en ondernemingen die beschikken over sensitieve technologie. Deze partijen moeten zelf een wijziging van zeggenschap melden (i.e., fusie of overname) bij Bureau toetsing en investeringen (BTI) waarna BTI een beoordeling maakt of er een risico is voor de nationale veiligheid. Indien dit het geval is, kunnen er voorwaarden verbonden worden aan de investering. In uiterst geval kan de investering worden tegengehouden/teruggedraaid.

- Daarnaast moeten meldingen ook gedeeld worden met andere EU-lidstaten. Op deze manier kunnen lidstaten signaleren wanneer een lidstaat een bepaalde investering goedkeurt, maar de andere lidstaat alsnog risico's ziet.
- Wanneer een melding betreffende een vitale financiële instelling leidt tot een veiligheidstoets wordt FIN hierbij betrokken. Dit kan op twee manieren:
    - FIN kan deelnemen aan het onderzoek en operationeel meedoen aan de veiligheidstoets. De veiligheidstoets leidt tot een rapport met daarin de nationale-veiligheidsrisico's.
    - FIN wordt enkel betrokken bij de weging van de nationale-veiligheidsrisico's als beschreven in het rapport. FIN adviseert samen met BTI en de betrokken ministers over de voorgenomen investering.
- Hoewel BTI een proces heeft vormgegeven over het uitvoeren van de veiligheidstoets en de rol van de vakdepartementen; moet het proces zich uitkristalliseren in de praktijk. Tot op heden heeft er nog geen toets plaatsgevonden voor een financiële instelling.
- De rol van AFM en DNB lijkt tijdens toetsingsproces bescheiden. Informatie van AFM en DNB, zoals input voor en de uitkomsten van personentoetsing, zijn toezichtvertrouwelijk. FM gaat verder in gesprek met AFM & DNB om te bepalen hoe beide in het toetsingsproces worden meegenomen en of toezichthouders en BTI daadwerkelijk dezelfde relevante gegevens hebben.
- Twee medewerkers van FM zijn aangewezen als contactpersoon voor FIN ten aanzien van alle meldingen over financiële instellingen die bij BTI binnenkomen. Voorts ontvangt BTI alle meldingen van investeringen, fusies en overnames in financiële instellingen in andere landen, die in de EU worden gemeld aan de CIE. BTI deelt deze gegevens met FM (voor zover het dus gaat om een investering in een vitale financiële instelling in een andere lidstaat). Dit is tot op heden nog niet gebeurd.

Economische veiligheid & directie Financiële markten

- Op dit moment bestaat het team dat zich met dit onderwerp bezighoudt uit 3 man/vrouw, en bij elkaar grofweg 0,8-1 fte. Vanwege deze beperkte capaciteit zijn er keuzes gemaakt op welke onderwerpen wij inzetten.
- In de tabel onder toelichting staat een overzicht van de lopende beleidsacties.

Beleidsactie	Inzet
Vitaal algemeen	
Beleidscyclus vitaal	
Met de NCTV is afgesproken dat elke vier jaar de "beleidscyclus vitaal" moet worden doorgenomen. Hierbij bekijkt elk departement of alle sectoren die als vitaal worden geacht als zodanig worden aangemerkt.	FIN gaat als onderdeel van de beleidscyclus vitaal bepalen, in samenwerking met AFM & DNB, welke partijen vitaal worden. De cyclus zal op korte termijn starten, met besluitvorming voorzien in de loop van 2024. Er moet uiteindelijk in ieder geval een besluit op politiek niveau genomen moeten waarna ook de Kamer geïnformeerd dient te worden. Dit is een belangrijk traject, maar we hebben slechts beperkte capaciteit. AFM en DNB hebben ook aangegeven weinig ruimte te hebben. We zouden daarom de optie open willen houden om evt. externe hulp in te zetten.
Bevoegde autoriteit	
Vanwege de nieuwe systematiek in de NIS2 en CER-richtlijnen (zie verderop) en de implementatie hiervan in nationale wetgeving,	Met de implementatie van NIS2 en CER, en de eventuele andere partijen die in de betaalcyclus geïdentificeerd worden, zal het aantal vitale instellingen groter worden

zal Financiën als bevoegde autoriteit worden aangewezen om partijen formeel als vitaal aan te wijzen. Momenteel is dat DNB. wijst DNB de vitale financiële instellingen aan omdat al deze instellingen op één na onder het vergunnings- en toezichtregime van DNB vallen. Dit gaat veranderen, waardoor ook meer AFM-partijen waarschijnlijk als vitaal worden aangemerkt.	dan de huidige 20. Tot nu staan al deze partijen, op 5.1.1b na, onder (formeel of informeel) toezicht van DNB, waardoor het logisch is dat DNB de bevoegde autoriteit is om partijen als vitaal aan te merken (i.o.m. Financiën). Echter, wij verwachten dat er meer AFM-partijen als vitaal gaan kwalificeren, waardoor het logischer is om Financiën als bevoegde autoriteit aan te wijzen (dit is ook hoe andere departementen dit doen). Praktisch betekent dit dat FM t.z.t. formeel partijen als vitaal moet aanwijzen. Op dit moment is het onduidelijk hoe veel structurele capaciteit dit vergt. De verwachting is dat dit meevalt, maar dit moeten wij de komende tijd in kaart brengen.
Cyberveiligheid	
Verordening digitale operationele weerbaarheid (DORA)	
De EU-verordening digitale operationele weerbaarheid harmoniseert bestaande cyberveiligheidsregels voor financiële instellingen en introduceert nieuwe regels voor de sector met als doel een hoog niveau van cyberweerbaarheid te bewerkstelligen.	DORA treedt in januari 2025 in werking. Momenteel ligt de uitvoeringswetgeving voor DORA bij de Raad van State voor advies. Wij verwachten de wetgeving op korte termijn in te kunnen dienen bij de Tweede Kamer. DORA is een prioriteit voor FM.
Richtlijn Netwerk- en Informatiesystemen (NIS2)	
De herziene richtlijn Netwerk- en Informatiesystemen (NIS2) stelt horizontale regels op het gebied van cyberveiligheid. JenV is beleidsverantwoordelijk.	DORA is lex specialis op NIS2, wat betekent dat DORA voorgaat op NIS2. Desondanks vloeit er voor Financiën wel werk uit. De implementatie van DORA moet in lijn lopen met NIS2 (en vice-versa) wat afstemming nodig maakt. Daarnaast zijn er een aantal financiële instellingen die wel al vitaal zijn, maar niet onder DORA en NIS2 vallen. Er moet voor gezorgd worden dat deze partijen goed meegenomen zijn in de wetgeving. Wij hebben gezien beperkte capaciteit gekozen ons alleen te focussen op die interdepartementale gremia voor de implementatie van NIS2 waar raakvlakken zijn met DORA. Dit betekent echter wel dat wij soms minder goed zijn aangesloten of mogelijk iets missen.
Fysieke veiligheid	
Richtlijn weerbaarheid kritieke entiteiten (CER)	
De richtlijn weerbaarheid kritieke entiteiten (CER) introduceert regels voor de fysieke bescherming van vitale sectoren en instellingen. JenV is beleidsverantwoordelijk.	Ook hier geldt dat DORA lex specialis is, dus de inzet voor CER is dezelfde als voor NIS2. Ook hier geldt dat wij uit eigen keuze beperkt betrokken zijn gezien de capaciteit.
Economische veiligheid	
Wet veiligheidstoets investeringen, fusies en overnames (Vifo)	
De Wet vifo introduceert een veiligheidstoets voor investeringen in, of fusies en overnames van vitale instellingen. Hierbij wordt specifiek gekeken naar risico's voor de nationale veiligheid.	De toetsen worden uitgevoerd door Bureau Toetsing Investeringen (BTI) van EZK. Indien BTI risico's ziet, geeft het een advies aan de ministers van EZK, JenV en de relevante vakminister, die gezamenlijk besluiten of de investering moet worden tegengehouden. Vifo is van toepassing op alle instellingen die als vitaal zijn aangemerkt. Dit betekent dat de 20 vitale financiële instellingen hieronder vallen, en dat toekomstige vitale instellingen hier ook onder gaan vallen. Wij verwachten

	dat dit slechts incidenteel zal spelen en kunnen dit naar verwachting opvangen binnen de huidige capaciteit mocht er een toets gedaan worden in de financiële sector.
Screenen van vertrouwensfuncties bij vitale aanbieders	
Samen met BVA onderzoekt FM of bepaalde functies bij vitale financiële instellingen als vertrouwensfunctie moeten worden aangemerkt. Dit na een vraag vanuit de veiligheidsdiensten.	Momenteel worden er gesprekken gevoerd met BVA, DNB en de AIVD om te bekijken of dit nodig is en waarom, en wat dit betekent voor de financiële instellingen en de unit die de veiligheidsonderzoeken uitvoeren. Aangezien dit een kortdurend project is, is dit voorlopig op te vangen binnen de huidige capaciteit maar heeft het geen prioriteit.
Europese economische veiligheidsstrategie	
Economische veiligheid treedt steeds meer op de voorgrond. De recente Europese economische veiligheidsstrategie heeft tot doel de economische veiligheid van de EU te beschermen. De strategie voorziet in een expertgroep die kijkt naar een nieuw op te richten instrument om investeringen naar het buitenland te screenen (omgekeerde vifo). Recentelijk heeft de VS een dergelijk instrument gelanceerd.	BZ en EZK zijn primair verantwoordelijk. Binnen Financiën is BFB primair verantwoordelijk. FM kijkt en doet mee voor het geval het instrument de financiële sector zou raken (zoals het geval is bij de VS). De meeste lidstaten lijken niet voornemens een nieuw instrument op te tuigen en zien meer in uitbreiding van bestaande exportcontrolemechanismen. FM kan alleen beperkte capaciteit leveren.

Vooruitblik en aandachtsgebieden

Economische veiligheid

- Er is veel aandacht voor economische veiligheid. BZ en EZK zijn hier primair beleidsverantwoordelijk voor.
- Vifo is een uitvloeisel van de EU-verordening tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie (FDI verordening), die in oktober 2020 inwerking is getreden. Het raamwerk wordt door de Europese Commissie geëvalueerd als onderdeel van de Europese Economische veiligheidsstrategie.
- Andere jurisdicties denken na over aanvullende beleidsmaatregelen op buitenlandse investeringen. Zo heeft de VS een screeningmechanisme en verbod voor investeringen naar China. Hoewel het middel (de investering) financieel is, is het onderliggende beleidsvraagstuk economisch en geopolitiek van aard. Tevens zullen mogelijk restrictieve maatregelen voor dit type investeringen gewogen moeten worden met het Nederlands beleid op vestigings- en investeringsklimaat dat onder EZK valt.

5.1.2a

Andere onderwerpen

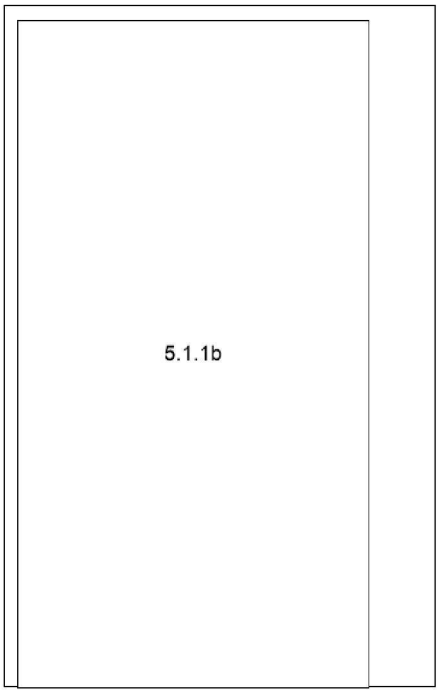
5.1.1b

Communicatie
Niet van toepassing.

Politiek/bestuurlijke context
Economische veiligheid heeft de aandacht van de TK. Op 28 maart 2023 is een motie van het lid Heinen aangenomen over of de Wet vifo voldoende waarborgen biedt om te voorkomen dat privacygevoelige data of vitale onderdelen van de financiële sector belanden bij landen met hoge veiligheids- en spionagerisico's. Op 6 juli 2023 heeft het lid Rajkowski een motie ingediend over het in kaart brengen in hoeverre (analoge) terugvalopties nodig zijn voor het versterken van onze digitale weerbaarheid bij de eerstvolgende digitale weerbaarheids-analyse.

Informatie die niet openbaar gemaakt kan worden
Informatie over vitale financiële instellingen inclusief bijlage 1.

BIJLAGE I Lijst vitale financiële instellingen



Ministerie van Financiën

TER BESLISSING
5.1.2e

Generale Thesaurie
Directie Financiële Markten

5.1.2e

nota

Verzoek uitvoeringstoet uitvoeringsbesluit digitale operationele weerbaarheid financiële sector

Datum
16 januari 2024

Notanummer
2024-0000173519

Bijlagen
1. Uitvoeringstoets DNB
2. Uitvoeringstoets AFM
3. Uitvoeringsbesluit

Aanleiding

Binnenkort zal de openbare consultatie starten van het uitvoeringsbesluit digitale operationele weerbaarheid financiële sector (DORA). Het besluit is geagendeerd voor de MR van 17 mei. Via bijgevoegde brieven worden DNB en AFM verzocht om een uitvoeringstoets te doen op dit besluit.

Beslispunten

U wordt geadviseerd in te stemmen met de brief aan DNB en AFM (bijlage 1 en 2). Als u zich daarin kunt vinden, verzoeken wij deze te ondertekenen.

Kernpunten

- Op 16 januari 2023 is de verordening Digitale operationele weerbaarheid in de financiële sector (DORA) in werking getreden. Het DORA-pakket bestaat uit twee stukken EU-wetgeving: een verordening en een richtlijn.
- De richtlijn en de verordening vormen een gezamenlijk kader ter verbetering van de digitale operationele weerbaarheid voor de financiële sector.
- De verordening is vanaf 17 januari 2025 van toepassing en de richtlijn dient voor dezelfde datum geïmplementeerd te zijn.
- Voor de richtlijn dienen wijzigingen op wets- en besluitniveau doorgevoerd te worden. Deze wijzigingen zijn nodig zodat de artikelen niet strijdig zijn met de verordening.
- Het besluit regelt dat de Autoriteit Financiële Markten (AFM) en de Nederlandsche Bank (DNB) als bevoegde autoriteiten als bedoeld in de verordening worden aangewezen. Ook de sanctionering van overtredingen van de verordening wordt middels dit uitvoeringsbesluit geregeld. Het onderliggende verzoek voor een uitvoeringstoets richt zich hierop.

Toelichting

- Digitale operationele weerbaarheid (ICT en cyberweerbaarheid) speelt een steeds grotere rol voor financiële instellingen. De financiële sector is in toenemende mate afhankelijk van ICT en digitale dienstverlening. Verstoring en uitval van ICT-systemen kunnen leiden tot risico's voor de financiële stabiliteit. Ook de toenemende dreiging van statelijke actoren en andere kwaadwillende tonen aan dat het belangrijk is dat instellingen systemen hebben zodat ze weerbaarder zijn voor ICT en cyberincidenten.

- DORA heeft verschillende doelen:
    - Bestaande sectorale ICT-eisen worden gecentraliseerd op één plek.
    - Er worden regels geïntroduceerd voor financiële instellingen om ICT-risico's te beheersen;
    - Ernstige ICT-incidenten dienen te worden gemeld bij de toezichthouders en er dienen systemen te worden opgezet om incidenten te monitoren, vast te leggen en te classificeren;
    - Instellingen dienen hun digitale weerbaarheid periodiek te testen;
    - Er worden regels geïntroduceerd voor derde partijen die ICT-diensten aanbieden aan financiële instellingen. Deze komen ook, indien ze kritiek zijn bevonden, onder licht toezicht (oversight) van de ETA's te vallen.

Communicatie
N.v.t.

Politiek/bestuurlijke context
N.v.t.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.

Ministerie van Financiën

DEPARTEMENTAAL VERTROUWELIJK
TER INFORMATIE
Aan
de minister

Directie Financiële Markten

5.1.2e
5.1.1c
5.1.2e

nota

Multisafepay

Datum
7 februari 2024

Notanummer
2024-0000161802

Bijlagen
1. NRC-artikel

Aanleiding

NRC schrijft op 6 februari 2024 in het artikel '*Zorgen om Nederlandse betaaldienstverlener die waarschijnlijk in Chinese handen komt*' (bijlage 1) dat het Chinese ANT Group de Nederlandse betaaldienstverlener Multisafepay wil overnemen.

Kernpunten

- NRC bericht dat ANT Group, één van de grootste betaalbedrijven uit China en moederbedrijf van Alipay, de Nederlandse betaaldienstverlener Multisafepay wil overnemen. Dit was weer gebaseerd op een artikel van Reuters van 5 januari 2024.
- Multisafepay is een relatief kleine Nederlandse betaaldienstverlener, met een omzet van €12 mln. in 2022 en 18.000 klanten in de gehele EU.[1] Multisafepay biedt online betaalplatforms aan, waarmee klanten kunnen kiezen tussen verschillende betaalmethodes.
- In het artikel uiten MEP-er Bart Groothuis en Clingendael-deskundigen hun zorgen over de overname, gezien de groeiende strategische rol van data in de financiële sector en de kans dat de overname er in hun ogen kan leiden dat gevoelige betaalgegevens kunnen doorvloeien naar de Chinese overheid. Hierbij wordt de wet Vifo genoemd als mogelijk instrument om de overname tegen te houden.
- De wet Vifo is op dit moment echter niet van toepassing op betaaldienstverleners. Betaaldienstverleners zijn momenteel niet als vitaal aangemerkt. Indien Nederland het onwenselijk vindt dat Multisafepay door ANT Group overgenomen zou worden, dan kan dat dus op dit moment niet via de wet Vifo worden geblokkeerd.
- De Chinese betaaldienstverleners ANT Group en Tencent zijn momenteel overigens al actief in NL. Alipay, onderdeel van de ANT Group, heeft zelfs een Nederlandse vergunning als afwikkelonderneming (verwerker van betalingen). Dit was een *greenfield* investering. Tencent heeft geen vergunning in NL, maar wel een kantoor in Amsterdam, dat dient als EU-hoofdkantoor.
- Wij hebben contact met de NCTV om eventuele risico's van deze overname, en mogelijke manieren om deze te mitigeren, in kaart te brengen. Wij zullen u hierover binnenkort nader over informeren.

[1] Ter vergelijking: Mollie had in 2022 een omzet van €123 mln., en Adyen €1,3 mld.

Toelichting

Samenvatting NRC-artikel

- De Nederlandse betaaldienstverlener Multisafepay staat mogelijk op het punt overgenomen te worden door de Chinese ANT Group, moederbedrijf van Alipay, voor ongeveer $200 miljoen.
- In het artikel wordt door een expert gespeculeerd dat ANT Group met deze overname een positie wil verwerven in het Europese betalingsverkeer.
- Daarnaast uiten experts in het artikel bezorgdheid over de mogelijke toegang van een Chinese multinational tot financiële transactiedata en de gevolgen voor nationale veiligheid.
- Europarlementariër Bart Groothuis waarschuwt voor de macht van een Chinees bedrijf in het Europese financiële landschap en roept op tot Europese betrokkenheid in de besluitvorming.
- Analisten van Clingendael benadrukken dat de overname een strategische afweging vereist, gezien de groeiende rol van data in de financiële sector, en suggereren mogelijk voorwaarden voor goedkeuring. De analisten noemen de wet Vifo als mogelijk instrument om de overname tegen te houden.

Risico-inschatting NCTV

- 5.1.1b
- Chinese betaaldienstverleners zijn al actief in Nederland. FIN heeft bij de NCTV aandacht gevraagd voor mogelijke inconsistenties wanneer de overname van Multisafepay wordt geblokkeerd terwijl ANT Group door middel van greenfieldinvesteringen wel actief is in NL. Deze dienstverlening ziet met name op het bedienen van Chinese toeristen door Alipay aan te bieden op locaties waar veel Chinese toeristen komen. Tot nu toe hebben ze zich niet op Nederlandse consumenten gericht.
- We gaan samen met NCTV de risico's uitwerken, en bekijken of er eventuele mitigerende maatregelen getroffen zouden kunnen worden.

Juridische mogelijkheden

- De Wet veiligheidstoets investeringen, fusies en overnames (Vifo) is sinds 2023 inwerking. De wet Vifo maakt een veiligheidstoets mogelijk voor overnames van vitale instellingen of bedrijven die sensitieve technologieën ontwikkelen die een risico vormen voor de nationale veiligheid.
- Het tegenhouden van nationale investeringen op grond van nationale veiligheid is een vergaande maatregel. Daarom heeft Nederland ervoor gekozen om de nationale veiligheidstoets onder de wet Vifo alleen in te voeren voor vitale instellingen of sensitieve technologie, essentieel voor de Nederlandse vitale infrastructuur. Een overname van Multisafepay brengt geen direct gevaar voor Nederlandse vitale infrastructuur, aangezien het niet gaat om een vitale instelling. Multisafepay is een kleine partij, en een eventuele verstoring zou weinig effecten hebben op het betalingsverkeer en de rest van de financiële sector.
- DNB dient bij een elke deelneming of overname in Nederland een verklaring van geen bezwaar (vvgb) af te geven. Ook kijkt DNB naar prudentiële risico's.

- Als er een concreet signaal is dat er risico's zijn, zou dat met DNB gedeeld kunnen worden en zouden ze dit meekunnen nemen in besluitvorming over de vvgb. Multisafepay is een kleine partij, waarbij de prudentiële risico's beperkt zijn. Wij verwachten dat DNB moeilijk een vvgb kan weigeren.
- 5.1.1b
- Vooralsnog lijken de juridische mogelijkheden beperkt om de overname tegen te houden. Als we Multisafepay wel onder Vifo willen brengen duurt dit in allerbeste scenario 5 maanden, maar waarschijnlijk 8 tot 9 maanden. Hierbij geldt dat Multisafepay een bescheiden omzet heeft (€12 mln. in 2022) en dat het eerste nieuws van het bod al van begin januari is (Reuters). Het is dus de vraag over het bedrijf überhaupt groot genoeg zou zijn om onder de wet Vifo te vallen en een uitbreiding van de reikweidte van Vifo zal zeer waarschijnlijk te lang gaan duren.

Vervolg

- 5.1.1b
- 5.1.1b
- Tegelijkertijd zijn wij begonnen met het onderzoeken of er binnen de financiële sector nog nieuwe onderdelen als vitaal aangemerkt dienen te worden. Hierbij gaan wij expliciet ook naar betaalinstellingen kijken. Betaalinstellingen worden ook door de EC genoemd in het recent verschenen voorstel om nationale investeringscreeningsregimes te harmoniseren. Het is echter de vraag of Mulitsafepay na deze herziening überhaupt als groot genoeg zou worden geacht om onder Vifo-toets te vallen.

Communicatie
n.v.t.

Politiek/bestuurlijke context

- BZ heeft de casus deze week ingebracht bij de Taskforce Economische Veiligheid. Mogelijk wordt het binnenkort ook in de RVI geagendeerd. Wij zullen u dan nader adviseren.
- De discussie over uitgaande en ingaande investeringen wordt gevoerd. Zowel de Tweede Kamer heeft hier aandacht voor als ook de Europese Commissie.

Informatie die niet openbaar gemaakt kan worden

De nota bevat mogelijk informatie die raken aan bedrijfsgevoelige informatie of informatie die raakt aan de nationale veiligheid en daardoor niet gedeeld kunnen worden.

Ministerie van Financiën

DEPARTEMENTAAL VERTROUWELIJK
TER BESLISSING
Aan
de minister

Generale Thesaurie
Directie Financiële Markten

5.1.2e

nota

Voorstel bijgestelde beleidscyclus vitaal in lichte vorm en wijziging Wet Vifo

Datum
23 februari 2024

Notanummer
2024-0000190998

Bijlagen
1. lijst type financiële instellingen

Aanleiding

- U heeft gevraagd om te kijken naar de mogelijkheden voor een versnelde vitaalbeoordeling voor de financiële sector.
- We doen in deze nota een voorstel voor het uitvoeren van een lichte variant van de beleidscyclus vitaal en eventueel het wijzigen van de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) naar aanleiding van de toelichting omtrent de nationale veiligheid die wij op 16 februari ontvangen hebben.

Beslispunten

1. Bent u akkoord met het versneld doorlopen van de beleidscyclus vitaal (circa 6 maanden in plaats van twee jaar) voor de gehele financiële sector? De instellingen waarvan mogelijk uit deze beleidscyclus volgt dat ze vitaal moeten zijn, kunnen vervolgens per AMvB onder de reikwijdte van de Wet Vifo gebracht worden (dat duurt circa 1 jaar) of in het reguliere traject met wetswijziging van 2 tot 3 jaar.
2. Bent u tevens akkoord om de Tweede Kamer langs de lijnen van deze nota te informeren (wij leggen u dan binnenkort een conceptbrief voor)?

Kernpunten

- De beleidscyclus vitaal zou dit jaar gestart worden voor vier processen binnen de financiële sector, te weten het betaal- en effectenverkeer en pensioen- en verzekeringsprocessen. Hierbij wordt beoordeeld of deze processen als vitaal aangemerkt dienen te worden, en zo ja, welke instellingen binnen deze processen. Na deze beoordeling kunnen deze partijen onder het bereik van de Wet Vifo worden gebracht.
- Deze beleidscyclus kent normaliter een doorlooptijd van twee jaar, waarbij ook onafhankelijk advies wordt ingewonnen en uitgebreid met de sector en toezichthouders wordt gesproken.
- Naar aanleiding van 5.1.2i en berichten omtrent de nationale veiligheid willen we voorstellen de beleidscyclus versneld en in lichte vorm te doorlopen (circa 6 maanden), waarna deze – indien nodig – opgevolgd kan worden met een AMvB ter wijziging van de vitale processen die onder de Wet Vifo vallen, of met een reguliere wetswijziging.

- Omdat het bericht omtrent de nationale veiligheid niet ziet op één specifieke sector of partij, zal deze exercitie zich in eerste instantie richten op de gehele financiële sector en dus verder gaan dan de oorspronkelijke afbakening tot de vier eerdergenoemde processen. Hierbinnen wordt gezocht naar de juiste afbakening om de opname van bepaalde sectoren in de Wet Vifo proportioneel en effectief te houden.
- Het versneld uitvoeren van de vitaalcyclus zal gevolgen hebben voor de kwaliteit en kosten van de beleidscyclus. Zo hebben we minder tijd dan de eerst voorgestelde twee jaar om marktonderzoek te doen en uitgebreid met toezichthouders en instellingen te spreken. Tevens kan dit versnelde traject ertoe leiden dat capaciteit op andere dossiers beperkt zal worden, en dat er gekeken moet worden naar extern advies.

Toelichting

- Overwegingen van nationale veiligheid vereisen in onze ogen op dit moment geen spoedaanpassing van de Wet Vifo. Wel heeft nationale veiligheid inmiddels onze extra aandacht in relatie tot de financiële sector en achten we het wenselijk de cyclus versneld te doorlopen.
- Een belangrijke vraag is welke grenswaarden aangehouden moeten worden om de reikwijdte van Wet Vifo proportioneel en uitvoerbaar te houden. Hierbij kan, per sector, gekeken worden naar marktaandeel, financiële kerncijfers zoals omzet, hoeveelheid personeel en hoeveelheid klanten. Idealiter vinden we een grenswaarde die voor elk type instelling consistent kan worden toegepast. Dit zal uitdagend zijn gezien de zeer verschillende grootte en aard van de instellingen. Hierdoor lopen de risico's zeer uiteen en zijn deze niet evenredig met de grootte van een instelling. Daarnaast kan het zo zijn dat in bepaalde processen specifieke kleine, gespecialiseerde instellingen alsnog heel belangrijk kunnen zijn.
- Het handboek voor de vitaliteitsbeoordeling en de Europese richtlijn kritieke entiteiten (CER) biedt handvatten om te bepalen wanneer een incident een aanzienlijk verstorend effect heeft. Hierin wordt ook gekeken naar het marktaandeel van de entiteit en het geografische gebied dat door een incident kan worden getroffen. Deze twee elementen kunnen bijvoorbeeld ook meegenomen worden in de bepaling van de grenswaarden.
- Op hoofdlijnen zullen we kijken naar grote, invloedrijke financiële instellingen die veel (gevoelige) persoonsgegevens verwerken en een vitale rol spelen voor de Nederlandse samenleving. De huidige lijst vitale aanbieders in de financiële sector en de EU-verordening digitale operationele weerbaarheid voor financiële instellingen (DORA) biedt een eerste startpunt voor de afbakening van het type instellingen waarnaar gekeken zal worden. Zie bijlage 1 voor een overzicht van de verschillende financiële instellingen, hun activiteiten en of ze op dit moment al vitaal zijn.
- We zullen het Nationaal Cyber Security Centrum, EZK en het Bureau Toetsing Investeringen meenemen in dit traject.
- We gaan bekijken of we de ondersteuning van een externe partij hiervoor kunnen inzetten. De termijnen voor aanbesteding zijn hierbij een aandachtspunt.

Communicatie
N.v.t.

Politiek/bestuurlijke context
- Het belang van de weerbaarheid van de vitale infrastructuur wordt onderschreven door de regering. Zo heeft de minister van Justitie en Veiligheid op 30 mei 2023 een Kamerbrief geschreven over de 'Versterkte aanpak bescherming vitale infrastructuur' waarin ingegaan wordt op de beleidscyclus vitaal en op bewustwording bij vitale aanbieders over het signaleren van risico's.
- Tijdens het commissiedebat van 21 juni 2023 heeft uw ambtsvoorganger ook een toezegging gedaan om te kijken of de Wet Vifo voldoende waarborgen biedt om te voorkomen dat privacygevoelige data of vitale onderdelen van de financiële sector belanden bij landen met hoge veiligheids- en spionagerisico's, naar aanleiding van de motie van het lid Heinen. Hierin wordt toegezegd de vitaalcyclus te starten en de Kamer in de loop van 2024 te informeren over de stand van zaken. Gezien deze toezegging en een eventuele volgende AMvB adviseren wij u nu de Kamer te informeren dat u deze lichtere vorm van de vitaal cyclus start.

Informatie die niet openbaar gemaakt kan worden
Bij eventuele openbaarmaking moet worden bezien of de verwijzingen naar nationale veiligheid gelakt moeten worden.

Ministerie van Financiën

TER ADVISERING
Aan
5.1.2e

Generale Thesaurie
5.1.2e

nota

Voorbereiding DG-overleg maatschappelijke weerbaarheid
14/3 13u

Datum
13 maart 2024

Notanummer
2024-0000206134

Bijlagen
geen

Aanleiding

De NCTV, samen met Defensie, signaleren dat dat de dreiging van een gewapend of hybride militair conflict in de buurt van of in Nederland toeneemt. Daarom is in de NVR-Oek van 30 januari een tweeledige opdracht vastgesteld:

1. Intensiever en geïntegreerd communiceren over de dreiging, de impact op Nederland en noodzaak van voorbereiding, en
2. Verkennen wat een whole-of-society-aanpak in het kader van militaire en hybride dreiging in Nederlandse context betekent en welke vervolgstappen en intensiveringen in dit kader nodig zijn.

Hier wordt interdepartementaal over gesproken. In overleg wordt u gevraagd akkoord te gaan met:

1. Het scenario voor uitwerking van de vervolgopdracht;
2. Twee sporen: versterking militaire paraatheid en maatschappelijke weerbaarheid;
3. Aanpak na DG-overleg;
4. Uitgangspunten voor de uitwerking van de opdracht.

Adviezen

Wij adviseren met bovengenoemde vier punten akkoord te gaan.

Kernpunten

- Het doel van het overleg is de maatschappelijke weerbaarheid van Nederland verhogen in geval een militair conflict waar Nederland bij betrokken is.
- Weerbaarheid verhogen moet via inventarisatie en synergie op bestaande beleidstrajecten.
- Dit overleg dient vooral om bewustzijn te creëren bij alle departementen dat hierover wordt nagedacht en ervoor te zorgen dat er capaciteit wordt vrijgemaakt – wanneer dit laatste nodig is.
- Het uiteindelijke doel van het gehele traject is om een kabinetsbrede Kamerbrief op te stellen en hierin de uitkomsten van de verschillenanalyse en dilemma's tot het komen van een verdringingsreeks uiteen te zetten.

Toelichting

Hieronder spreekpunten per agendapunt.

1. Het scenario voor uitwerking van de vervolgopdracht

- In dit scenario wordt ervan uitgegaan dat Nederland wordt geconfronteerd met een militair conflict in bondgenootschappelijk verband dat is gebaseerd op de *crisis management excercise* 2023 (CMX'23) van de NAVO.

- U kunt noemen dat het goed is dat er met één scenario wordt gewerkt.
- U kunt noemen dat een gewapend conflict met een front in Oost-Europa, Financiën waarschijnlijk niet het eerste departement naar waar wordt gekeken.
- Tegelijkertijd is de vitale financiële infrastructuur vatbaar voor hybride dreigingen. Dit omdat de financiële sector sterk geïntegreerd, gedigitaliseerd en grensoverschrijdend is.
- Daarnaast is de vitale financiële infrastructuur belangrijk voor het functioneren van de maatschappij. Hierbij kunt u opmerken dat vitale financiële infrastructuur belangrijk is voor het maatschappelijke vertrouwen. Wanneer er bijvoorbeeld geen contant geld meer voorhanden is, of betalen is niet meer mogelijk is, kan dit paniek veroorzaken.

2. Twee sporen: versterking militaire paraatheid en maatschappelijke weerbaarheid

1. De versterking van de militaire paraatheid – waar ook inzet van de samenleving bij nodig is (DEF coördinerend) – en;
2. De versterking van maatschappelijke weerbaarheid (JenV coördinerend).

In het licht van het geschetste scenario zijn op dit moment vier kerntrajecten geïdentificeerd:

A. Het Landelijk Crisisplan Militaire Dreiging (LCP-MD).
B. De NAVO Resilience Objectives (RO's).
   - Waar het LCP-MD een kaderstellend civiel-militair crisisplan betreft, beoogt het NAVO RO's traject op basis van NAVO kaders de civiele paraatheid te versterken (incl. mogelijke beleidsvorming en implementatie). Op dilemma's die in beide trajecten in kaart worden gebracht vindt uitwisseling plaats en aanbevelingen uit het LCP-MD proces worden in het NAVO RO's traject meegenomen. In het laatste kwartaal van 2024 vindt gezamenlijke besluitvorming plaats op het concept LCP-MD en de vaststelling van de nationale doelstellingen van de NAVO RO's.
C. Het Nationaal Defensie Plan van cruciaal belang in het kader van dit scenario.
   - Ook het Nationaal Defensie Plan zal eind 2024 worden vastgesteld.
D. Landelijke agenda crisisbeheersing en spoor weerbaarheid.
   - Hierover wordt in het Veiligheidsberaad van 18 maart gesproken met beoogde spoedige verzending aan de Kamer. Dit is een onderdeel van de Veiligheidsstrategie voor het Koninkrijk der Nederlanden.

- Defensie en JenV hebben een eerste verkenning gedaan van de beleidstrajecten die bijdragen aan de maatschappelijke weerbaarheid tegen militaire dreigingen. Deze verkenning is nog niet af.
- Voor FIN staat in deze verkenning: Noodwet financieel verkeer, Wet financieel toezicht, Wet chartaal betalingsverkeer (borgen contact geld, red.), wet Vifo, DORA, vitaalbeoordeling financiële sector, tripartiet crisisoverleg tussen DNB, AFM, FIN.

- U kunt noemen dat het goed is dat er eerst goed wordt gekeken naar wat er al wordt gedaan aan het versterken van de maatschappelijke weerbaarheid. Het lijkt inderdaad het meest logisch om te kijken naar synergie van bestaande trajecten.
- U kunt noemen dat de financiële sector veel instrumenten kent, zoals wet- en regelgeving en sectorcrisismanagement, om de weerbaarheid van de sector te garanderen.
- U kunt noemen dat dit belangrijk is omdat in geval van een hybride dreiging het niet ondenkbaar is dat dit is gericht aan de financiële sector. Dit heeft ermee te maken dat de sector sterk geïntegreerd en grensoverschrijdend is, waardoor een aanval in potentie een groot bereik heeft. Daarnaast kan de financiële sector gebruikt worden voor beïnvloeding en bezitten zij veel (gevoelige) persoonsgegevens. Bovendien is de sector sterk gedigitaliseerd waardoor de sector vatbaar is voor cyberaanvallen.
- De vatbaarheid voor cyberaanvallen is Europees erkend waardoor er nu Europese regelgeving is waardoor de financiële sector haar cyberweerbaarheid verplicht is op orde te hebben (DORA).
- U kunt vragen hoe de geïdentificeerde kerntrajecten zich verhouden tot internationale en Europese samenwerking. Worden dergelijke scenario's ook in andere lidstaten besproken?

3. Aanpak na DG-overleg
- U kunt aangeven dat u zich kan vinden in de planning.

4. Uitgangspunten vervolgtraject
- De NCTV en nota schrijven: "*serieuze stappen te zetten om de weerbaarheid tegen militaire dreigingen te versterken met een focus op civiele en militaire paraatheid en weerbaarheid tegen militaire dreigingen.*" En dat: "*Dit traject doet geen afbreuk aan bestaande (beleids-)verantwoordelijkheden, maar vergt wel versterkte inzet van betrokken departementen. Departementen maken hier dedicated capaciteit voor beschikbaar.*"
- Voor FIN specifiek geldt dat FM nu bezig is om de beleidscyclus vitaal in zes maanden in plaats van twee jaar te voltooien. Het aanwijzen van vitale financiële instellingen kan ingezet worden om deze instellingen onder Wet vifo te laten vallen. Bovendien krijgen deze instellingen bijstand van het Nationaal Cyber Security Centrum in geval van een cyberaanval. Dit verhoogt de weerbaarheid van Financiële instellingen.
- Het voltooien van de beleidscyclus vitaal in zes maanden sluit mooi aan bij de roep om versterkte inzet van betrokken departementen.
- U kunt noemen dat FIN binnen zes maanden de vitaalcyclus voor de financiële sector wil voltooien.
- U kunt noemen het eens te zijn met de uitgangspunten van het vervolgtraject.
- U kunt noemen het eens te zijn dat een maatschappijbrede aanpak. Input en communicatie met bijvoorbeeld vitale instellingen is belangrijk om draagvlak blijvend te creëren.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.

To: 5.1.2e (FM/IBI)[5.1.2e @minfin.nl]
Cc: 5.1.2e 5.1.2e @minfin.nl]; 5.1.2e (FM/IBI)[5.1.2e @minfin.nl]; 5.1.2e (FM/IBI)[5.1.2e @minfin.nl]; 5.1.2e @dnb.nl[5.1.2e @dnb.nl]; 5.1.2e @dnb.nl[5.1.2e @dnb.nl]; 5.1.2e @dnb.nl[5.1.2e @dnb.nl]; 5.1.2e @dnb.nl[5.1.2e @dnb.nl]
From: 5.1.2e @dnb.nl
Sent: Wed 7/24/2024 1:52:55 PM
Subject: RE: Dreigingsscenario [Decrypted using DNB TLS][Encrypted using DNB TLS]
Received: Wed 7/24/2024 1:53:08 PM

Beste 5.1.2e

We hebben intern even geschakeld hoe we e.e.a. kunnen accommoderen. Ik heb ook kort even met 5.1.2e gesproken over een mogelijke opzet, die ons brengt naar een afdronk die we met jullie kunnen bespreken in oktober.

We richten binnen DNB een klein kernteam op die de voorbereidingen treft en de bevindingen zal opstellen, met daarin opgenomen het TCO secretariaat. Het TCO secretariaat lijkt inderdaad een goed punt van coördinatie, dus 5.1.2e zal jullie liaison zijn. Dat schakelt makkelijk. Het idee op dit moment is om het scenario eerst per organisatie door te exerceren en daarna de bevindingen in oktober met elkaar te delen. Dat houdt het compact en à tempo.

Onderstaande beschrijving plaatst het effectenverkeer buiten scope en begrenst de exercitie tot onze twee organisaties. Mocht dat toch anders zijn, dan horen we dat graag.

Met vriendelijke groet,

5.1.2e

Van: 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>
Verzonden: dinsdag 23 juli 2024 16:37
Aan: 5.1.2e (BCM_BCM) <5.1.2e @dnb.nl>
CC: 5.1.2e 5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>
Onderwerp: RE: Dreigingsscenario [Decrypted using DNB TLS][Encrypted using DNB TLS]

External: Pause and review the sender's email address, any URLs before clicking links, opening attachments, or following requests. When in doubt, contact our CDC via the scam mailbox, use the report message or the report scam button..

Beste 5.1.2e

5.1.1b

5.1.1b Het gaat om de volgende deelopgaven:

- Zorgdragen voor betrouwbaar, weerbaar en veilig betalingsverkeer ten behoeve van de maatschappij, die ook continueert bij langdurige ontwrichting.
- Zorgdragen voor de continuïteit van de vitale processen: financiering van de staatsschuld, schatkistbankieren, en betalingsverkeer van het Rijk.

Ook heb ik het format voor de zogenaamde quickscan bijgevoegd die wij moeten invullen.

Graag leggen we dit scenario eens naast bestaande scenario's van DNB zodat we gezamenlijk kunnen bekijken of deze scenario's en noodplannen voldoende zijn, of er zaken missen en zo ja hoe we dit verder kunnen oppakken. We kunnen dit in TCO-verband doen. Met wie uit jouw organisatie kunnen we het beste contact opnemen? Mocht er behoefte zijn om eerst het een en ander (telefonisch) verder toe te lichten dan hoor ik dat graag.

Bij voorbaat dank en met vriendelijke groet,

5.1.2e
Senior beleidsmedewerker
Afdeling Institutioneel Beleid, Betalingsverkeer en Integriteit (IBI)
.....
Ministerie van Financiën
Generale Thesaurie | Directie Financiële Markten
Korte Voorhout 7 | 2511 CW | Den Haag
Postbus 20201 | 2500 EE | Den Haag
.....
T 5.1.2e
E 5.1.2e @minfin.nl

Van: 5.1.2e @dnb.nl < 5.1.2e @dnb.nl>
Verzonden: dinsdag 23 juli 2024 10:24
Aan: 5.1.2e (FM) < 5.1.2e @minfin.nl>
CC: 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl
Onderwerp: Re: Dreigingsscenario [Decrypted using DNB TLS][Encrypted using DNB TLS]

Ha 5.1.2e

Dank voor je bericht, en dank voor toezending van het dreigingsscenario.

De voorgestelde aanpak lijkt me uitstekend. Wellicht kan je team in eerste instantie het beste me 5.1.2e contact opnemen: zij kan het beste beoordelen wie hier namens DNB een bijdrage aan kunnen leveren.

Hartelijke groet,
5.1.2e

5.1.2e
De Nederlandsche Bank N.V.
M: 5.1.2e

Van: 5.1.2e (FM) < 5.1.2e @minfin.nl>
Verzonden: dinsdag, juli 23, 2024 9:51 AM
Aan 5.1.2e (DIR_DIR) < 5.1.2e @dnb.nl>
CC: 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>
Onderwerp: Dreigingsscenario [Decrypted using DNB TLS]

External: Pause and review the sender's email address, any URLs before clicking links, opening attachments, or following requests. When in doubt, contact our CDC via the scam mailbox, use the report message or the report scam button..

Beste 5.1.2e

Tijdens het FSC onlangs noemde ik het militaire dreigingsscenario dat we binnen Financiën (en overheid breed) hebben uitgedacht. buiten verzoek

Zie bijgevoegd het scenario zoals we in onze bestuursraad besproken hebben. 5.1.1b

5.1.1b

Hierbij kwamen een aantal deelvragen op, zoals: wat zijn de gevolgen voor de financiële sector in het geval van een volledige uitval van een datacentrum vanwege een bomaanslag, of: moet er een verbod ingesteld worden op het wegsluizen van spaargeld buiten de landsgrenzen/NAVO-gebied. Dit zijn opgaven en vragen die ook DNB raken.

In algemene zin was de conclusie dat onze sector zeer goed uitgerust is om om te gaan met crisis van operationele- (cyber) of prudentiële aard, maar dat nadenken over militaire dreiging relatief nieuw is. Tegelijkertijd is het nog maar de vraag of dit zo'n wezenlijk andere benadering behoeft.

Het lijkt ons nuttig om dit scenario naast bestaande scenario's en crisisplannen (van o.a. DNB) te leggen en op die manier een *gap analysis* uit te voeren, waarbij we kijken of onze bestaande (crisis)plannen en (nood)wetgeving voldoende handvatten bieden voor het scenario. Op basis van de uitkomsten hiervan zouden we kunnen bezien of een gedeelde aanpak of extra maatregelen nodig zijn. We zouden dit dan eventueel in TCO-verband (FIN, DNB en AFM) kunnen oppakken.

Indien je hiermee akkoord bent, dan kan mijn team contact opnemen met team Paraat.

Met vriendelijke groet,

5.1.2e

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

De informatie verzonden met dit e-mailbericht is uitsluitend bestemd voor de geadresseerde. Indien u als niet-geadresseerde dit bericht ontvangt, wordt u verzocht direct de afzender hierover te informeren en het bericht te vernietigen. Gebruik van informatie door onbevoegden, openbaarmaking of vermenigvuldiging is verboden en kan leiden tot aansprakelijkheid.

Als het e-mailbericht of het document de classificatie "DNB-PUBLIC" bevat, kan de informatie vrij verspreid worden. Bij de overige classificaties (DNB-UNRESTRICTED, DNB-RESTRICTED, DNB-CONFIDENTIAL of DNB-SECRET): behandel deze informatie vertrouwelijk. Verdere verspreiding van deze informatie is alleen toegestaan na toestemming van de afzender.

De afzender is niet aansprakelijk voor schade die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten. De e-mails en eventueel bijgevoegde bestanden zijn volgens een standaardprocedure gecontroleerd op computervirussen. Deze controle kan aanwezigheid van malware, zoals virussen, echter niet geheel uitsluiten.

The information sent in or attached to this email is intended solely for the addressee. If you have received this email but are not the intended recipient, please notify the sender immediately and delete the message. Please be advised that the unauthorised use, disclosure, dissemination or distribution of information is prohibited by law and may entail liability.

If this email is classified as DNB-PUBLIC, the recipient is free to distribute the information. However, the information must always be treated as confidential if this email is classified as DNB-UNRESTRICTED, DNB-RESTRICTED, DNB-CONFIDENTIAL or DNB-SECRET. In that case, its distribution is permitted only after obtaining the sender's consent.

The sender cannot be held liable for any damage or loss in connection with risks inherent in electronic message transfer. The sender has taken reasonable standard precautions to ensure no computer viruses are present in this email or any attachments it may contain. However, the presence of malware, such as viruses, cannot be ruled out.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

FIN – Verdiepende werksessie maatschappelijke weerbaarheid tegen militaire dreiging 12/07/2024 [Dep.V.]

<u>Zorgen voor betrouwbaar, weerbaar en veilig betalingsverkeer ten behoeve van de maatschappij, die ook continueert bij langdurige ontwrichting.</u>

Cash

- Grotendeels digitaal betalingsverkeer, burgers hebben weinig tot geen contant geld meer in bezit.
- Hoe zorg je dat er voldoende cash is, waar je op kan terugvallen bij grootschalige uitval?
- Bestaanszekerheid van burgers is afhankelijk van doorgang betalingsverkeer.
- Opkomst andere alternatieven zoals crypto.

Bankrun / vertrouwen in het monetaire stelsel

- Er is al veel staand beleid om een bankrun te voorkomen: buffers, depositogarantie, etc.
- Internationale standaarden en kaders EU waar op vertrouwd kan worden.
- Echter zijn mensen niet altijd rationeel, hoe zou een dergelijk scenario kunnen uitpakken?
- Wat als burgers op grote schaal het vertrouwen verliezen? Communicatieaanpak nodig?
- Er is nog geen rekening gehouden met militaire dreiging in staand beleid.
- Het is mogelijk om een freece te zetten op de hoeveelheid cash dat mensen kunnen pinnen.
- Er wordt veel geoefend, maar nog niet met een militair scenario. Crisissimulaties uitvoeren.

Fysieke beveiliging

- 5.1.1b
- Capaciteit KMar is beperkt, wie gaat beveiliging opvangen?
- 1 partij verantwoordelijk voor geldtransport, hoe continuïteit waarborgen?
- Single points of failure digitale infrastructuur: oproep om bij DEF aan te geven welke objecten fysieke beveiliging behoeven. (Bijvoorbeeld datacentra in Apeldoorn)
- Is fysieke beveiliging van banken nodig?

Cyberbeveiliging

- Er ligt een goede basis voor de cyber weerbaarheid.
- 5.1.1c grote redundantie, bijvoorbeeld eigen stroomnetwerk.
- Grote financiële instellingen hebben datacenters op verschillende locatie om de redundantie te verhogen.
- Er is een grote testcultuur op cyberveiligheid, gelden ook wettelijke verplichtingen om te testen.
- Daarnaast is er ook een samenwerkingsverband tussen banken om de weerbaarheid te verhogen.
- Training van personeel en burger op het herkennen van cyber dreiging.
- Is er voldoende kennis en kunde bij grootschalig cyber-aanvallen?

Onzekerheden bankieren

- Wat gebeurd er met je spaargeld als je deze wilt overzetten naar een bank elders in de wereld, welke garanties heb je? (wat gebeurd er bijvoorbeeld met inkomensheffing over een aantal jaar?)
- Duidelijk communiceren aan burgers wat wel en niet mag.

Afhankelijkheid telecom en energie

- Als de stroom uitvalt is er een backup van 4 uur.
- Het scenario houdt echter rekening met grootschalige uitval voor een langere tijd, welke opties liggen er dan?
- Buiten de normale kaders denken is hierbij belangrijk.
- Wat is het herstelplan en prioplan bij totale uitval? Wie ga je als eerste bedienen?

Bevoegdheden en regelgeving

- Welke bevoegdheden wet wetgeving is er nodig? Wanneer gaat het schuren?
- Kunnen mogelijk als overheid straks minder transparant zijn, wat kun je vooraf daar vast over afstemmen met de Rekenkamer?

Host Nation Support

- Doorvoer van militaire materieel door Nederland, rekening houden dat wegen zijn afgesloten voor civiel.
- Hoe zit het met waardetransporten?

Eurozone

- Met de Eurocrisis gezien dat er een aantal zwakkere partners zijn onder de eurolanden zoals Griekenland of Italië.
- Welke afspraken zijn er gemaakt? Is de Eurozone robuust genoeg?
- Er is veel Europese wetgeving waar elk land aan moet voldoen. Vraag is of huidige wetgeving voldoende is voor militaire dreiging.

Oorlogseconomie

- Lange tijd geen rekening meer gehouden met een oorlogseconomie, wat voor effecten heeft een oorlogseconomie op de financiële markt?
- Effecten van sancties op banken.

Europese banken

- Europese investeringsbank en Europese Bank voor Wederopbouw en Ontwikkeling, staan niet onder toezicht.
- Hebben wel grote exposure en veel geld in beheer, zij juist ook actief in Oost-Europa.
- Welke kwetsbaarheid ligt hier?

Overig

- Zijn de FIU en FIOD voldoende geëquipeerd? Zowel capaciteit als wetgeving.

Pagina's zijn geweigerd

3 - 7

buiten verzoek

Spreeklijn algemeen

- 5.1.2i

Financiële Markten

- 5.1.2i

Agentschap

- 5.1.2i

- 5.1.2i

BFB

- buiten verzoek
- 5.1.1b

Deelnemingen

buiten verzoek

HVP

buiten verzoek

buiten verzoek

Algemene toelichting

- In de BR wordt een fictief militair scenario uiteengezet waarbij eruit gegaan wordt van de activering van artikel 5 (oorlog op NAVO-grondgebied) waarbij Nederland ingezet wordt als 'logistieke hub'.
- Er moet per departement nagedacht worden over wat een dergelijk scenario betekent voor het ministerie en de kerntaken die zij uitvoert. Deze opdracht volgt uit de NVR-OEK.
- Voor elk departement zijn specifieke deelopgave geïdentificeerd, zie bijlage. Voor de GT zijn deze relevant:
  - Zorgdragen voor betrouwbaar, weerbaar en veilig betalingsverkeer ten behoeve van de maatschappij, die ook continueert bij langdurige ontwrichting (FM)
  - Zorgdragen voor de continuïteit van de kritische processen: financiering van de staatsschuld, schatkistbankieren, en betalingsverkeer van het Rijk' (AGT)
- In de voorbereidende sessie hebben we ook nagedacht over: Zorgdragen voor een weerbare financiële markt, die onder buitengewone (oorlogs)omstandigheden blijft functioneren, en daarmee ondersteunend is aan zowel de continuïteit van de samenleving als het voortzettingsvermogen van nationale en bondgenootschappelijke troepen.
- De impact is voor Financiële Markten en het Agentschap het grootst.
- Andere deelopgave voor Financiën zien meer toe op andere DG's:

buiten verzoek

  - Toeslagen – zorgen dat betalingen doorgaan, afhankelijkheden van deeloverheden voor de basisadministratie
- buiten verzoek

To: 5.1.2e (FM/IBI)[5.1.2e @minfin.nl]; 5.1.2e (FM/IBI)[5.1.2e @minfin.nl]
From: 5.1.2e (FM/IBI)
Sent: Tue 4/8/2025 12:39:28 PM
Subject: FW: Ter review: (concept)eindrapport, incl. MOB-adviezen en communicatieplan, van de MOB Kerngroep Weerbaar Betalingsverkeer
Received: Tue 4/8/2025 12:39:30 PM

In het rood

Van: 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>
Verzonden: dinsdag 8 april 2025 14:11
Aan: 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>
Onderwerp: RE: Ter review: (concept)eindrapport, incl. MOB-adviezen en communicatieplan, van de MOB Kerngroep Weerbaar Betalingsverkeer

Nog een aanvulling op onderstaande:

Vraag: wanneer krijgen we te zien wat er gepubliceerd gaat worden? Het valt of staat met het uiteindelijke advies.
Dat moet in het MOB worden geaccordeerd en dat moet (al dan niet ter info) naar de minister.

Nog andere aanvullingen?

Van: 5.1.2e (FM/IBI)
Verzonden: dinsdag 8 april 2025 13:58
Aan: 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) <5.1.2e @minfin.nl>
Onderwerp: FW: Ter review: (concept)eindrapport, incl. MOB-adviezen en communicatieplan, van de MOB Kerngroep Weerbaar Betalingsverkeer

Hi 5.1.2e

Ik denk dat het goed is om de MOB (en daarmee 5.1.2e de volgende punten nog mee te geven:

5.1.2i

Hebben jullie nog aanvullingen? Deadline voor het MOB is 14 april.
Zullen we tevens een mailtje maken voor 5.1.2e en begin aan de nota voor de Min.

Groet, 5.1.2e

Van: 5.1.2e @dnb.nl <5.1.2e @dnb.nl>
Verzonden: maandag 7 april 2025 16:03

Aan: 5.1.2e @betaalvereniging.nl; 5.1.2e @retailkantoor.nl; 5.1.2e @de-vgi.nl; 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e @dnb.nl; 5.1.2e @consumentenbond.nl; 5.1.2e @dnb.nl; 5.1.2e @betaalvereniging.nl; 5.1.2e @cm.com; 5.1.2e @vemobin.nl; 5.1.2e @vnoncw-mkb.nl; 5.1.2e @visma.com; 5.1.2e @kbo-brabant.nl; 5.1.2e @thuiswinkel.org; 5.1.2e @action.nl; 5.1.2e @retailkantoor.nl; 5.1.2e @anbo.nl; 5.1.2e @cbl.nl; 5.1.2e @thuiswinkel.org; 5.1.2e @betaalvereniging.nl; 5.1.2e @nvb.nl; 5.1.2e @de-vgi.nl; 5.1.2e 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e (FM/IBI) < 5.1.2e @minfin.nl>; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @geldmaat.nl; 5.1.2e @vnoncw-mkb.nl; 5.1.2e < 5.1.2e @seniorenbrabantzeeland.nl>; 5.1.2e @rndweb.nl; 5.1.2e @geldmaat.nl
CC: 5.1.2e @nvb.nl; 5.1.2e @planet.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @dnb.nl; 5.1.2e @oogvereniging.nl; 5.1.2e @dnb.nl
Onderwerp: FW: Ter review: (concept)eindrapport, incl. MOB-adviezen en communicatieplan, van de MOB Kerngroep Weerbaar Betalingsverkeer

[Encrypted using DNB TLS]

Beste leden van de WEE en leden van de Kerngroep Weerbaar Betalingsverkeer,

Zie onderstaande mail en bijlage.

@ leden van de Kerngroep: Hartelijk dank voor jullie review van het stuk! We hebben geprobeerd jullie suggesties daar waar mogelijk in het stuk te verwerken.

Hartelijke groet, ook namens 5.1.2e
5.1.2e

5.1.2e

Betalen, Cash & Marktinfrastructuur/ Payments, Cash & Market Infrastructures
Retail Betalen & Onderzoek / Retail Payments & Research

M 5.1.2e
E 5.1.2e @dnb.nl

DeNederlandscheBank
EUROSYSTEEM

Bezoekadres: Frederiksplein 61, 1017 XL Amsterdam

Van: BVM-MOB < 5.1.2e @dnb.nl>
Verzonden: maandag 7 april 2025 15:53
Aan: 5.1.2e @oogvereniging.nl; 5.1.2e @khn.nl; 5.1.2e @goededoelennederland.nl; 5.1.2e @nvb.nl; 5.1.2e @retailkantoor.nl; 5.1.2e @consumentenbond.nl; 5.1.2e @anbo.nl; 5.1.2e @vgz.nl; 5.1.2e @gmail.com; 5.1.2e @betaalvereniging.nl; 5.1.2e @onlinepaymentplatform.com; 5.1.2e @gmail.com; 5.1.2e @rndweb.nl; 5.1.2e @iederin.nl; 5.1.2e @planet.nl; 5.1.2e @mkb.nl; 5.1.2e @khn.nl; 5.1.2e @thuiswinkel.org; 5.1.2e @minfin.nl; 5.1.2e @minez.nl
CC: 5.1.2e (BCM_BCM) < 5.1.2e @dnb.nl>; 5.1.2e (DIR_DIR) < 5.1.2e @dnb.nl>; 5.1.2e (BCM_RBO) < 5.1.2e @dnb.nl>; 5.1.2e (COM_COM) < 5.1.2e @dnb.nl>; 5.1.2e @iederin.nl; 5.1.2e @nvb.nl; 5.1.2e @consumentenbond.nl; 5.1.2e @anbo.nl; 5.1.2e @vgz.nl; 5.1.2e @consumentenbond.nl; 5.1.2e @cbl.nl; 5.1.2e @lvkk.nl; 5.1.2e (BCM_CDS) < 5.1.2e @dnb.nl>; 5.1.2e < 5.1.2e @dnb.n 5.1.2e (BCM_RBO) < 5.1.2e @dnb.nl>; 5.1.2e 5.1.2e @dnb.nl>; Office 5.1.2e (DIR) < 5.1.2e @dnb.nl>; BVM-MOB < 5.1.2e @dnb.nl>; 5.1.2e < 5.1.2e @dnb.nl> 5.1.2e 5.1.2e @dnb.nl>; 5.1.2e < 5.1.2e @dnb.nl>; 5.1.2e @boyag.nl; 5.1.2e @vnoncw-mkb.nl 5.1.2e (BCM_CDS) < 5.1.2e @dnb.nl>; 5.1.2e @minfin.nl; 5.1.2e BCM_RBO) < 5.1.2e @dnb.nl>; 5.1.2e BCM_CDS)

< 5.1.2e @dnb.nl>; Office-BCM < 5.1.2e @dnb.nl>; 5.1.2e @nvb.nl; 5.1.2e @thuiswinkel.org; 5.1.2e (BCM_CBO) < 5.1.2e @dnb.nl>; 5.1.2e @consumentenbond.nl; 5.1.2e (COM_COM) < 5.1.2e @dnb.nl>
Onderwerp: Ter review: (concept)eindrapport, incl. MOB-adviezen en communicatieplan, van de MOB Kerngroep Weerbaar Betalingsverkeer

Beste leden van het MOB,

Namens de Kerngroep Weerbaar Betalingsverkeer ontvangt u bijgaand, ter review, het (concept)eindrapport, incl. MOB-adviezen en communicatieplan.

Mocht u daar zaken in aangevuld of aangepast willen zien, kunt u die mij dan uiterlijk op **maandag 14 april as.** doorgeven? O.b.v. van uw evt. terugkoppeling passen wij het eindrapport waar nodig aan en leggen het een dag later, ook weer via e-mail, t.b.v. een 'final flaw-review' opnieuw aan u voor (met een reactietermijn van 2 dagen).

Nog even ter achtergrond (uit het resultatenoverzicht van de MOB-vergadering van 14 nov. jl.):

Weerbaar betalingsverkeer in een onzekere wereld

Het MOB ziet dat de wereld om ons heen guurder is geworden door toegenomen geopolitieke spanningen en cyberdreigingen. Het kan de weerbaarheid van het betalingsverkeer – een kritieke infrastructuur – ook in ons land op de proef stellen. Denk bijvoorbeeld aan een cyberaanval die ons digitale betalingsverkeer, zowel in winkels als online, langere tijd platlegt. Een weerbaar betalingsverkeer vraagt van de individuele partijen in het MOB, zoals de banken en andere betaaldienstverleners, ondernemers, consumenten, almede hun eigen samenwerkingsverbanden, om alertheid, voorbereiding en wendbaarheid. Dat geldt ook voor het MOB zelf als maatschappelijk forum. Het MOB verkent daarom welke voorzorgsmaatregelen zij op korte termijn kan nemen.

*NB: Bijgevoegde concepteindrapportage bevat o.a. de (concept)adviezen die op do. 8 mei as. gepubliceerd worden en naar wij verwachten de nodige media-aandacht zullen krijgen. Daarom aan u het verzoek om bijgevoegd document als **vertrouwelijk** te behandelen en niet buiten de eigen organisatie – en enkel waar nodig binnen de eigen organisatie – te verspreiden.*

Alvast hartelijk dank en hartelijke groet,

namens de MOB Kerngroep Weerbaar Betalingsverkeer,

5.1.2e

Secretariaat MOB
T 5.1.2e
E 5.1.2e @dnb.nl

MOB
Maatschappelijk Overleg Betalingsverkeer

De informatie verzonden met dit e-mailbericht is uitsluitend bestemd voor de geadresseerde. Indien u als niet-geadresseerde dit bericht ontvangt, wordt u verzocht direct de afzender hierover te informeren en het bericht te vernietigen. Gebruik van informatie door onbevoegden, openbaarmaking of vermenigvuldiging is verboden en kan leiden tot aansprakelijkheid.

Als het e-mailbericht of het document de classificatie "DNB-PUBLIC" bevat, kan de informatie vrij verspreid worden. Bij de overige classificaties (DNB-

UNRESTRICTED, DNB-RESTRICTED, DNB-CONFIDENTIAL of DNB-SECRET): behandel deze informatie vertrouwelijk. Verdere verspreiding van deze informatie is alleen toegestaan na toestemming van de afzender.

De afzender is niet aansprakelijk voor schade die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten. De e-mails en eventueel bijgevoegde bestanden zijn volgens een standaardprocedure gecontroleerd op computervirussen. Deze controle kan aanwezigheid van malware, zoals virussen, echter niet geheel uitsluiten.

The information sent in or attached to this email is intended solely for the addressee. If you have received this email but are not the intended recipient, please notify the sender immediately and delete the message. Please be advised that the unauthorised use, disclosure, dissemination or distribution of information is prohibited by law and may entail liability.

If this email is classified as DNB-PUBLIC, the recipient is free to distribute the information. However, the information must always be treated as confidential if this email is classified as DNB-UNRESTRICTED, DNB-RESTRICTED, DNB-CONFIDENTIAL or DNB-SECRET. In that case, its distribution is permitted only after obtaining the sender's consent.

The sender cannot be held liable for any damage or loss in connection with risks inherent in electronic message transfer. The sender has taken reasonable standard precautions to ensure no computer viruses are present in this email or any attachments it may contain. However, the presence of malware, such as viruses, cannot be ruled out.

Ministerie van Financiën

TER INFORMATIE
Aan
de minister
17/5

Generale Thesaurie
Directie Financiële Markten

5.1.2e
5.1.2e

nota

MOB-advies contant geld - weerbaar betalingsverkeer

Datum
8 mei 2025

Notanummer
2025-0000102160

Bijlagen
1. MOB-advies

Aanleiding

- Het Maatschappelijk Overleg Betalingsverkeer (MOB) publiceert op 20 mei de adviezen aan consumenten en toonbankinstellingen (winkels e.d.) over hoe zij zich kunnen voorbereiden op een noodsituatie waarbij het 72 uur (gedeeltelijk) niet mogelijk is om elektronisch te betalen (bijlage 1). Onderdeel van het advies is een berekening van het Nibud over hoeveel contant geld mensen moeten aanhouden.
- Op 20 mei worden de adviezen openbaar gemaakt met een persbericht en een persconferentie door DNB. Er wordt media-aandacht verwacht gelet op eerdere berichtgeving. Daarom informeren we u nu over dit advies. We vragen nu geen acties of besluiten van u.

Kernpunten

- Op basis van onderzoek door het Nibud gaat het MOB aan huishoudens adviseren om 70 euro per volwassene aan te houden en 30 euro per kind. Dit bedrag kan het beste worden aangehouden in biljetten met lage waardes en in muntgeld.
- Het advies aan burgers is deze voorraad de komende maanden geleidelijk op te bouwen, om zo te voorkomen dat mensen massaal gaan pinnen.
- Tevens gaat het MOB adviseren om vooral zelf goed na te denken wat er nodig is om 72 uur zelfredzaam te zijn en wordt geadviseerd om meerdere betaalmiddelen te hebben naast contant geld. Denk hierbij bijvoorbeeld aan mobiel betalen per telefoon en het hebben van bankpassen van twee verschillende banken.
- Toonbankinstellingen krijgen van het MOB het advies om voldoende wisselgeld aan te houden om 72 uur te overbruggen. Ook worden toonbankinstellingen aangemoedigd om na te denken over passende terugvalopties voor als pinnen niet werkt. Hiervoor wordt verwezen naar www.pin.nl, een website van de betaalvereniging, waar verschillende mogelijkheden toegelicht worden.
- Het advies wordt op 20 mei gepubliceerd door DNB (als voorzitter van het MOB). De adviezen zijn zo opgesteld dat de capaciteit van de geldautomaten en het waardetransport zo min mogelijk opeens onder druk komen te staan. Dit gebeurt mede door vooraf de publicatiedatum af te stemmen en erop te sturen dat consumenten geleidelijk het contante geld verzamelen in plaats van in één keer pinnen. Wij zullen dit samen met DNB monitoren.

14/5

Toelichting

- Met de toegenomen geopolitieke spanningen is het belangrijk dat de samenleving als geheel weerbaar is. Een goed voorbereide maatschappij kan tijdens noodsituaties de rust zoveel mogelijk bewaren en de impact van de noodsituatie verkleinen.
- In dit kader heeft het MOB, een overlegorgaan van alle betrokkenen partijen bij het betalingsverkeer (consumenten- en werkgeversorganisaties, banken, DNB, met Financiën als waarnemer), gekeken welke adviezen zij kan geven aan consumenten en toonbankinstellingen om de maatschappelijke weerbaarheid te vergroten.
- Hierbij is uitgegaan van een scenario van 72 uur verstoring van het elektronisch betalingsverkeer. Dit sluit aan bij het scenario dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) huishoudens adviseert op www.denkvooruit.nl (de overheidscampagne om burgers zelfredzaam te maken).
- In samenspraak met Geldmaat, Brink's (waardetransporteur) en INretail is gekozen voor 20 mei als publicatiedatum. De chartale infrastructuur is dan voorbereid op een mogelijke toename van geldopnames.
- De adviezen worden op 20 mei integraal gepubliceerd via een bericht op de MOB-pagina van de DNB-website en een persbericht. Beide berichten bevatten ook Q&A's en een link naar het onderliggende Nibud-rapport.
- Deze adviezen worden zo snel mogelijk geïntegreerd op denkvooruit.nl, in afstemming met de NCTV.
- De woordvoerders van de grootbanken ontvangen vooraf (onder embargo) het persbericht. Daarnaast dragen de MOB-partijen die consumenten en retailers vertegenwoordigen de adviezen zo snel als mogelijk– het liefst vrijwel direct – na publicatie via de eigen communicatiekanalen (websites, nieuwsbrieven e.d.) uit naar hun achterbannen.

Communicatie

- DNB heeft regie over de bekendmaking van het advies en voert het woord. DNB bekijkt of 5.1.2e 5.1.2e op – of daags voor – 20 mei korte interviews (aan bijv. NOS, Nu.nl en De Telegraaf) kan geven.
- De leden van de kerngroep (inclusief FIN als waarnemer) ontvangen het communicatieplan inclusief deze persberichten en krijgen de kans mee te denken over de inhoud. COMM staat in contact met de woordvoering van DNB. Bij eerdere berichten over het aanhouden van contant geld was er veel media-aandacht.
- Wij zorgen voor goede aanhaking op de 'denkvooruit.nl – communicatie'. Verder passen we rijksoverheid.nl aan met het advies van het MOB.

Politiek/bestuurlijke context

- Op 6 december 2024 hebben de ministers van JenV en Defensie een brief naar de Tweede Kamer gestuurd over wat er nodig is om de weerbaarheid van Nederland tegen militaire en hybride dreigingen te versterken. Hierin wordt genoemd dat Financiën verantwoordelijk is voor het borgen van het betaal- en effectenverkeer in tijden van dreiging.

Informatie die niet openbaar gemaakt kan worden

Niet van toepassing.

Geprint met Digidoc 2 op 13-05-2025, 16:00

Parafenoverzicht

Werkmap

Onderwerp: FM 102160 informeren MOB-advies weerbaar betalingsverkeer
Nummer: 2025-0000010785
Algemeen taakverzoek:

Document: FM 102160 MOB-advies weerbaar betalingsverkeer (2025-0000102160)

Naam	Datum en Tijd	Inbox
5.1.2e		

Bijlage 1. Factsheet compensatiemodel digitale euro

In het kort (zie schema)

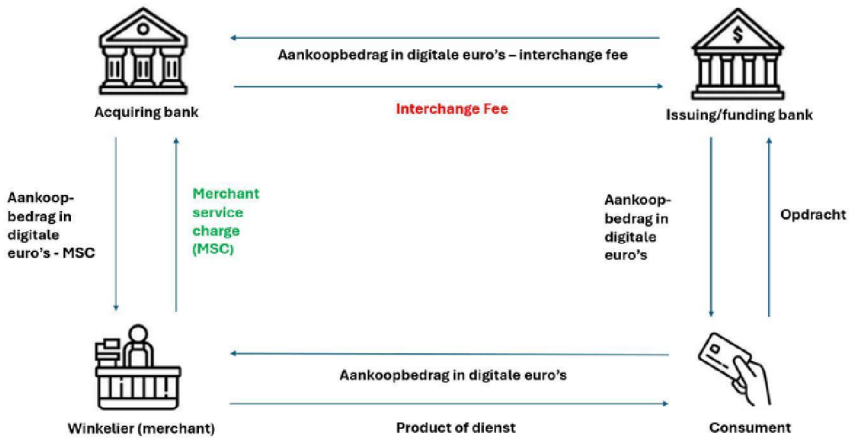
- Het compensatiemodel van de digitale euro bepaalt de regels voor banken en betaaldienstverleners bij het vaststellen van tarieven voor hun diensten.
- De winkelier betaalt een vergoeding (*Merchant Service Charge,* MSC) aan zijn/haar bank (*acquiring bank*) voor het verwerken van de betaling die de consument heeft gedaan.
- De acquiring bank draagt een deel van deze MSC-fee af aan de *issuing bank*, voor de verrichte werkzaamheden bij deze transactie. Dit is de interchange fee.
- Omdat winkeliers verplicht worden digitale euro betalingen te accepteren, hebben ze beperkte (markt)macht om te onderhandelen over de kosten. Ditzelfde geldt voor de banken en betaaldienstverleners, die verplicht distribueren. Bovendien vervullen niet alle banken/betaaldienstverleners de rol van *acquiring* en *funding* bank. De Commissie stelt daarom voor beide *fees* te maximeren met *caps*. Over de hoogte, berekening en vaststelling van deze caps is al vaak gesproken.
- De ECB komt de *issuing* en *acquiring* banken tegemoet door de *scheme and settlement* kosten voor haar rekening te nemen. In het Nederlandse betalingsverkeer betalen betaaldienstverleners een *fee* aan bijv. Visa of Mastercard voor het onderhouden van de betaalinfrastructuur en voor het afwikkelen van transacties. De ECB gaat dit niet vragen.

Transitiefase

- Aangezien er onvoldoende bekend is over de totale kosten van de digitale euro is het lastig om tot een proportionele verdeling te komen. Daarom wordt er gesproken over het instellen van een transitiefase waarbij de ECB data verzamelt over het gebruik en kosten van de digitale euro. Tijdens deze fase kan het compensatiemodel per lidstaat verschillen.
- Tijdens de transitiefase worden winkeliers tegemoet gekomen door begrenzing van de MSC-fee. Omdat je in deze fase de adoptie wilt vergroten, kunnen wij ons hierin vinden.
- Over de interchange fee wordt nog gesproken. Mogelijk wordt hiervoor een EU-gemiddelde interchange fee bepaald gedurende de transitiefase, op basis van nader te bepalen vergelijkbare en al bestaande digitale betalingen.

Na de transitiefase

- Na de transitiefase wordt toegewerkt naar een geharmoniseerd compensatiemodel met dezelfde *fees* in de hele eurozone. Dit vinden we passend voor een pan-Europees betaalinstrument.
- Er is bij het compensatiemodel sprake van een verdelingsvraagstuk met imperfecte informatie. We kiezen voor een evenwichtige verdeling. Winkeliers zullen in de transitiefase beschermd worden. Na de transitiefase wil Nederland banken/betaaldienstverleners tegemoet komen door het kostenmodel te baseren op de daadwerkelijke kosten van een digitale euro betaling, inclusief een redelijke winstmarge.
- Hierbij speelt alsnog het risico dat wanneer de kosten te hoog zijn, winkeliers ervoor moeten opdraaien. Nederland begrijpt in dat geval dat een extra cap nodig kan zijn, op basis van het Europees gemiddelde. Omdat Nederland een efficiënt betaalsysteem heeft, liggen de kosten voor Nederlandse PSP's lager dan het gemiddelde en zou een EU-brede cap voor hen gunstig zijn.



Bijlage 1

Tabel 1: Analyse beleidsdoelen digitale euro			
Beleidsdoel digitale euro	**Achtergrond**	**Toelichting**	**Weging toegevoegde waarde**
Strategische autonomie	De digitale euro kan de afhankelijkheid van niet-Europese partijen in het betalingsverkeer verkleinen.	In Nederland zijn we voor het toonbankbetalingsverkeer afhankelijk van niet-Europese bedrijven, specifiek VISA en Mastercard. Waar andere landen een nationaal alternatief hebben (C*art Bancaire* in Frankrijk), heeft Nederland dat niet meer. Voor strategische autonomie moet een digitale euro gestoeld zijn op Europese infrastructuur. Daarnaast wordt er door EPI en EuroPA gewerkt aan Europese, private betaaloplossingen.	**Toegevoegde waarde**: Afhankelijk van het ontwerp en van de partijen die betrokken zijn bij de infrastructuur, kan de digitale euro bijdragen aan strategische autonomie van het betalingsverkeer. Daarbij zal ook worden gewogen of de digitale euro een noodzakelijk en proportioneel instrument is om bij te dragen aan strategische autonomie, mede afhankelijk van de vraag of private Europese initiatieven zich weten te verenigen.
Weerbaarheid	De *offline* functionaliteit van de digitale euro kan een tijdelijke terugvaloptie in het betalingsverkeer zijn, bijvoorbeeld bij stroomuitval of andere storingen.	De *offline* functionaliteit bestaat nog niet in het huidige betalingsverkeer, terwijl steeds minder mensen in Nederland contant geld bij zich hebben. Het succes van deze extra terugvaloptie hangt af van 1) de mate van bekendheid en gebruik van de *offline* digitale euro en 2) de technische specificaties die zijn vereist, bijvoorbeeld op telefoons en bij terminals aan de toonbank.	**Toegevoegde waarde**: In het licht van huidige geopolitieke ontwikkelingen biedt de *offline* variant concrete toegevoegde waarde voor het Nederlandse betalingsverkeer. 5.1.1c 5.1.1c 5.1.1c Dit maakt de offline digitale euro, die het meest lijkt op een digitale vorm van cash, een prioriteit voor Nederland tot nu toe. Wel moet er aandacht zijn voor de technische specificaties die dit vereist en voor het gebruik in de praktijk. Hier is ook een proportionaliteitsvraag over hoe duur de digitale euro mag zijn, naast de bestaande terugvaloptie (contant geld).
Monetair anker	De digitale euro is een digitale vorm van publiek geld. Publiek geld doet dienst als 'monetair anker' in het betalingsverkeer en garandeert de 1:1-inwisselbaarheid tussen het commercieel geld van verschillende banken.	Geld als betaalmiddel is een publiek goed: het stelt iedereen in staat om op gelijke en betrouwbare wijze deel te nemen aan het economische verkeer. Door de toenemende digitalisering en het afnemende gebruik van contant geld, komt deze publieke functie steeds meer onder druk te staan. Om ook in de toekomst te borgen dat publiek geld in omloop blijft, is er behoefte aan een digitale vorm van publiek geld.	**Toegevoegde waarde**: Het 'monetair anker' blijft gewaarborgd met het voortbestaan van contant geld en de toegang van commerciële banken tot centrale bankreserves. Bij verdere afname van gebruik van contant geld in NL kan de digitale euro ervoor zorgen dat publiek geld ook in de toekomst blijft circuleren. Dit past bij een digitaliserende samenleving. Tegelijkertijd zijn de meningen internationaal verdeeld over de noodzaak van een digitale vorm van publiek geld als monetair anker voor het betalingsverkeer.

Een digitaal pan-Europees betaalmiddel	Met een acceptatieplicht voor winkeliers ontstaat een digitaal, pan-Europees betaalmiddel dat in alle eurozone landen gelijkwaardig geaccepteerd moet worden.	Tot op heden is het Europese betaallandschap gefragmenteerd, met verschillende voorkeuren van de lidstaten voor betalingen met contant geld, giraal geld (direct debit of credit) of een nationale betaalmethode zoals Cart Bancaire (FRA) of Girocard (DUI). Ook hier beginnen private initiatieven zoals EPI en EuroPA het 'gat' in de Europese betaalmarkt te vullen. Een vrees van banken en betaaldienstverleners is dat de verplichte invoering van de digitale euro de capaciteit beperkt om private pan-Europese oplossingen te ontwikkelen en deze initiatieven ruimte ontneemt, bijvoorbeeld door financiële ondersteuning van het Eurosysteem.	**Toegevoegde waarde**: De digitale euro kan door wettelijke bepalingen rond de acceptatieplicht een pan-Europees betaalmiddel worden. Private alternatieven zouden deze rol ook kunnen pakken maar lijken tot nu toe tegen barrières aan te lopen voor beschikbaarheid in heel Europa. Een (publieke) digitale euro zou de ontwikkeling en innovatie van private, marktgestuurde Europese, digitale betaalmiddelen tegelijkertijd niet moeten belemmeren. Vooralsnog lijken private alternatieven geen pan-Europees betaalmiddel te kunnen bieden, bijvoorbeeld omdat er nu twee concurrerende private initiatieven zijn.
Versterken van de internationale rol van de euro	Als dollar-gedenomineerde stablecoins of andere (crypto)valuta een grote rol in de Europese economie gaan spelen, verkleint dit de internationale rol van de euro en de controle van de ECB over het monetair beleid in de Eurozone.	Met wetgeving voor cryptomarkten en stablecoins (MiCA-verordening) wordt de rol van cryptovaluta en stablecoins in de Europese economie begrensd. Hoewel stablecoins met name in dollars gedenomineerd zijn, is er nog geen sprake van een scenario waarin de internationale rol van de euro door deze ontwikkelingen wordt ingeperkt. De digitale euro is daarnaast beoogd als betaalmiddel in het eurogebied, met beperkingen in de vorm van aanhoudingslimieten die moeten voorkomen dat gebruikers geen bank meer nodig hebben. De rol van de digitale euro als spaarproduct wordt hiermee ingeperkt. Los van de ontwikkeling van deze *retail* digitale euro werkt de ECB aan innovatie in het *wholesale* betalingsverkeer tussen financiële instellingen, waarbij een *wholesale* variant van centrale bankgeld een belangrijke rol kan spelen.	**Toegevoegde waarde**: Wij zien voor nu geen rol voor de *retail* digitale euro om de internationale rol van de euro te versterken. Met wetgeving kan de internationale rol van de euro beschermd worden tegen de opkomst van stablecoins en cryptovaluta, voor zover dat nodig is. *Wholesale* ontwikkelingen – niet in de scope van de voorstellen waarover momenteel wordt onderhandeld - in het betalingsverkeer kunnen de internationale rol van de euro op termijn wel versterken door grote transacties in euro's ter vergemakkelijken. Er is een scenario denkbaar in de toekomst waarin de digitale euro interoperabel is met digitale bankgeld in andere jursidicties. Hoewel een dergelijk scenario ver weg is, kan dit internationale betalingen, zoals *remittances*, goedkoper en makkelijker maken.

Tabel 2: Wensen en positie berokken partijen		
Partij	**Belangen**	**Status in de Europese onderhandelingen**
Kamer	• Strenge privacy-waarborgen en niet-programmeerbaarheid. • De digitale euro moet van toegevoegde waarde zijn voor Nederlandse burgers en bedrijven. • De digitale euro levert een bijdrage aan de weerbaarheid en strategische autonomie van het Europese betalingsverkeer.	• Op deze thema's gaan de onderhandelingen de goede kant op. • De niet-programmeerbaarheid is in de conceptverordening gewaarborgd. 5.1.2a
Consument	• De digitale euro moet een toegankelijk betaalinstrument zijn, gratis in gebruik en breed geaccepteerd worden. • Hoog niveau van privacy, niet-programmeerbaar. • De offline functionaliteit voegt waarde toe als tijdelijke terugvaloptie bij verstoringen in het betaalverkeer.	• Er zijn waarborgen voor toegankelijkheid van de digitale euro en er komt een acceptatieplicht. Er wordt nog gesproken over de omvang van de acceptatieplicht. • De kosten voor de digitale euro infrastructuur zullen, via betaaldienstverleners of via winkeliers, bij de consument terecht komen, maar transacties worden voor consumenten kosteloos. • De onderhandelingen over privacy, niet-programmeerbaarheid en de offline digitale euro gaan de goede kant op.
Banken en betaaldienst-verleners	• Weinig tot geen animo voor de digitale euro omdat het opzetten van de infrastructuur geld kost en private innovatie (Wero) in de weg zou zitten, bijvoorbeeld omdat het beslag zou leggen op innovatiecapaciteit. • Zorgen over het compensatiemodel, zeker gezien additionele regulering in Nederland t.o.v. Europese regulering (m.n. een lidstaatoptie in de IFR, zie bijlage 1, factsheet compensatiemodel). • Lage *holding limits*, om te voorkomen dat deposito's wegstromen bij banken en negatieve impact hebben op rentebaten en de financiering van de economie.	• Nederland zet zich in voor voldoende ruimte voor private initiatieven. Hierbij moet zorgvuldig worden afgewogen in hoeverre de markt de doelstellingen van de digitale euro (gedeeltelijk) kan realiseren. • Eventueel zou de digitale euro de noodzaak van vergaande ontwikkeling van de Wero en bijbehorende kosten kunnen wegnemen. • De intentie van het Poolse voorzitterschap is om tot een akkoord op hoofdlijnen te komen voor het compensatiemodel. 5.1.2a 5.1.2a • Op aanhoudingslimieten is er o.i. ruimte voor een compromis, waarbij de ECB een voorstel doet en medewetgevers hierop invloed uit kunnen oefenen of moeten accorderen. 5.1.2a 5.1.2a
Winkeliers	• Lage kosten per transactie, om te voorkomen dat winkeliers klanten *nudgen* naar cash/debitkaarten. • Voldoende uitzonderingen voor de acceptatieplicht. • Een gefaseerde invoering van de digitale euro, zodat de betaalterminals geleidelijk vervangen kunnen worden.	• Voor de transitiefase (eerste 5 jaar) is nu een *no-worse off*-bepaling voorzien, die maakt dat betalingen in digitale euro voor winkeliers niet duurder mogen zijn dan andere digitale betalingen. Mogelijk kunnen banken en betaaldienstverleners hun kosten hierdoor niet volledig terugverdienen in de eerste fase, maar het stimuleert wel het gebruik van de digitale euro. Op lange termijn kan een transactie in digitale euro duurder worden voor winkeliers, meer in lijn met de daadwerkelijke kosten.

Ministerie van Financiën

TER BESLISSING
Aan
de minister
29/6

Generale Thesaurie
Directie Financiële Markten

5.1.2e

nota

Strategie digitale euro voorjaar 2025

Datum
23 juni 2025

Notanummer
2025-0000165700

Bijlagen
1 Tabel analyse beleids-doelen & wensen betrokker partijen
2 Factsheet compensatie-model digitale euro

Aanleiding

Mede door de geopolitieke ontwikkelingen komt er steeds meer druk om de behandeling van de wetsvoorstellen voor de digitale euro af te ronden, ook al liggen er nog meerdere vraagstukken open. De aankomende Deense voorzitter heeft de ambitie uitgesproken tot een raadspositie te komen dit kalenderjaar. In deze nota vindt u een toelichting op de stand van zaken en het speelveld. Daarnaast leggen wij u ter akkoord een aantal verdiepingen in de Nederlandse inzet ter beslissing voor.

Beslispunten

Bent u akkoord met de voorgestelde verdiepingen (pagina 3) in de Nederlandse inzet rond de digitale euro? Desgewenst kunnen we die met u bespreken.

Kernpunten

- Nederland heeft door pro-actieve inzet voorafgaand aan de totstandkoming van de wetsvoorstellen voor de digitale euro al vroegtijdig succesvol het ontwerp van de digitale euro beïnvloed, zoals rond privacybescherming en niet-programmeerbaarheid.
- De digitale euro is o.i. met name van toegevoegde waarde voor de strategische autonomie en weerbaarheid van het Europese en Nederlandse betalingsverkeer.
- Om het draagvlak voor de digitale euro te vergroten, adviseren we een aantal verdiepingen in de Nederlandse inzet, specifiek rond het compensatiemodel en de aanhoudingslimieten.

Toelichting

Stand van zaken digitale euro

- Raad: De raadsonderhandelingen lopen sinds de zomer van 2023 en het tempo is onder het Poolse voorzitterschap versneld. De Denen nemen op 1 juli het stokje over en hebben de ambitie om voor het einde van het jaar een raadsakkoord te bereiken. Op 8 juli zullen ze deze ambitie in de Eurogroep voorleggen en hier mogelijk *commitment* voor vragen.
- Europees Parlement: Het is nog onduidelijk wat de tijdlijn is voor de behandeling van de wetsvoorstellen voor de digitale euro in het Europees Parlement (EP); 5.1.2e, moet zijn conceptrapport nog publiceren. De verwachting is dat dit na de zomer zal

27/6

gebeuren, waarna 5.1.2e de schaduwrapporteurs tot een gedeeld standpunt moeten komen en hierover gestemd moet worden door het EP.

- ECB: De ECB werkt gelijktijdig aan de onderhandelingen in hoog tempo aan de voorbereiding van de digitale euro. In november dit jaar loopt de voorbereidingsfase af, die twee jaar heeft geduurd. Om verder te kunnen gaan met de ontwikkeling van de digitale euro, is meer duidelijkheid nodig over het regelgevend kader. Naar verwachting verlengt de ECB de voorbereidingsfase.
- Private sector: De private sector is ondertussen druk bezig met het verder ontwikkelen van Wero, een pan-Europees betaalproduct. Wero wordt ontwikkeld door een alliantie van meerdere Europese financiële instellingen, het European Payments Initiative (EPI). In 2023 heeft EPI het Nederlandse betaalsysteem iDeal overgenomen. De verwachting is dat Wero in 2026 in Nederland zal worden uitgerold, ter vervanging van iDeal. Naast Nederland zijn Frankrijk, Duitsland, België en Luxemburg aangesloten bij EPI. De wens van deze alliantie is om Europa-dekkend te zijn, maar mede door fragmentatie en naast elkaar bestaande initiatieven (bijvoorbeeld EuroPA in Spanje, Andorra, Portugal, Italië, Polen en Noorwegen) is dit nog niet aan de orde.

Analyse beleidsdoelen digitale euro

De argumentatie voor een digitale euro is de afgelopen jaren in ontwikkeling geweest. Argumenten rond strategische autonomie en weerbaarheid hebben aan kracht gewonnen, terwijl argumenten rond het monetair anker en een pan-Europees betaalmiddel tegenwoordig minder aandacht krijgen. Aan de hand van verschillende publicaties[1] en gesprekken[2] hebben we de belangrijkste argumenten voor een digitale euro opnieuw gewogen in tabel 1 (bijlage 1): 1) strategische autonomie; 2) weerbaarheid; 3) een monetair anker, 4) een pan-Europees, digitaal betaalmiddel; 5) internationaal gebruik van de euro.

Wensen en positie belanghebbenden

Ook draagvlak is cruciaal om de invoering van een digitale euro te laten slagen. Om het draagvlak in de Nederlandse samenleving en sector te vergroten, is het belangrijk aan te blijven sluiten bij de wensen en de positie van de Kamer en belanghebbenden. In tabel 2 (bijlage 1) wordt hierop ingegaan.

Krachtenveld en positionering Nederland

Nederland stelt zich constructief op in de onderhandelingen. Door proactieve betrokkenheid destijds, voorafgaand aan de publicatie van de wetsvoorstellen, wordt aan veel kernpunten van Nederland in de conceptverordening voldaan: met name een hoog niveau van privacy en niet-programmeerbaarheid.

5.1.2a

Voorstel tot verdieping van de Nederlandse inzet

- Op basis van bovenstaande analyse stellen wij de volgende verdiepingen voor ten opzichte van het BNC-fiche uit augustus 2023. Indien akkoord

[1] Een recente speech van Philip Lane (hoofdeconoom van de ECB), vormde de basis: Lane (2025), *The digital euro: maintaining the autonomy of the monetary system*.
[2] Onder meer met sectorpartijen, de NCTV, de rapporteur in het Europees Parlement en DNB.

met deze wijzigingen, zullen wij u een voorstel doen om de Kamer te informeren via het Eurogroep/Ecofinraad-verslag:

1. Herprioritering rond weerbaarheid: De *offline* functionaliteit van de digitale euro biedt mogelijk een unieke toevoeging aan het Nederlandse betaallandschap, als terugvaloptie tijdens stroomstoringen of andere onderbrekingen. Gezien de afname van het gebruik van contant geld zijn er voor deze functionaliteit concrete baten die – geheel of gedeeltelijk - opwegen tegen de mogelijke lasten van de digitale euro voor winkeliers, banken en betaaldienstverleners.
2. Specificeren inzet rond compensatiemodel: de inrichting van het compensatiemodel is een verdelingsvraagstuk, waarbij kosten terecht komen bij winkeliers, betaaldienstverleners of consumenten. Met het oog op een succesvolle introductie is het wenselijk winkeliers tijdens de transitiefase tegemoet te komen en basisdienstverlening gratis te maken voor consumenten, ook als dit betekent dat banken en betaaldienstverleners hun kosten in deze fase niet zouden kunnen terugverdienen. Op de lange termijn moeten de kosten van de digitale euro infrastructuur echter wel gereflecteerd worden in het compensatiemodel, om te voorkomen dat banken en betaaldienstverleners structureel kosten maken voor het in stand houden van deze publieke infrastructuur. Binnen dit distributievraagstuk vinden we het passend dat het compensatiemodel geharmoniseerd wordt in heel Europa en gebaseerd is op de kosten van een transactie (+ redelijke winstmarge). Zie bijlage 1 voor een toelichting op het compensatiemodel.
3. Specificeren inzet rond aanhoudingslimieten: De aanhoudingslimieten hebben niet alleen invloed op de balansgrootte van de ECB (monetair beleid), maar ook, afhankelijk van de online of offline variant[3], op witwasrisico's, de weerbaarheid van het betalingsverkeer en de financiële stabiliteit. In het initiële voorstel staat dat de ECB de algemene aanhoudingslimiet bepaalt (de *holding limit*) en dat de Commissie bevoegd is een transactielimiet te bepalen voor betalingen met offline digitale euro's. Dit houdt dus in dat er twee limieten zullen worden vastgesteld: een algemene limiet, en een lagere limiet voor offline betalingen. Gezien de impact van de limieten, en gezien de noodzaak om op dit onderwerp tot een compromis te komen, stellen we voor dat er betrokkenheid van de Raad en/of het EP is bij vaststelling van één of beide limieten. Dit kan in verschillende vormen die we verder onderzoeken. Ook over de hoogte van de aanhoudingslimieten bestaat discussie. Banken geven de voorkeur aan een laag maximumlimiet van €500[4] om de financiële stabiliteit te waarborgen, terwijl verschillende ECB- en DNB-studies aantonen dat

[3] De online variant van de digitale euro zal vergelijkbaar werken met het bestaande digitale betalingsverkeer, maar dan via publieke infrastructuur en met publiek geld. Voor deze online variant zal een aanhoudingslimiet gelden (*holding limit)* om financiële stabiliteit risico's te beperken. Aangezien de online variant invloed heeft op het monetair beleid, is het aannemelijk dat de ECB een rol heeft in het vaststellen van deze limiet. De offline variant is een nieuwe vorm van digitaal betalen, waarvoor geen internetverbinding nodig is. Vergelijkbaar met fysiek geld, laadt een gebruiker vooraf offline digitale euro's in een digitale wallet, waarna transacties kunnen worden gedaan. Deze transacties worden uitgevoerd en geregistreerd als één van beide betrokken apparaten weer internetverbinding heeft. Voor de offline variant zal, mede met het oog op witwasrisico's, een lagere transactielimiet gelden dan voor online betalingen met de digitale euro. Het valt te voorzien dat de medewetgevers meer inspraak krijgen bij het vaststellen van de offline transactielimiet.

[4] EACB (2023) Digital euro. EACB Position Paper, 28 maart.

digitale euro is geen spaar product, rol ECB wordt te groot op deze manier.

een hogere limiet dit eveneens kan realiseren.[5][6][7] De ECB is momenteel bezig met het uitwerken van een voorstel voor een methodologie om de aanhoudingslimieten vast te stellen, met aandacht voor onder meer gebruiksgemak en financiële stabiliteit. Dit voorstel wordt naar verwachting in september gepubliceerd en zal meer inzicht geven in het vraagstuk. Het voorstel voor de methodologie zal geen concrete limiet bevatten, mogelijk wel een bandbreedte.

Communicatie
Niet van toepassing.

Politiek/bestuurlijke context
De Tweede Kamer stelt met regelmaat schriftelijke vragen over de toegevoegde waarde van de digitale euro, over de Nederlandse rol in de onderhandelingen en over privacy en niet-programmeerbaarheid. In het Schriftelijk Overleg rond de Eurogroep/Ecofinraad van mei 2025 werden vragen gesteld door de VVD-fractie, de BBB-fractie en de PVV-fractie over deze onderwerpen. Maandelijks wordt daarnaast gerapporteerd aan de Kamer over de voortgang van de digitale euro onderhandelingen.

Informatie die niet openbaar gemaakt kan worden
Niet van toepassing

[5] Meller en Soons (2022) Occasional Paper Series: Know your (holding) limits: CBDC, financial stability and central bank reliance.
[6] Lambert, Pancaro en Pellicani (2023) A digital euro: gauging the financial stability implications.
[7] Van der Horst en van Gent (2025) The offline digital euro and holding limits: a user-centred approach

Geprint met Digidoc 2 op 25-06-2025, 12:26

Parafenoverzicht

Werkmap

Onderwerp:	FM 165700 - Strategie digitale euro
Nummer:	2025-0000015540
Algemeen taakverzoek:	

Document: FM165700 - strategie digitale euro (2025-0000165700)

5.1.2e