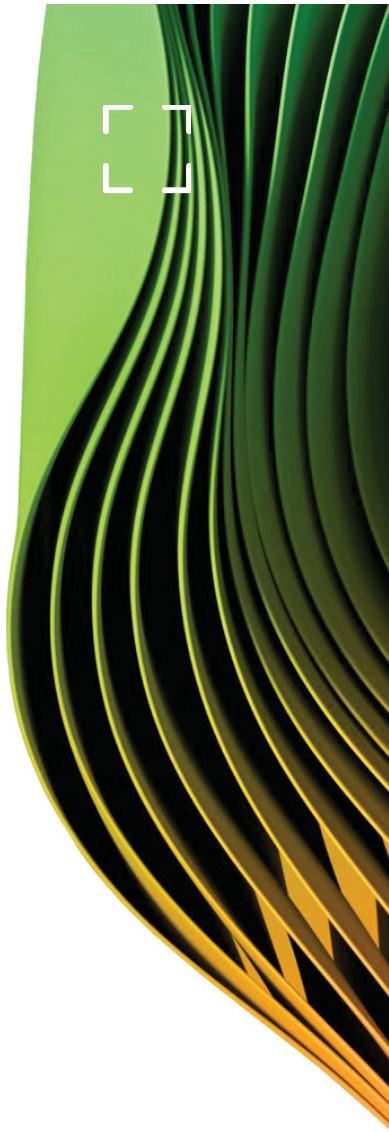
Deloitte.

Verkennend onderzoek naar anti-fraudecentra

Rapportage | Ministerie van Justitie en Veiligheid

29 mei 2026

Inhoudsopgave



0. Managementsamenvatting

(1/3)

Aanleiding

Online fraude groeit snel in schaal en complexiteit. Digitalisering in communicatie, financiële transacties en opslag van gevoelige informatie, in combinatie met de groei van het internetgebruik en socialmediaplatforms, zijn factoren die daar aan ten grondslag liggen. De problematiek van online fraude wordt bovendien door de rol van Kunstmatige Intelligentie versterkt. Binnen Nederland en de EU, maar ook daarbuiten, wordt consequent het belang van een gecoördineerde publiek-private aanpak onderstreept. Daarbij wordt een samenhangende keten van preventie, detectie, repressie en slachtofferhulp als noodzakelijk gezien. Dit roept de vraag op of het bundelen van kernfuncties in één centraal knooppunt de effectiviteit van de aanpak van online fraude kan vergroten.

Samenhang met de Integrale Aanpak tegen Online Fraude

Binnen deze context heeft het ministerie van Justitie en Veiligheid aan Deloitte de opdracht gegeven om onderzoek te doen naar een aantal vooraf geselecteerde anti-fraudecentra ter ondersteuning van de doorontwikkeling van de Integrale Aanpak tegen Online Fraude (IAOF). De IAOF beoogt samenwerking structureel en organisatorisch te borgen door stevige inzet en betrokkenheid van partners, focus op delen van gegevens, barrières en interventies, regie op resultaten, innovatie als fundament en (internationale) samenwerking. De feitelijke bevindingen op hoofdlijnen uit dit onderzoek dienen ter ondersteuning van het besluitvormingsproces rondom een mogelijk Nederlands ‘fraudecentrum’ en de verdere doorontwikkeling van de IAOF.

Doelstelling en reikwijdte onderzoek

Het doel is het systematisch in kaart brengen en vergelijken van vier anti-fraudecentra. De volgende centra zijn geanalyseerd:

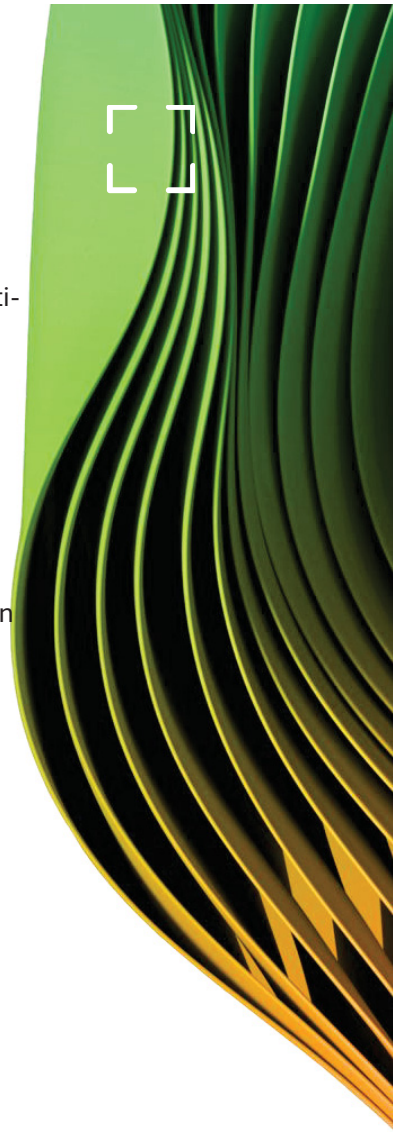
- National Anti-Scam Centre (NASC) – Australië;
- Centre for Cybersecurity Belgium (CCB) – België;
- Stop Scams UK (SSUK) – Verenigd Koninkrijk;
- Stichting Informatieknooppunt Zorgfraude (IKZ) – Nederland.

Het rapport heeft nadrukkelijk een verkennend karakter en is geen beslisdocument. De bevindingen en inzichten vormen een basis voor reflectie over welke elementen toepasbaar, wenselijk en uitvoerbaar zijn binnen de Nederlandse context.

Onderzoeksaanpak

De onderzoeksaanpak is iteratief en gebaseerd op verifieerbare informatie, bestaande uit drie fasen:

1. Een documentenanalyse van openbare bronnen;
2. Interviews met sleutelpersonen bij de vier centra ter verificatie en verdieping;
3. Een integratie en validatie van alle bevindingen in een vergelijkende analyse gefinaliseerd tot een rapport.

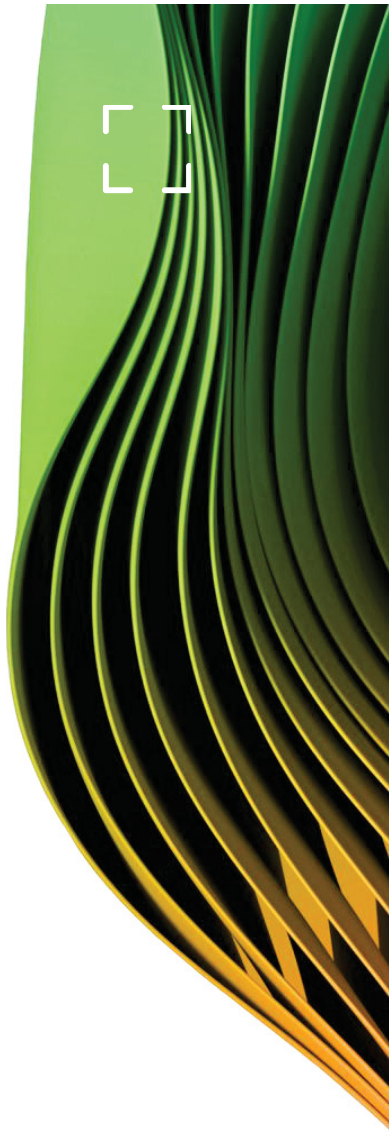


0. Managementsamenvatting
(2/3)

Bevindingen anti-fraudecentra

- **CCB**, opgericht in 2014, is een federale overheidsinstelling en functioneert als publieke autoriteit op het gebied van cyberveiligheid. Het CCB speelt een centrale rol in Europese kaders zoals NIS2, de Cyber Resilience Act en de Cybersecurity Act. Het centrum vervult een coördinerende, beleidsmatige en toezichthoudende rol en heeft van oorsprong een voorname oriëntatie op organisaties (organisaties van vitaal belang (OVI's), bedrijven, overheden) en heeft daar ook een oriëntatie op consumentenbescherming aan toegevoegd. Het Belgian Anti-Phishing Shield (BAPS) is daar een voorbeeld van en blokkeert jaarlijks circa 240 miljoen bezoeken aan kwaadaardige websites.
- **SSUK** is een private non-profit organisatie, bestaat sinds 2020 en wordt gefinancierd door leden die afkomstig zijn uit de financiële, telecom- en techsector. Deelname is vrijwillig, maar de participatie uit de sectoren is groot (de leden dekken >99% van de particuliere bankrekeningen en 100% van de mobiele operators). SSUK functioneert als intermediair met een centraal dataplatform voor pilots. De 159-lijn is een voorbeeld van een project dat landelijk opgeschaald is. Het is een kort, niet-spoofbaar telefoonnummer dat burgers en bedrijven in het Verenigd Koninkrijk kunnen bellen bij verdachte communicatie van banken om veilig verbonden te worden met hun bank. Sinds de start in 2021 zijn meer dan 1 miljoen oproepen verwerkt.
- **NASC** is in juli 2023 ingesteld onder de Australian Competition & Consumer Commission en fungeert als publiek knooppunt, dat is verankerd in de Scams Prevention Framework Act. Deze wet verplicht private sectoren tot samenwerking en staat boetes tot AUD 50 miljoen toe. Een belangrijk onderdeel binnen de aanpak van NASC zijn thematische Fusion Cells: tijdgebonden, multidisciplinaire en vaak cross-sectorale projectteams die zich met een operationele focus richten op de technische en tactische ontwrichting van een specifiek type oplichting. Zo resulteerde de Fusion Cell Job Scams in de verwijdering van >29.000 social-media accounts. Daarnaast heeft NASC in 2025 meer dan 7.500 scam-URL's verwijderd (+30% t.o.v. 2024) en verwees het ruim vier keer zoveel telefoonnummers door aan telecompartners voor verstoring.
- **IKZ** is opgericht per 1 januari 2025 als privaatrechtelijke stichting met wettelijke taak (op grond van de Wet bevorderen samenwerking en rechtmatige zorg) en bouwt voort op een sinds 2016 bestaand samenwerkingsverband. Het IKZ verbindt negen partners, met als doel om signalen over zorgfraude te bundelen en uitwisseling tussen partners mogelijk te maken. Dit gebeurt via ontvangst en verrijking van signalen van zorgfraude tot Samengestelde Informatieproducten (SIPs), delen van SIPs met partners, organiseren van casustafels en middels trend- en fenomeenonderzoek. Het ontving in 2025 678 signalen van de negen partners.

De initiatieven van de centra bieden input voor de besluitvorming over de mogelijke producten, diensten en functies bij de eventuele inrichting van een Nederlands 'fraudecentrum'. Die zijn in dit rapport geordend op basis van de zes pijlers van de IAOF.



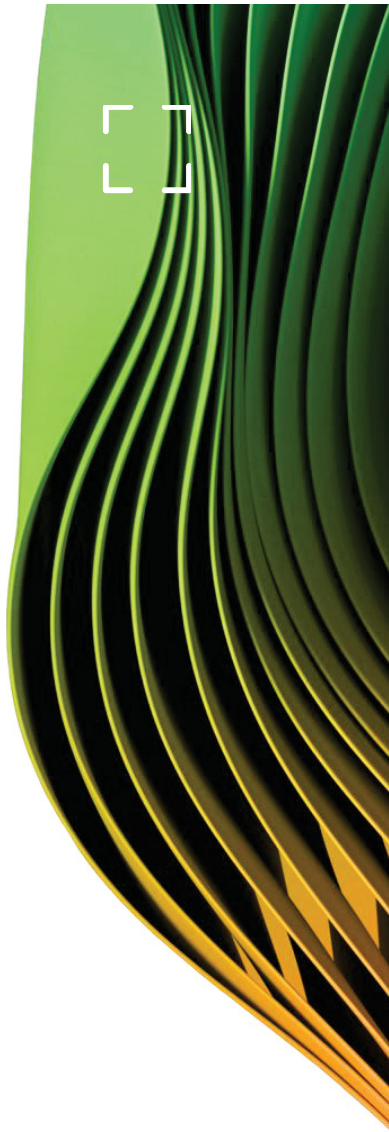
0. Managementsamenvatting

(3/3)

Verkenning op hoofdlijnen als basis voor besluitvorming

De vier onderzochte centra vertegenwoordigen verschillende modellen voor de bestrijding van fraude. Zij verschillen onder meer in omvang, doelstelling, mandaat en middelen. Naast de feitelijke bevindingen, biedt dit rapport inzicht in enkele (randvoorwaardelijke) factoren die mogelijk van invloed kunnen zijn op de effectiviteit van een fraudecentrum en relevant kunnen zijn bij een eventueel inrichtingsvraagstuk van een fraudecentrum in Nederland.

- **Privaat vs. Publiek.** De centra verschillen in de mate waarin publieke en private organisaties aangesloten zijn, in het hart dan wel in de periferie van de samenwerking. CCB coördineert publieke en private samenwerkingen binnen nationale en Europese cybersecurity kaders, NASC fungeert als verbinder en faciliteert publiek-private samenwerking. IKZ verbindt publieke partners en private zorgverzekeraars, terwijl SSUK een private organisatie is die uitsluitend uit private partijen bestaat, maar ook relaties met publieke instanties onderhoudt.
- **Wettelijke basis en afdwingbaarheid.** Het spectrum loopt van wettelijk afdwingbare deelname met handhavingsmogelijkheden (NASC) tot volledig vrijwillig op basis van gezamenlijk belang en de angst om kansen mis te lopen (SSUK). CCB en IKZ hebben een wettelijke basis, maar zijn voor opvolging en handhaving afhankelijk van partners in de keten.
- **Voorlichting vs. Operationele instrumenten voor interventies.** De rol varieert van voorlichting en bewustwording tot een focus op operationele instrumenten voor interventies. NASC en CCB combineren beide. Ook de SSUK richt zich op beide dimensies, maar met een steviger accent op operationele instrumenten, waar hun pilot-projecten een voorbeeld van zijn. IKZ richt zich primair op operationele interventies door partners, maar organiseert ook casustafels en fenomeentafels. Hun rol is faciliterend; partners voeren de interventies uit.
- **Consumenten vs. Organisaties.** CCB heeft een focus op organisaties van vitaal belang (OVI's), bedrijven en overheden, maar ook op consumenten via SafeOnWeb. SSUK is uitsluitend gericht op consumenten met hun 159-lijn en zet hier de expertise van de drie sectoren voor in. NASC combineert beide, verzamelt meldingen van burgers via Scamwatch maar faciliteert ook publiek-private samenwerking. IKZ richt zich met name op de partners die onderdeel zijn van het samenwerkingsverband.
- **Architectuur voor gegevensdeling.** Er is een duidelijk onderscheid tussen centra met gecentraliseerde, geautomatiseerde systemen voor grootschalige, real-time dataverwerking (NASC, CCB) en een aanpak waarin data meer verspreid en handmatig is, gericht op specifieke pilots of casuïstiek (SSUK, IKZ).



1. Inleiding en achtergrond
(1/3)

1.1 Aanleiding

Online fraude groeit snel in schaal en complexiteit. Digitalisering in communicatie, financiële transacties en opslag van gevoelige informatie, in combinatie met de groei van het internetgebruik en socialmediaplatforms, zijn factoren die daaraan ten grondslag liggen. De problematiek van online fraude wordt bovendien door de rol van Kunstmatige Intelligentie versterkt. Politieonderzoeken registreren tienduizenden online fraudezaken en een breed scala aan technieken en modus operandi. Online fraude leidt tot grote financiële en emotionele impact, die zich niet alleen beperkt tot de directe slachtoffers, maar vaak ook impact heeft op gezinnen of complete families. Het verlies van spaartegoeden, oudedagvoorzieningen en/of potentiële erfenissen kan de toekomst van velen ontwrichten. Nationaal, Europees en internationaal wordt daarom consequent het belang van een gecoördineerde publiek-private aanpak onderstreept en een samenhangende keten van preventie, detectie, repressie en slachtofferhulp als noodzakelijk gezien.*

1.2 Integrale Aanpak tegen Online Fraude en verzoek tot onderzoek

De doorontwikkeling van de Integrale Aanpak tegen Online Fraude (hierna: “IAOF”) beoogt samenwerking structureel en organisatorisch te borgen, door de inrichting van een organisatie voor onder meer informatiedeling en meldingen. Voorbeelden uit het buitenland (o.a. Australië, België en het Verenigd Koninkrijk) laten zien dat er verschillende modellen bestaan; binnen Nederland biedt de Stichting Informatieknooppunt Zorgfraude leerpunten vanuit een ander domein.

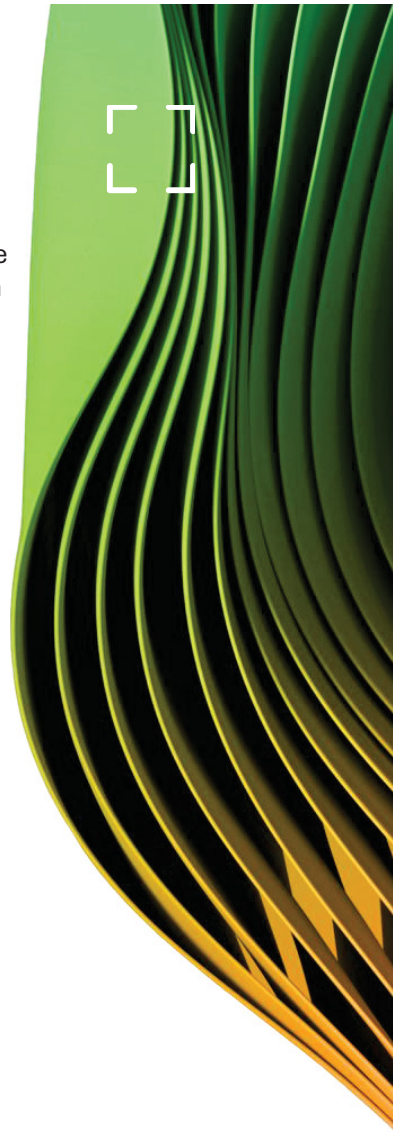
Deze ontwikkelingen maken het moment geschikt om te verkennen welke lessen uit het feitelijke onderzoek naar anti-fraudecentra kunnen worden meegenomen, en hoe deze mogelijk kunnen bijdragen aan de inrichting van een Nederlands ‘fraudecentrum’. Om besluitvorming over een mogelijk anti-fraudecentrum te ondersteunen, heeft het ministerie van Justitie en Veiligheid (hierna: “ministerie van JenV”) aan Deloitte Consultative Services B.V. (hierna: “Deloitte”) gevraagd een verkennend onderzoek uit te voeren naar anti-fraudecentra en/of knooppunten in het binnen- en buitenland.

1.3 Doelstelling

Dit onderzoek heeft tot doel om relevante elementen van de beschreven anti-fraudecentra op hoofdlijnen in kaart te brengen, waaronder:

- Doel en functie;
- Maatschappelijk effect;
- Organisatiestructuur;
- Juridische grondslag en bevoegdheden;
- Taken en producten;
- Begroting en wijze van financiering; en
- Klantrelaties en samenwerking met partners.

Deze set is gebaseerd op de opdrachtformulering van het ministerie van JenV en vormt het vergelijkend analysekader voor de factsheet over de genoemde anti-fraudecentra in dit rapport (zie voor meer duiding hoofdstuk 3 en in het bijzonder *Bijlage I. Factsheet*).



*Europol (2024), *Internet Organized Crime Threat Assessment 2024;* Politie (2024), *Online Fraude in Beeld: Fenomeenbeeld 2024;* Europol (2025), *Steal, deal and repeat: How Cybercriminals trade and exploit your data;* United Nations (2026), *Global Fraud Summit 2026: Call to Action on Combating Fraud.*

1. Inleiding en achtergrond
(2/3)

1.4 Reikwijdte

Het onderzoek omvat een analyse van vier anti-fraudecentra en/of vergelijkbare knooppunten, waarbij zowel beleid en governance als de operationele praktijk worden betrokken:

- Centre for Cybersecurity Belgium (hierna: “CCB”) – België;
- Stop Scams UK (hierna: “SSUK”) – Verenigd Koninkrijk;
- National Anti-Scam Centre (hierna: “NASC”) – Australië;
- Stichting Informatieknooppunt Zorgfraude (hierna: “IKZ”) – Nederland.

Per centrum worden de in 1.3 genoemde aspecten onderzocht, zodat vergelijkbare, feitelijke informatie beschikbaar komt ter ondersteuning van het besluitvormingsproces binnen het ministerie van JenV en de verdere doorontwikkeling van de IAOF.

1.5 Leeswijzer

De opzet van dit rapport is als volgt:

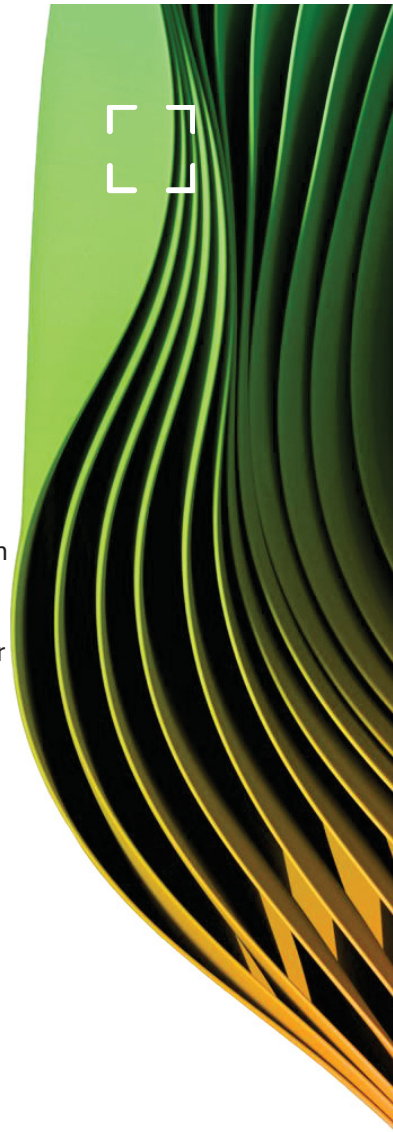
- De managementsamenvatting bevat een korte beschrijving van opzet en uitkomsten van dit onderzoek;
- Hoofdstuk 1 beschrijft de aanleiding, doelstelling en reikwijdte van dit onderzoek;
- Hoofdstuk 2 bevat informatie over de onderzoeksuitgangspunten, onderzoeksaanpak en tijdslijnen;
- Hoofdstuk 3 toont de introductie van de anti-fraudecentra en hoog-over analyse aan de hand van het vergelijkend analysekader;
- Hoofdstuk 4 bevat verdiepende analyses op de anti-fraudecentra aan de hand van geselecteerde thema’s;
- Hoofdstuk 5 beschrijft de IAOF waarbij de initiatieven vanuit de anti-fraudecentra geplot zijn op de zes pijlers van de IAOF.

De bijlagen bestaan uit: I. Factsheet, II. Begrippenlijst en III. Bronnenlijst. Een overzicht van geïnterviewde personen is op aanvraag beschikbaar.

1.6 Verkenning op hoofdlijnen als basis voor besluitvorming

Dit rapport is opgesteld in opdracht van het ministerie van JenV en biedt een strategische verkenning op hoofdlijnen. Het rapport dient ter ondersteuning van het denk- en besluitvormingsproces rondom een mogelijk Nederlands ‘fraudecentrum’ en de verdere doorontwikkeling van de IAOF. Het rapport heeft nadrukkelijk een verkennend karakter en is geen beslisdocument. De bevindingen en inzichten vormen een basis voor reflectie over welke elementen toepasbaar, wenselijk en uitvoerbaar zijn binnen de Nederlandse context.

Hoewel het beschikbare onderzoeksmateriaal geen eenduidig beeld geeft welk 'type' organisatie het meeste effectief is, ontstaat bij elk van de vier centra de indruk dat de bundeling en borging van kernfuncties in één centraal knooppunt de effectiviteit van de (anti-)fraudeketen versterkt – zowel bij de formeel aangesloten partners als bij de partners in de periferie van de samenwerking van de betreffende centra. Een fraudecentrum, met nationale en integrale focus, is in staat om het betreffende fraude onderwerp in de keten op de agenda te zetten en aangesloten organisaties duurzaam 'in beweging' te krijgen.



1. Inleiding en achtergrond
(3/3)

1.6 Verkenning op hoofdlijnen als basis voor besluitvorming (vervolg)

Naast de feitelijke bevindingen, biedt dit rapport daarom inzicht in enkele factoren die mogelijk van invloed kunnen zijn op de effectiviteit van een fraudecentrum en relevant kunnen zijn bij een eventueel inrichtingsvraagstuk van een fraudecentrum in Nederland. De anti-fraudecentra dekken namelijk verschillende organisatiemodellen (publiek, privaat, hybride), juridische verankering (wettelijke verplichtingen en afdwingbaarheid versus vrijwilligheid en vrijblijvendheid) en reikwijdte (van brede cybersecurity tot vormen van (online) oplichting tot zorgfraude). Het is daarbij van belang om op te merken dat dit niet tot een panklaar recept leidt, op basis waarvan een fraudecentrum zou moeten worden opgebouwd. Het zijn kenmerken die in overweging kunnen worden genomen bij een eventueel vervolg.

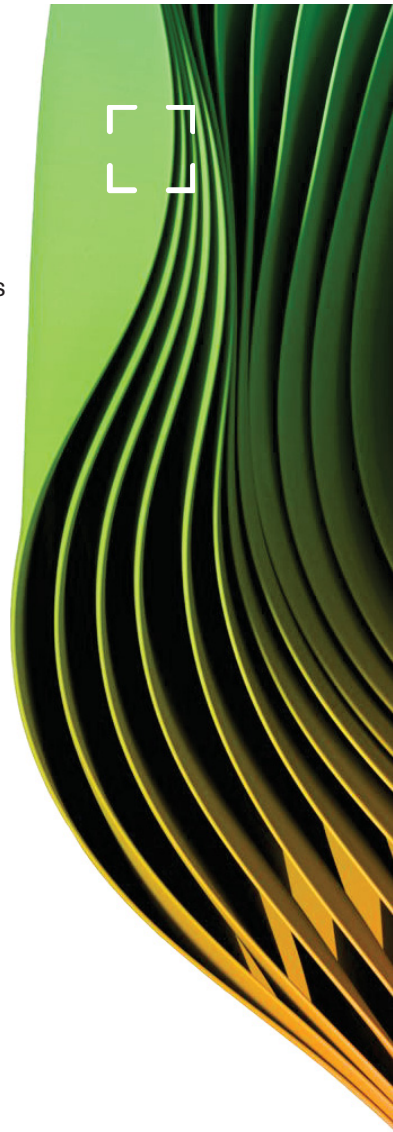
Het gaat daarbij bijvoorbeeld om de mate waarin een anti-fraudecentrum beschikt over een wettelijke basis en publieke, private of hybride samenstelling. Publieke centra zoals het CCB, NASC en IKZ opereren vanuit een overheidsmandaat en zijn ingebed in bestaande wettelijke kaders. SSUK werkt daarentegen als private ledenorganisatie, op basis van vrijwillige afspraken tussen deelnemende partijen, zonder eigen wettelijk mandaat.

Een ander kenmerk is de mate van afdwingbaarheid. Sommige centra beschikken zelf over toezicht- of nalevingsbevoegdheden. Andere centra zijn vooral afhankelijk van samenwerking met bevoegde partners, zoals toezichthouders, politie of justitie.

Ook de mate van (gecentraliseerde en/of geautomatiseerde) gegevensdeling – van informatie over een fraudefenomeen tot subjectgegevens – komt in alle centra terug en wordt op verschillende manieren georganiseerd. Bij IKZ bestaat bijvoorbeeld een wettelijke basis voor het ontvangen, verrijken en doorgeleiden van signalen binnen de zorgfraudeketen. SSUK werkt juist met vrijwillige datadeling op basis van afspraken tussen leden. Gegevensdeling, ook van persoonsgegevens, is niet alleen een technische kwestie, maar vraagt ook om juridische grondslagen en het opbouwen van vertrouwen tussen organisaties.

Tenslotte is de mate waarin anti-fraudecentra zich richten op producten en diensten die direct door consumenten en/of door organisaties/bedrijven worden afgenomen een onderscheidend element – waarin het een het ander niet hoeft uit te sluiten.

Hoofdstuk 4 biedt inzicht in deze factoren, die in meer of mindere mate aanwezig zijn bij de vier centra en van invloed kunnen zijn op de effectiviteit van een anti-fraudecentrum en mogelijk relevant kunnen zijn bij een eventueel inrichtingsvraagstuk van een fraudecentrum in Nederland.



2. Onderzoeksaanpak

2.1 Inleiding

Dit hoofdstuk zet de onderzoeksaanpak uiteen voor het verkennend onderzoek naar de vier geselecteerde anti-fraudecentra. Het doel van het onderzoek is om een vergelijkend overzicht te realiseren van relevante centra om werkwijzen te identificeren die relevant kunnen zijn voor de Nederlandse context. De aanpak, die iteratief is en gebaseerd op verifieerbare informatie, bestaat uit drie fasen: (1) voorbereiding en documentenanalyse, (2) interviews en verdieping en (3) afronding en terugkoppeling. Voor de vergelijkbaarheid is een vooraf vastgesteld analysekader toegepast dat zich richt op vaste aspecten – gebaseerd op de opdrachtformulering van het ministerie van JenV.

Fase 1:
Voorbereiding en documentenanalyse

Week 0-3

Beschrijving
- Leggen van de feitelijke basis en inrichting van het onderzoek. Dit omvat de afstemming van de onderzoeksopzet en de systematische analyse van openbare bronnen

Activiteiten
- Vaststellen van de onderzoeksopzet, planning en gewenste opleveringen in startbijeenkomsten met de opdrachtgever en de klankbordgroep
- Uitwerken van het vergelijkend analysekader en systematisch analyseren van bronnen
- Samenbrengen van de uitkomsten in een overkoepelende concept-factsheet, inclusief het identificeren van vragen voor fase 2

Resultaten
- Vastgestelde onderzoeksopzet, planning en vergelijkend analysekader
- Een overkoepelende concept-factsheet met kernkenmerken en geïdentificeerde vragen ter verdieping
- Een gerichte interviewagenda voor fase 2

Fase 2:
Interviews en verdieping

Week 4-6

Beschrijving
- Verifiëren en verdiepen van de bevindingen uit de documentenanalyse door middel van gerichte gesprekken. De focus ligt op de operationele praktijk, governance, juridische kaders, financiering en uitvoering(sknelpunten)

Activiteiten
- Afname van interviews met sleutelpersonen bij de geselecteerde centra
- Verwerken van de uitkomsten in één concept-factsheet
- Voorleggen van de concept-factsheet aan de vier centra ter verificatie
- Verwerken van de feedback op feitelijke juistheid

Resultaten
- Afgeronde interviews met sleutelpersonen
- Eén concept-factsheet, aangevuld met de bevindingen uit de interviews
- Een door de centra op feitelijke juistheid geverifieerde factsheet

Fase 3:
Afronding en terugkoppeling

Week 7-8

Beschrijving
- Integreren van de onderzoeksresultaten tot een vergelijkende analyse, het toetsen van bevindingen en prioritering in een validatiesessie, en het vaststellen van het definitieve rapport met terugkoppeling

Activiteiten
- Integreren van alle resultaten tot een samenhangende, vergelijkende analyse
- Organiseren van een validatiesessie met de kerngroep en de opdrachtgever om prioritering te toetsen
- Vaststellen van het definitieve, feitelijke rapport
- Verzorgen van een inhoudelijke terugkoppeling aan de opdrachtgever

Resultaten
- Door de kerngroep en opdrachtgever gevalideerde prioritering
- Een geactualiseerde factsheet die als vergelijkend kader dient
- Afgeronde inhoudelijke terugkoppeling aan de opdrachtgever

3. Analyse op anti-fraudecentra
(1/7)

3.1 Inleiding

Deze analyse richt zich op de vier anti-fraudecentra met uiteenlopende profielen die samen een relevant spectrum aan ontwerpopties voor een Nederlands ‘fraudecentrum’ illustreren:

- Een publieke coördinatieorganisatie met een wettelijke basis en een sterke focus op private partijen (NASC);
- Een nationale publieke autoriteit met sterke EU-inbedding – o.a. de NIS en NIS2-richtlijn (CCB);
- Een vrijwillige non-profit ledenorganisatie vanuit de private sector (SSUK);
- Een Nederlandsspecifiek informatieknooppunt met een wettelijke taak binnen het zorgdomein (IKZ).

De selectie is onder andere gemotiveerd door een inschatting van relevantie voor de Nederlandse context, op basis van de verschillende organisatiemodellen (publiek, privaat, hybride), reikwijdte in taakopvatting (van brede cybersecurity tot vormen van oplichting tot zorgfraude) en de operationele instrumenten die worden ingezet. De vier anti-fraudecentra bieden samen inzicht in zowel systeeminrichting (regels, governance, financiering) als uitvoeringsprocessen (meldkanalen, takedowns, waarschuwingen, thematische samenwerkingsinitiatieven). Deze combinatie biedt een basis voor het afwegen van ontwerpkeuzes en randvoorwaarden voor een mogelijk Nederlands ‘fraudecentrum’. Hierna volgt een korte introductie van de vier geselecteerde anti-fraudecentra voor dit onderzoek.

3.2 Introductie Cybersecurity Centre België (CCB)

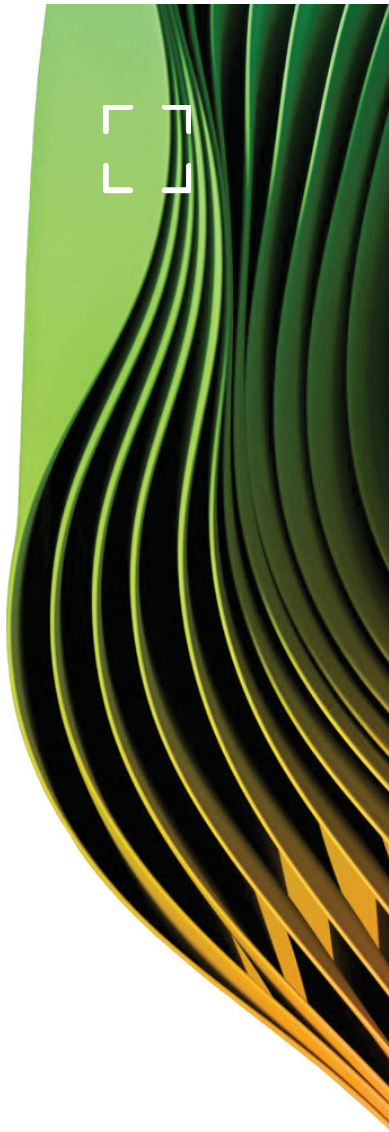
Het CCB werd in 2014 opgericht bij Koninklijk Besluit, mede naar aanleiding van een toename aan cyberincidenten in de periode 2012–2014 (waaronder de Belgacom-hack), de Europese oproep tot nationale coördinatie van cyberveiligheid en de implementatie van Europese regelgeving zoals de NIS1-richtlijn, inmiddels opgevolgd door de NIS2-richtlijn. Het CCB speelt een centrale rol in Europese kaders zoals NIS2, de Cyber Resilience Act en de Cybersecurity Act.

Doel is het bewaken, coördineren en versterken van de nationale cyberweerbaarheid, met de ambitie om België tot de minst kwetsbare landen van Europa te maken. Kernfuncties beslaan onder andere:

- Preventie: Belgian Anti-Phishing Shield en bewustwording via SafeOnWeb en het CyberFundamentals-raamwerk;
- Detectie: Early Warning System, gerichte “spear warnings” voor dreigingsinformatie;
- Recover: Incidentrespons en crisiscoördinatie via CERT.be.

Het type fraude/dreiging is breed en omvat onder meer ransomware, DDoS-aanvallen, datalekken, cyberspionage en phishing.

Het CCB is een publieke, federale autoriteit en valt momenteel onder de bevoegdheid van de Eerste Minister. In de toekomst verschuift dit naar het ministerie van Binnenlandse zaken. Voor dit rapport wordt uitgegaan van de huidige situatie.



3. Analyse op anti-fraudecentra
(2/7)

3.3 Introductie Stop Scams UK (SSUK)

SSUK is in 2020 opgericht als reactie op de snelle groei van oplichting in het Verenigd Koninkrijk, waar fraude de meest voorkomende vorm van criminaliteit is. Doel is om oplichting bij de bron te stoppen door gestructureerde samenwerking tussen banken, technologiebedrijven en telecomaanbieders te bevorderen. Kernfuncties omvatten onder andere:

- Facilitering van gegevensuitwisseling en proefprojecten die belemmeringen voor samenwerking en interventies wegnemen;
- Bescherming van slachtoffers via het korte, niet te vervalsen beveiligde nummer 159 (rechtstreekse veilige verbinding met de bank);
- Beïnvloeding van beleid en regelgeving om effectieve gegevensdeling mogelijk te maken.

Het type fraude in scope betreft vormen van online fraude, zoals phishing, bankhelpdeskfraude en beleggingsfraude en de technieken die daar aan ten grondslag liggen (zoals spoofing).

SSUK is een door de private sector geleide ledenorganisatie (non-profit) zonder handhavende bevoegdheden; deelname is vrijwillig en de organisatie wordt gefinancierd door de aangesloten leden.

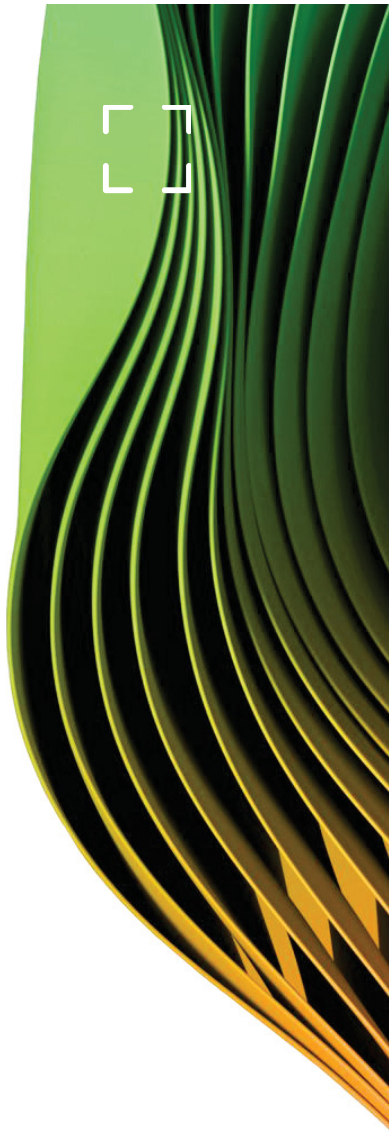
3.4 Introductie National Anti-Scam Centre (NASC)

NASC is in juli 2023 ingesteld onder de Australian Competition & Consumer Commission (hierna: “ACCC”) naar aanleiding van de behoefte aan een gecoördineerde, systeembrede aanpak van online oplichting en het doorbreken van gefragmenteerde gegevensdeling. Doel is versterking van samenwerking tussen overheid, opsporing en private partijen, het mogelijk maken van gegevensdeling en het organiseren van gecoördineerde acties tegen oplichting. Kernfuncties zijn onder andere:

- Preventie en verstoring door tijdgebonden, publiek-private Fusion Cells tegen specifieke oplichtingstypen;
- Publieksbewustwording met campagnes als Stop. Check. Protect;
- Melden van fraude via Scamwatch;
- Slachtofferondersteuning door doorverwijzing naar gespecialiseerde diensten.

Het type fraude in scope omvat onder meer beleggingsfraude, bankhelpdeskfraude, datingfraude en phishing.

NASC heeft een publieke knooppuntfunctie binnen de overheid (ACCC) en werkt nauw samen met private partijen. De Scams Prevention Framework Act 2025 geeft het stelsel een juridische basis met verplichtingen voor banken, telecom en platforms en wettelijke basis voor NASC om boetes op te leggen bij niet-naleving.



3. Analyse op anti-fraudecentra
(3/7)

3.5 Introductie Stichting Informatieknooppunt Zorgfraude (IKZ)

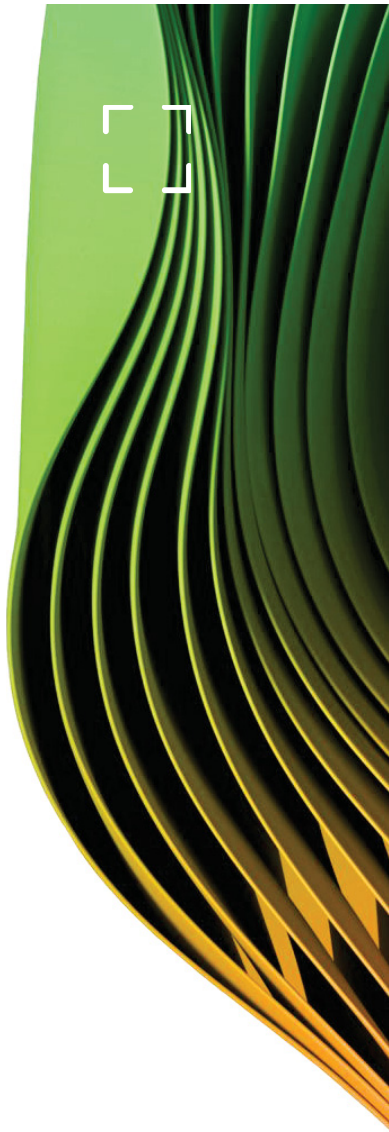
IKZ is opgericht per 1 januari 2025 als privaatrechtelijke stichting met wettelijke taak (op grond van de Wet bevorderen samenwerking en rechtmatige zorg). De stichting bouwt voort op een sinds 2016 bestaand samenwerkingsverband. Aanleiding was de behoefte aan een centraal, juridisch geborgd knooppunt om signalen over zorgfraude te bundelen en uitwisseling tussen partners mogelijk te maken.

Doel is het voorkomen en aanpakken van misbruik van zorggelden door zorgfraudesignalen van negen partners te verzamelen, te verrijken en gericht door te leiden. Kernfuncties omvatten:

- Informatie-uitwisseling door team Casuïstiek; onder meer door verrijking en deling van Samengestelde Informatieproducten (SIPs) en organiseren van casustafels
- Onderzoek en analyse door team Onderzoek & Analyse; onder meer door trend- en fenomeenonderzoek, fenomeentafels en kennisdeling)

Het type fraude in scope betreft zorgspecifieke vormen zoals upcoding, spookzorg en onvoldoende of onjuiste zorgverlening.

IKZ is een publieke stichting met wettelijke taak (RWT), zonder handhavende of opsporingsbevoegdheden; detectie en opvolging worden verzorgd door de bevoegde partners (zoals toezichthouders, opsporingsdiensten en gemeenten).



3. Analyse op anti-fraudecentra

(4/7)

3.6 Introductie anti-fraudecentra

Onderstaand overzicht vat de eerder beschreven kernkenmerken van de centra samen

	Centre for Cybersecurity Belgium (CCB)	Stop Scams UK (SSUK)	National Anti Scam Centre (NASC)	Stichting Informatieknooppunt Zorgfraude (IKZ)
Oprichtingsjaar	2014	2020	2023	2016 (samenwerkingsverband) 2025 (stichting)
Aanleiding	Toenemende cyberdreiging en EU-strategie (2013)	Fraude: meest voorkomende misdaad in Engeland en Wales (41%)	Ontbreken van gecoördineerde systeembrede aanpak van online fraude	Behoefte aan centraal juridisch geborgd knooppunt voor informatie-uitwisseling tussen partners over zorgfraude
Scope/insteek	Preventie, detectie en herstel	Preventie, detectie en respons	Preventie, detectie en respons	Informatie-uitwisseling, onderzoek en analyse
Type fraude	Cybersecurity: ransomware, DDoS-aanvallen, datalekken, malware, cyberespionage, phishing, CEO-fraude	Geautoriseerde push-betalingen: beleggingsfraude, bankhelpdeskfraude, factuurfraude, BEC-fraude, phishing, vishing en spoofing	Geautoriseerde push-betalingen, waaronder beleggingsfraude (incl. crypto), datingfraude, phishing, remote access-fraude, vacaturefraude	Zorgfraude: upcoding, spookzorg en onvoldoende of onjuiste zorgverlening
Strategie	Versterken van de cyberweerbaarheid: bewustwording, detectie en verstoring	Faciliteren van sectorsamenwerking voor preventie, bescherming en beleid	Preventie en verstoring van oplichting, bewustwording en slachtofferhulp via publiek-private samenwerking	Verzamelen en analyseren van zorgfraudesignalen en faciliteren van samenwerking tussen partners
Aansluiting bij nationale context	Coördineren van cybersecuritybeleid en publiek-private samenwerking binnen nationale en EU-kaders	Verbinden van private partijen in een landelijk ecosysteem voor datadeling en preventie en afstemming richting/met publieke partijen	Verbinden van publieke en private partijen en vertalen van data naar actiegerichte inzichten	Verbinden van publieke zorgpartijen en private zorgverzekeraars, verrijken signalen en stimuleren gezamenlijke analyse

3. Analyse op anti-fraudecentra

(5/7)

3.7 Vergelijkend analysekader

Onderstaand overzicht bevat een nadere uitwerking van het vergelijkend analysekader dat is beschreven in paragraaf 1.3. Dit vergelijkend analysekader is ontwikkeld aan de hand van de opdrachtomschrijving vanuit het ministerie van JenV

- **Doel:** beschrijving van de doelstelling en aansluiting van het doel bij de kerntaken en strategie
- **Functie:** beschrijving van de verschillende functies (waaronder registratie van meldingen, informatiedeling, verwerking persoonsgegevens en samenwerking met partners
- **Maatschappelijk effect:** beschrijving van de effectiviteit en het beoogde maatschappelijk effect (onderbouwd met cijfers)
- **Organisatiestructuur:** beschrijving van de organisatiestructuur (publiek/-privaat, inrichting afdelingen en wijze van bemensing)
- **Juridische grondslag:** beschrijving van de juridische grondslag en bevoegdheden
- **Taken en producten:** beschrijving van taken en producten (waaronder nieuwsberichten en rapportages)
- **Begroting:** beschrijving van de kostenopbouw op basis van een begroting
- **Wijze van financiering:** beschrijving van wijze van financiering
- **Samenwerking met partners:** beschrijving van wijze waarop organisaties hun relaties met partners en klanten vormgeven

3. Analyse op anti-fraudecentra
(6/7)

3.8 Hoog-over analyse

Onderstaand overzicht presenteert de belangrijkste bevindingen uit de documentenanalyse en de interviews. De opbouw volgt het analysekader zoals toegelicht in paragraaf 3.7. Voor een gedetailleerder beeld wordt verwezen naar de volledige factsheet in Bijlage I en een diepgaandere analyse van de initiatieven in hoofdstuk 5. Definities van specifieke termen zijn opgenomen in de begrippenlijst (Bijlage II)

	CCB	SSUK	NASC	IKZ
Doel	Beschermen van organisaties van vitaal belang (OVI's), bedrijven en burgers tegen cyberdreiging en fraude door preventie, detectie en herstel bij incidenten. Vervult de rol als nationale coördinator van de cyberintegratie en implementatie van EU-regels	Bestrijden van fraude door cross-sectorale samenwerking en datadeling tussen banken, technologiebedrijven en telecomaanbieders met operationele pilots en gerichte preventiecampagnes. Vervult de rol als facilitator tussen drie sectoren om fraude gezamenlijk tegen te gaan	Beschermen van burgers en bedrijven tegen fraude en oplichting via publiek-private samenwerkingen, voorlichtingscampagnes, meldkanalen en doorverwijzing naar hulpdiensten. Vervult de rol als facilitator van samenwerking tussen publieke en private partijen, centralisatie en analyse van data	Voorkomen en bestrijden van zorgfraude door verrijking, analyse en doorgeleiding van fraudesignalen, kennisdeling en faciliteren operationele aanpak op casusniveau
Functie	Nationaal cybercentrum dat online fraudemeldingen registreert via SafeOnWeb en cybermeldingen via CERT.be, waarschuwingen deelt en publiek-private incidentrespons coördineert	Bemiddelaar die veilige datadeling tussen banken, telecom en techbedrijven faciliteert via pilots	Nationale virtuele hub die registratie van meldingen, publiekscampagnes, data-analyse, partnercoördinatie en doorverwijzing naar slachtofferhulporganisatie IDCARE combineert	Ketenplatform voor zorgfraude dat signalen van partners verrijkt met gegevens en bronnen van partners, zoals het Handelsregister, analyseert en gericht doorgeleidt
Maatschappelijk effect	Versterken van cyberweerbaarheid via detectie, waarschuwing en incidentherstel: in 2025 635 incidenten behandeld, 10 miljoen verdachte e-mails verwerkt en 82% van de burgers is bekend met SafeOnWeb	Bestrijden van fraude door veilige datadeling en interventies tussen banken, telecoms en techbedrijven: sinds de start in 2021 > 1 miljoen 159-oproepen en een bereik van >99% van Britse betaalrekeningen	Beperken van schade door het analyseren van melddata, publiekscampagnes, blokkades en slachtofferdoorverwijzing: in 2025 6,5 miljoen Scamwatch-bezoekers en 200,675 Scamwatch-rapporten, >7.500 scam-URL's verwijderd en 8.536 doorverwijzingen naar IDCARE	Versterken van zorgfraudebestrijding door signalen van vermoedens van zorgfraude te verrijken, analyseren en doorgeleiden aan partners: in 2025 678 signalen ontvangen, 11 casustafels georganiseerd
Organisatie-structuur	Publieke federale overheidsinstantie met coördinerende afdelingen, twee operationele afdelingen (CERT.be en CyTRIS) en centrale stafdiensten; circa 135 fte	Private non-profit ledenorganisatie met klein kernteam dat samenwerking, beleid, pilots en datadeling faciliteert. Uitvoering leunt sterk op leden en partners; circa 21 stafleden	Publieke overheidsorganisatie onder de ACCC. 31 FTE in de operationele teams van NASC (datadeling; intelligence; verstoring, fusion cells; educatie en outreach). Dit is exclusief personeel dat werk doet op gebied van IT, strategische communicatie en handhaving	Onafhankelijke, privaatrechtelijke stichting met wettelijke taak voor signaalverwerking, analyse en ketencoördinatie in de zorgfraudeketen met twee operationele kernteams; circa 16,5 fte

3. Analyse op anti-fraudecentra
(7/7)

3.8 Hoog-over analyse (vervolg)

	CCB	SSUK	NASC	IKZ
Juridische grondslag	Publieke federale overheidsinstantie met taken en bevoegdheden vanuit EU- en nationale cyberregelgeving, waaronder NIS2. CCB coördineert cyberveiligheid en toezicht binnen NIS2, maar heeft geen bredere privaatrechtelijke handhavingsmacht	Private non-profit ledenorganisatie zonder eigen wettelijk mandaat. SSUK werkt via vrijwillige lidmaatschaps- en datadelingsovereenkomsten en kan samenwerking faciliteren, niet afdwingen	Publiek centrum binnen de ACCC met juridische grondslag: Scams Prevention Framework Act die aangewezen sectoren tot medewerking en datadeling verplicht. Heeft handhavingsbevoegdheid bij niet-naleving (boetes)	Rechtspersoon (stichting) met Wettelijke Taak (RWT) binnen de Wbsrz, wat data-deling mogelijk maakt. IKZ heeft de taak om signalen te verzamelen, te verrijken en te delen met partners, maar heeft zelf geen handhavings-, toezicht-, of opsporingsbevoegdheid
Taken en producten	Richt zich op detectie, waarschuwing en incidentherstel via o.a. SafeOnWeb, CERT.be, BAPS, EWS, CyberFundamentals-raamwerk, jaarverslagen, Cyber Threat Reports en technische adviezen	Faciliteert pilot-projecten en structurele programma's, zoals het Blocked SIMs-programma en de 159-lijn. Datadeling ter ondersteuning van deze projecten vindt plaats via een beveiligd dataplatform (AWS). Verschillende publicaties over fraude.	Beheert Scamwatch, bundelt melddata van Scamwatch, IDCARE, ReportCyber en AFCX, coördineert en publiceert Fusion Cell-rapporten, jaarlijkse rapporten over oplichting en voorlichtingsmaterialen (Little Book of Scams)	Ontvangt en verrijkt signalen van zorgfraude tot Samengestelde Informatieproducten en deelt deze met partners, publiceert thematische onderzoeken, organiseert casustafels, fenomeentafels en inspiratiesessies
Begroting	Totale begroting: €36.000.000 (2025) Een gedetailleerde, openbare begroting van CCB is niet beschikbaar	Een gedetailleerde, openbare begroting van SSUK is niet beschikbaar	Een gedetailleerde, openbare begroting van NASC is niet beschikbaar	Totale begroting: €3.991.464 (2025) Kostenopbouw 2025 is terug te vinden op pagi. 8 van het openbare jaarverslag, via: https://www.ikz.nl/wp-content/uploads/2026/03/2025-133-IKZ-jaarverslag_07.pdf
Wijze van financiering	Publiek gefinancierd via de Belgische federale begroting; budget groeit naar circa €36 miljoen in 2025	Privaat gefinancierd via ledenbijdragen en donaties	Publiek gefinancierd via de ACCC; aanvankelijk voor 3 jaar, verlengd met 1 jaar (2026-2027)	Publiek gefinancierd via een jaarlijkse toekenning van financiële bijdrage van VWS
Samenwerking	Werkt breed samen met federale overheden, politie, EU-netwerken, financiële instellingen en vitale bedrijven. De samenwerking richt zich vooral op cyberdetectie, waarschuwingen, incidentrespons en ondersteuning van OVI's	Functioneert als neutrale verbinder tussen banken, telecom en techbedrijven. Daarnaast samenwerking met politie (NCA)	Coördineert publiek-private samenwerking tussen toezichthouders, politie, banken, telecoms, social-mediaplatforms en slachtofferhulp	Verbindt negen zorgpartners: Nza, IGJ, Belastingdienst, FIOD, CIZ, SVB, NLA, gemeenten (VNG), zorgverzekeraars & zorgkantoren. Ministerie VWS is beleidsverantwoordelijk

4. Verdiepende analyse anti-fraudecentra

(1/11)

4.1.1 Inleiding

In het vorige hoofdstuk zijn de vier geselecteerde anti-fraudecentra geïntroduceerd. Dit hoofdstuk verdiept de analyse van de vier anti-fraudecentra door op hoofdlijnen hun overeenkomsten en verschillen in kaart te brengen. Deze dimensies weerspiegelen fundamentele keuzes en randvoorwaarden voor de effectiviteit van een anti-fraudecentrum:

1. *Organisatiestructuur (privaat vs. publiek):* de positionering van een anti-fraudecentrum als publieke of private organisatie;
2. *Wettelijke basis en afdwingbaarheid:* de wettelijke basis op grond waarvan een anti-fraudecentrum kan opereren en de mate waarin interventies kunnen worden afgedwongen;
3. *Voorlichting vs. operationele interventies:* de mate waarin een anti-fraudecentrum zich richt op voorlichting en bewustwording versus instrumenten voor operationele interventies;
4. *Doelgroep (consumenten vs. organisaties):* de mate waarin een anti-fraudecentrum zich richt op consumenten versus organisaties;
5. *Architectuur van gegevensdeling:* de wijze waarop data wordt uitgewisseld (gecentraliseerd/verspreid) en de verwerkingssnelheid.

4.1.2 Leeswijzer bij dit hoofdstuk

Het is van belang om op te merken dat de centra verschillen in onder meer omvang, doelstelling, mandaat en middelen. Vanwege die diversiteit is de classificering van de centra langs de genoemde dimensies voor meerdere interpretaties vatbaar en niet eenduidig. De weergave betreft een inschatting op basis van de beschikbare informatie. De dimensies en de weergave zijn bedoeld om richting te geven aan de dialoog, zonder daarbij iets uit te drukken over de unieke meerwaarde die elk van de centra biedt.

4. Verdiepende analyse anti-fraudecentra

(2/11)

4.2 Verdiepende analyse: Privaat vs. publiek

Deze dimensie ziet op de mate waarin publieke en private partijen zijn aangesloten bij de centra. De onderzochte centra verschillen in de mate waarin publieke en private partijen structureel zijn aangesloten. CCB is publiek gepositioneerd en coördineert publieke en private samenwerking binnen nationale en Europese cyberveiligheidskaders. SSUK is een private, door de private sector geleide organisatie. NASC vervult een verbindende rol tussen publieke en private partijen. IKZ verbindt publieke partners met private zorgverzekeraars binnen de zorgfraudeketen.

4.2.1 CCB

De samenwerking van het CCB is primair publiek ingebed, onder meer via afstemming met nationale overheidsdiensten en Europese netwerken. Tegelijkertijd werkt het CCB ook nauw samen met private partijen, waaronder organisaties van vitaal belang (OVI's) en bedrijven. Dit gebeurt bijvoorbeeld via SafeOnWeb en certificeringstrajecten. Het CCB is een federale overheidsinstelling en functioneert als publieke autoriteit op het gebied van cyberveiligheid. Het centrum is opgericht bij Koninklijk Besluit en vervult een coördinerende, beleidsmatige en toezichthoudende rol. Binnen de NIS2-scope houdt het CCB toezicht op meer dan 4.000 organisaties in 18 sectoren.

4.2.2 Stop Scams UK

In tegenstelling tot het CCB is Stop Scams UK een private, door de private sector geleide, non-profit organisatie. Binnen dit samenwerkingsverband zijn uitsluitend private partijen lid, voornamelijk uit de banken-, telecom-, en techsector. SSUK onderhoudt daarnaast nauwe banden met publieke partners, zoals opsporingsinstanties.

Figuur 4.2. Positionering van de vier anti-fraudecentra op de dimensies privaat vs. publiek (X-as: Publiek; Y-as: Privaat)

4. Verdiepende analyse anti-fraudecentra
(3/11)

SSUK heeft geen wettelijk mandaat; de werking is gebaseerd op vrijwillige deelname en consensus. De organisatie wordt gefinancierd door haar leden.

4.2.3 NASC

NASC fungeert als verbindende partij tussen publieke en private partijen. Het centrum is ondergebracht bij de ACCC, een publieke toezichthouder, heeft een adviesraad met vertegenwoordigers uit de private sector en werkt intensief samen met private partijen uit diverse sectoren. Deze samenwerking is wettelijk vastgelegd: de Scams Prevention Framework Act 2025 maakt het mogelijk om deelname van partners zoals banken, telecombedrijven en socialmediaplatforms te verplichten. NASC faciliteert samenwerking tussen overheidsinstanties, zoals politie en toezichthouders, en private organisaties, met name banken, telecombedrijven en socialmediaplatforms.

4.2.4 IKZ

IKZ werkt samen met negen partners: acht publieke partijen, zoals gemeenten en inspecties, en private zorgverzekeraars. IKZ is een onafhankelijke, privaatrechtelijke stichting met een wettelijke taak binnen de zorgfraudeketen. Sinds 1 januari 2025 heeft IKZ een wettelijke grondslag op basis van de Wet bevordering samenwerking en rechtmatige zorg. De stichting wordt gefinancierd met publieke middelen (€ 3,99 miljoen per jaar) en valt binnen de beleidsverantwoordelijkheid van het ministerie van VWS. De kerntaak van het IKZ is het ontvangen, verrijken en doorgeleiden van zorgfraudesignalen naar partners.

4. Verdiepende analyse anti-fraudecentra

(4/11)

4.3 Verdiepende analyse: Wettelijke basis en afdwingbaarheid

Deze dimensie meet de wettelijke basis op grond waarvan een anti-fraudecentrum kan opereren en de mate waarin interventies kunnen worden afgedwongen. Hoewel drie van de vier centra een wettelijke basis hebben, varieert de mate van afdwingbaarheid aanzienlijk. NASC bezit directe, bestuursrechtelijke afdwingingsmacht via haar positionering onder de ACCC. CCB en IKZ zijn afhankelijk van de afdwingingsmacht van partners. SSUK opereert volledig zonder juridische afdwingbaarheid en is gebaseerd op vrijwilligheid.

4.3.1 CCB

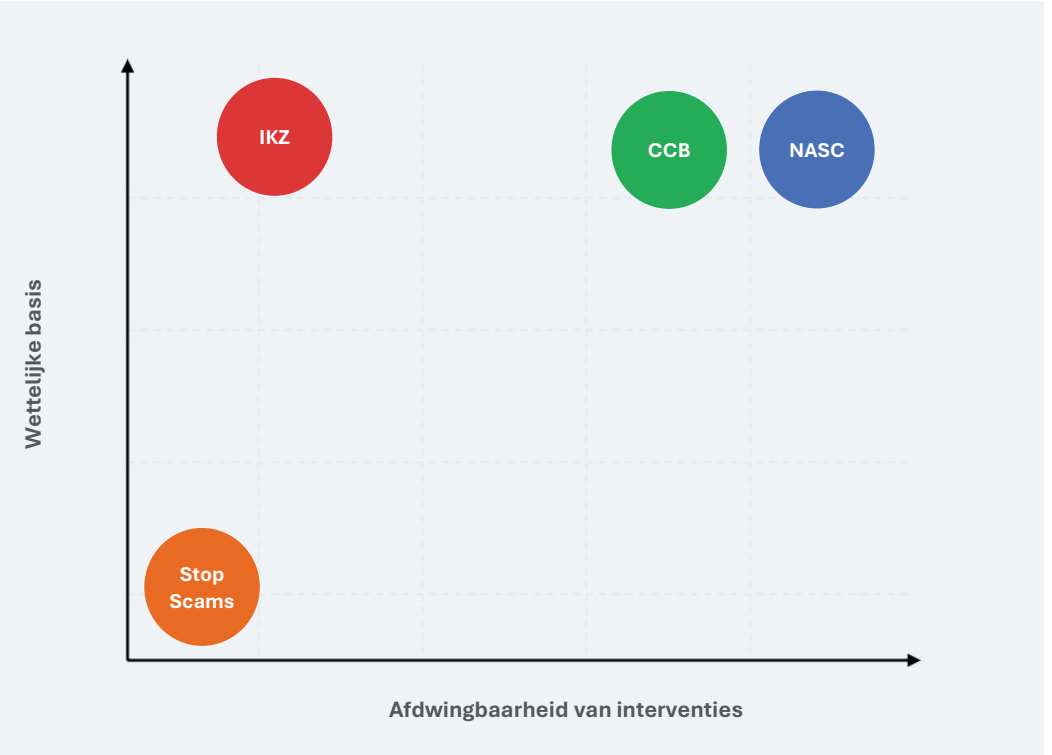
Het CCB opereert onder een Koninklijk Besluit uit 2014 en coördineert de implementatie van EU-wetgeving zoals NIS2 en de Cyber Resilience Act. Het CCB stelt richtlijnen op, oefent in bepaalde domeinen - onder andere in de rol als NCCA en toezichthouder onder NIS2 - ook toezicht- en nalevingsbevoegdheden uit. Strafrechtelijke handhaving verloopt via het Openbaar Ministerie en de relevante opsporingsdiensten.

4.3.2 Stop Scams UK

SSUK is een private non-profitorganisatie zonder wettelijk mandaat. In het Verenigd Koninkrijk ontbreekt een overkoepelende wet die cross-sectorale gegevensdeling verplicht stelt. Deelname is volledig vrijwillig. De effectiviteit van SSUK berust op de reputatie en het collectieve belang van de aangesloten leden, niet op juridische instrumenten.

4.3.3 NASC

Het NASC opereert onder de Scams Prevention Framework Act 2025. Deze wet verplicht banken, telecombedrijven en socialmediaplatforms tot het nemen van maatregelen.



Figuur 4.3. Positionering van de vier anti-fraudecentra op de dimensies wettelijke basis (Y-as) en afdwingbaarheid van interventies (X-as)

4. Verdiepende analyse anti-fraudecentra

(5/11)

De ACCC, toezichthouder op consumentenbescherming en digitale platforms, werkt samen met sectorale toezichthouders zoals ACMA voor telecom en ASIC voor financiële dienstverlening en kan bij niet-naleving boetes opleggen tot AUD 50 miljoen (bestuursrechtelijke afdwinging).

4.3.4 IKZ

Het IKZ heeft sinds 1 januari 2025 een formele wettelijke basis vastgelegd in de Wet bevordering samenwerking en rechtmatige zorg (Wbsrz). Deze wet verplicht partners om vermoedens van zorgfraude bij IKZ te melden. IKZ beschikt echter zelf niet over handhavings- of opsporingsbevoegdheden; detectie en (opsporings)interventies worden uitgevoerd door de partners (o.a. zorgverzekeraars, gemeenten, FIOD).

4. Verdiepende analyse anti-fraudecentra

(6/11)

4.4 Verdiepende analyse: Voorlichting vs. operationele interventies

Deze dimensie meet de mate waarin een anti-fraudecentrum zich richt op voorlichting en bewustwording versus operationele instrumenten voor interventies. NASC en CCB combineren beide. SSUK richt zich zowel op voorlichting als op operationele instrumenten voor interventies. IKZ richt zich voornamelijk op operationele instrumenten voor interventies via partners.

4.4.1 CCB

Het CCB combineert voorlichting en kennisdeling met instrumenten voor operationele interventies. Via SafeOnWeb (meldingsplatform en educatie), Quarterly Cyber Threat Reports en honderden technische advisories informeert CCB burgers en organisaties over cyberdreigingen. Operationeel signaleert het CCB dreigingen via het Early Warning System (EWS) en het Belgian Anti-Phishing Shield (BAPS) blokkeert automatisch schadelijke websites (240 miljoen bezoeken per jaar). Dit is een preventief model: burgers worden geïnformeerd en dreigingen worden proactief afgewend.

4.4.2 SSUK

Stop Scams UK combineert operationele instrumenten met voorlichting. Het hoofdprogramma is de 159-dienst: een kort telefoonnummer dat bellers direct veilig doorverbindt met hun bank voor real-time bescherming. Daarmee wordt de interactie met een mogelijke fraudeur op een kritiek moment doorbroken. Daarnaast faciliteert Stop Scams UK pilots (zoals Blocked SIMs) die door leden worden uitgevoerd om operationele interventies te testen. Publicaties, waaronder “The Future of Fraud”, en bewustwordingscampagnes vullen deze operationele aanpak aan met voorlichting en bewustwording.

Figuur 4.4. Positionering van de vier anti-fraudecentra op de dimensies focus op operationele instrumenten voor interventies (Y-as) en focus op voorlichting en bewustwording (X-as)

4. Verdiepende analyse anti-fraudecentra

(7/11)

4.4.3 NASC

NASC combineert beide dimensies. Voor voorlichting: Scamwatch publiceert jaarlijks het Targeting Scams Report met trends en modi operandi. NASC voert educatiecampagnes uit (Stop. Check. Protect.). Voor operationele interventies: NASC coördineert Fusion Cells die fraudenetwerken verstoren, URLs verwijderen en telefoonnummers blokkeren. In 2025 verwijderde NASC meer dan 7.500 scam-URLs en blokkeerde 4.246 telefoonnummers. Dit is een geïntegreerd model: burgers worden geïnformeerd en fraudeurs worden aangepakt.

4.4.4 IKZ

IKZ richt zich primair op instrumenten voor operationele interventies via partners. Het organiseert fenomeentafels voor specifieke onderwerpen (bv diplomafraude) en casustafels waar partners gezamenlijk fraudefenomenen aanpakken. In 2025 verwerkte IKZ 678 signalen en organiseerde het 11 casustafels. Voor voorlichting en bewustwording: IKZ publiceert gedetailleerde rapporten over misbruik (bv turboliquidaties). De rol is facilitair: partners voeren interventies uit. Dit is een handhavingsgericht model: fraude wordt aangepakt via partners; er is geen sprake van directe consumentenbescherming.

4. Verdiepende analyse anti-fraudecentra

(8/11)

4.5 Verdiepende analyse: Consumenten vs. organisaties

Deze dimensie meet de mate waarin een anti-fraudecentrum zich richt op consumentenbescherming versus organisatiegerichte maatregelen. NASC en CCB richten zich op beide. Stop Scams UK richt zich sterk op consumenten. IKZ richt zich op organisaties (partners).

4.5.1 CCB

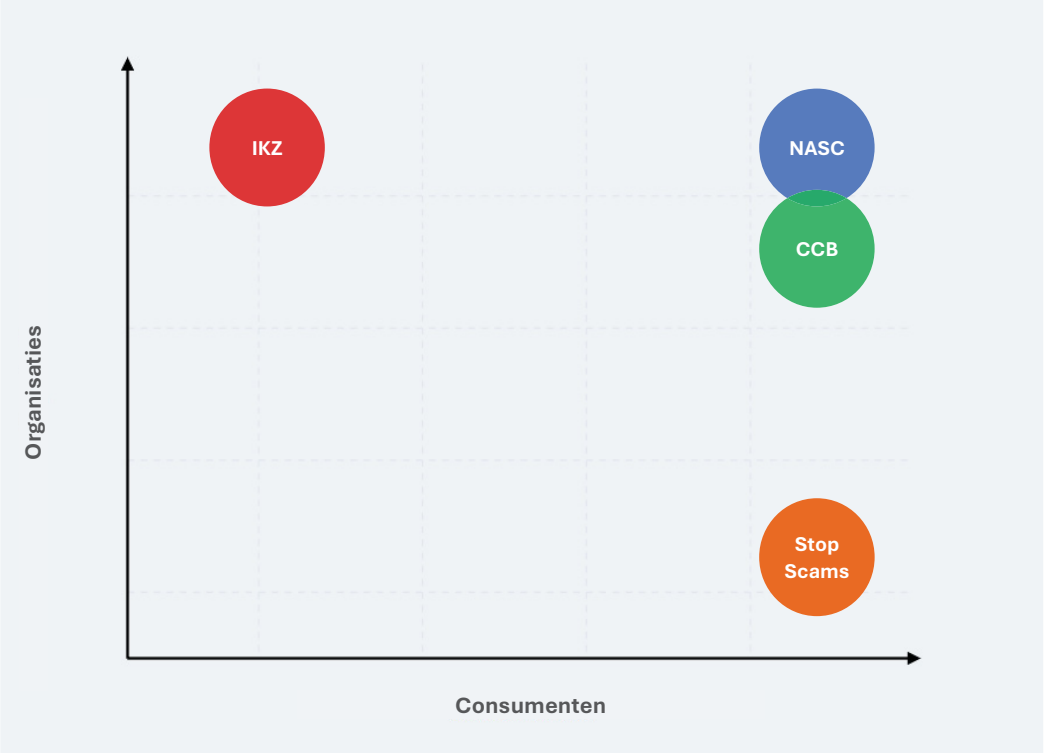
Het CCB combineert beide dimensies. Het richt zich op organisaties via SafeOnWeb (@work) door hulp bij certificering voor de NIS2-richtlijn, biedt technische expertise en bijstand bij cyberaanvallen, en fungeert als contactpunt voor incidentmeldingen, waarschuwingen en analyses. CCB richt zich op consumenten via SafeOnWeb(@home): meldingsplatform en educatie. In 2025 verwerkte SafeOnWeb bijna 10 miljoen verdachte e-mails.

4.5.2 SSUK

Stop Scams UK richt zich bijna uitsluitend op consumenten. De 159-dienst is het kernprogramma: een kort telefoonnummer dat bellers direct doorverbindt met hun bank voor real-time bescherming. In 2025 verwerkte de 159-dienst meer dan 1 miljoen oproepen. Voor bedrijven: Stop Scams UK faciliteert pilots die door leden (banken, tech, telecom) worden uitgevoerd. Dit is een consumentgerichte aanpak: bescherming van burgers staat centraal.

4.5.3 NASC

NASC combineert beide dimensies. Voor consumenten: Scamwatch verzamelt meldingen van burgers (481.523 in 2025). NASC publiceert waarschuwingen en educatie. Voor organisaties: NASC legt verplichte maatregelen op aan banken, telecombedrijven en socialmediaplatforms via de SPF Act 2025.



Figuur 4.5. Positionering van de vier anti-fraudecentra op de dimensies Organisaties (Y-as) en Consumenten (X-as)

4. Verdiepende analyse anti-fraudecentra

(9/11)

Dit is een geïntegreerd model: burgers worden beschermd en organisaties worden verplicht deel te nemen.

4.5.4 IKZ

IKZ richt zich primair op organisaties (partners). Het bundelt signalen van negen partners (gemeenten, zorgverzekeraars, inspecties) en faciliteert informatie-uitwisseling. In 2025 verwerkte IKZ 678 signalen en organiseerde het 11 casustafels. Voor consumenten: IKZ publiceert geen directe waarschuwingen aan burgers. De rol is faciliterend: partners voeren handhaving uit. Dit is een organisatiegerichte aanpak: fraude wordt aangepakt via partners, niet via directe consumentenbescherming.

4. Verdiepende analyse anti-fraudecentra

(10/11)

4.6 Verdiepende analyse: Architectuur van gegevensdeling

Deze dimensie meet de mate van centralisatie en de mate van automatisering van gegevensdeling. Dit gaat om hoe informatie wordt verzameld, verwerkt en gedeeld tussen partners. NASC en CCB hebben gecentraliseerde systemen waar gegevens op één plek samenkomen. SSUK is momenteel een gecentraliseerd systeem aan het ontwikkelen waar gegevens van partners op één plek kunnen samenkomen. IKZ ontvangt uitsluitend door de partners ingediende signalen van zorgfraude, de achterliggende dossiers blijven bij de partners.

4.6.1 CCB

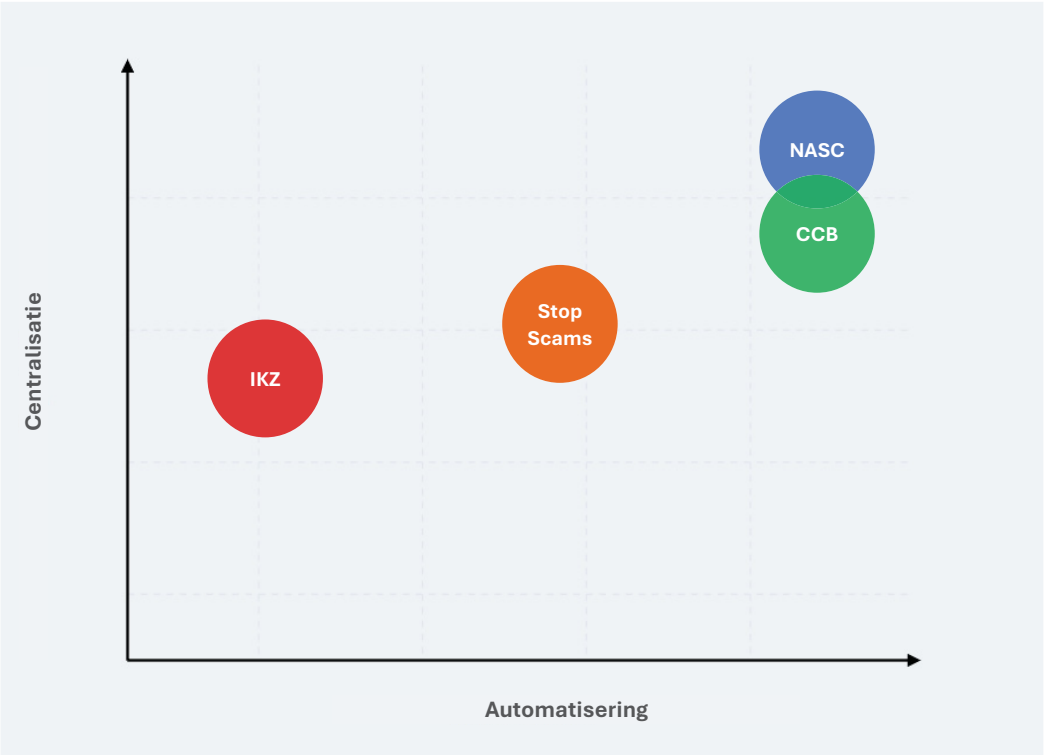
Het CCB opereert met meerdere gecentraliseerde systemen. Meldingen via SafeOnWeb en detecties door het EWS en BAPS leiden tot real-time actie. Lijsten met kwaadaardige URL's worden continu bijgewerkt en automatisch onderschept. Dit model kenmerkt zich door automatisering en real-time distributie.

4.6.2 SSUK

SSUK bevindt zich in een transitie van ad-hoc uitwisseling naar een gecentraliseerd, geautomatiseerd systeem. De organisatie heeft een eigen platform gebouwd op Amazon Web Services (AWS) om data sneller in te nemen en te distribueren. Er lopen circa 15 technologische pilots, waarvan er 6 operationeel zijn.

4.6.3 NASC

NASC opereert via Scamwatch, een centraal platform waar consumenten oplichting melden. Deze meldingen vormen de basis voor NASC's analyse.



Figuur 4.6. Positionering van de vier anti-fraudecentra op de dimensies centralisatie (Y-as: verspreid tot gecentraliseerd) en automatisering (X-as: handmatig tot automatisch/real-time)

4. Verdiepende analyse anti-fraudecentra
(11/11)

Gegevens worden snel verwerkt en gedeeld: NASC deelt wekelijks telefoonnummers met ongeveer 11 telecomaanbieders voor blokkering. Het deelt verdachte bankgegevens met AFCX (een non-profit gegevensdelingsplatform van ongeveer 11 banken) voor actie door de financiële sector.

4.6.4 IKZ

IKZ ontvangt signalen van partners en verrijkt deze met gegevens uit het Handelsregister, het dashboard Zicht op Zorgaanbieders en de Basisregistratie Personen (BRP). Verrijking vindt eveneens plaats met gegevens van partners, die zij op verzoek van IKZ moeten leveren. Achterliggende dossiers van de vermoedens van zorgfraude blijven bij partners (NZa, IGJ, FIOD, CIZ, SVB, NLA, gemeenten, zorgverzekeraars). In Wbsrz is vermeld welke partner welke informatie moet leveren. IKZ verwerkt deze signalen tot Samengestelde Informatieproducten; 1.710 in 2025. Verrijkte signalen worden gedeeld met aangesloten partners voor opvolging. Het proces is grotendeels handmatig. Technische koppelingen voor automatische gegevensdeling zijn in ontwikkeling en bevinden zich in een vergevorderde fase.

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(1/17)

5.1 Inleiding

In dit hoofdstuk worden de inzichten uit de voorgaande analyse (hoofdstuk 3 en 4) en de gedetailleerde factsheet (Bijlage II) gespiegeld aan het huidige programma van de Integrale Aanpak tegen Online Fraude (IAOF). Het doel is tweeledig:

- Werkwijzen identificeren die kunnen bijdragen aan de doorontwikkeling van de IAOF;
- Input leveren voor de besluitvorming over de mogelijke producten, diensten en functies bij de oprichting van een Nederlands 'fraudecentrum'.

De analyse die volgt is niet uitputtend, maar dient als referentiemateriaal voor verdere gedachtevorming, prioritering en besluitvorming.

5.2 Achtergrond en doel IAOF

Online fraude vormt een groeiend maatschappelijk probleem dat jaarlijks miljoenen burgers en bedrijven raakt en een belangrijk verdienmodel is voor georganiseerde criminaliteit. Om het aantal slachtoffers en de maatschappelijke schade terug te dringen, werken publieke en private partijen sinds medio 2022 samen binnen de IAOF. Ter ondersteuning van besluitvorming over een mogelijk Nederlands anti-fraudecentrum heeft het ministerie van JenV een verkennend onderzoek laten uitvoeren naar vier binnen- en buitenlandse anti-fraudecentra. De IAOF brengt partijen uit de gehele fraudeketen samen – van preventie tot technische barrières tot opsporing en slachtofferhulp – met als doel sneller, gerichter en efficiënter op te treden en zodoende de kansen voor criminelen om slachtoffers te maken, te reduceren.

Dit wordt nagestreefd via twee primaire strategische lijnen:

1. *Verhogen van de weerbaarheid*: het beter bestand maken van burgers en bedrijven tegen frauduleuze handelingen door preventie en bewustwording;
2. *Verstoren van criminele processen*: het implementeren van (technische) barrières en het verbeteren van de opsporing en vervolging om criminele activiteiten te bemoeilijken.

In het actieplan voor 2026 wordt de focus van de IAOF gelegd op het behalen van concrete en meetbare resultaten om het aantal slachtoffers van online fraude terug te dringen. Deze resultaten zijn ondergebracht in zes pijlers waar publieke en private partners gezamenlijk aan werken.

5.3 Ecosysteem van samenwerkingspartners

De IAOF wordt gedragen door een kerngroep van 13 publieke en private partners. Het ministerie van JenV voert de regie en zorgt voor de coördinatie. De kerngroep bestaat uit:

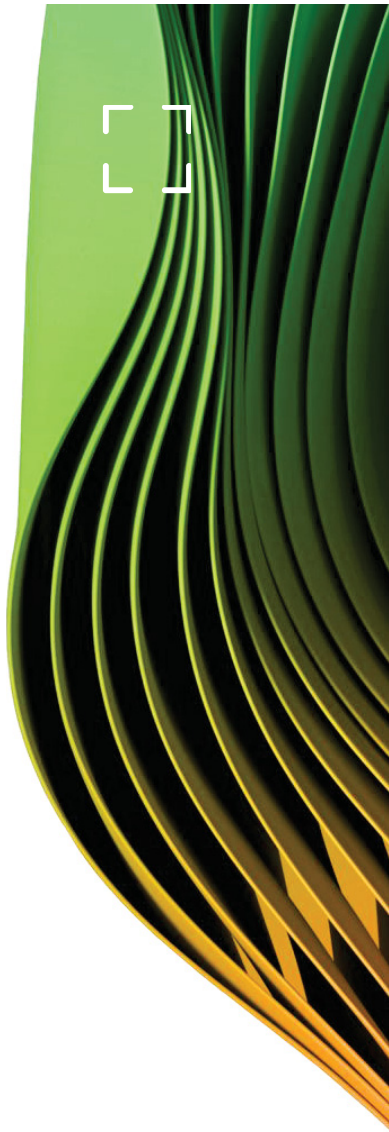
Overheid	Ministerie van Economische Zaken, ministerie van Financiën, ministerie van Justitie en Veiligheid, Politie, Openbaar Ministerie (OM) en Vereniging van Nederlandse Gemeenten (VNG)
Financiële sector	Nederlandse Vereniging van Banken (NVB) en De Nederlandsche Bank (DNB)
Bedrijfsleven en Infrastructuur	VNO-NCW/MKB Nederland, Thuiswinkel.org en COIN
Consumenten-belangen en hulpverlening	Consumentenbond, Fraudehelpdesk en Veiliginternetten.nl

5. IAOF: aanpak, activiteiten en anti-fraudecentra
(2/17)

Naast de kerngroep werkt de IAOF ook samen met een breder netwerk van meer dan 55 organisaties uit verschillende sectoren. Deze partners dragen bij aan specifieke doelen, zoals het ontwikkelen van barrières en interventies, en omvatten de meld- en hulporganisaties die samenwerken om de best mogelijke zorg voor slachtoffers te realiseren.

5.4 Introductie: zes pijlers van de IAOF

De zes pijlers van de IAOF hebben als doel de problematiek in de gehele fraudeketen te adresseren. Het jaarlijkse actieplan geeft richting aan de samenwerking en zorgt voor focus en prioritering. Het actieplan 2026 bouwt voort op de eerdere fase van opbouw en verbinding, maar legt sterker de nadruk op resultaatgerichte samenwerking, stevigere partnerbetrokkenheid en meer regie op concrete resultaten. Paragraaf 5.5 licht de zes pijlers toe zoals vastgesteld in het actieplan 2026, inclusief de bijbehorende activiteiten die de IAOF langs deze pijlers verricht.



5. IAOF: aanpak, activiteiten en anti-fraudecentra

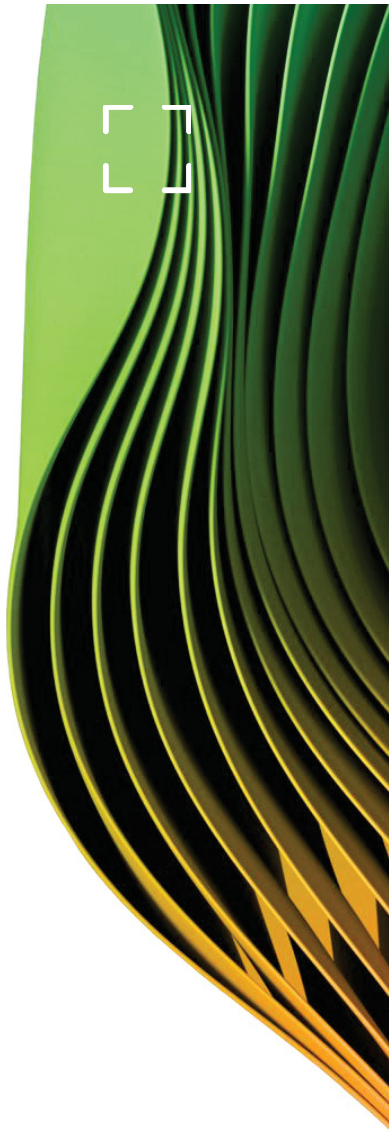
(3/17)

5.5 De zes pijlers van de IAOF

Hieronder volgt een gedetailleerde uitwerking van de pijlers van de IAOF

1. Barrières en interventies	2. Gegevensdeling	3. Opvolging door Politie en Openbaar Ministerie	4. Weerbaarheid van burgers en bedrijven	5. Hulp aan slachtoffers	6. Kennis en innovatie
Beschrijving					
• Partijen in de fraudeketen worden in positie gesteld om technische barrières en slimme interventies te ontwikkelen en toe te passen, gebaseerd op criminal journeys en barrièremodellen, met als doel fraude in een zo vroeg mogelijk stadium te voorkomen	• De aanpak brengt de mogelijkheden en de noodzaak van het delen van persoonsgegevens in kaart en faciliteert gezamenlijke gesprekken over oplossings-richtingen, zodat bestuurders keuzes kunnen maken ten aanzien van beleid en wetgeving	• Politie en OM informeren partners over opsporings- en vervolgingsresultaten, werken samen aan alternatieve interventies en verbeteren het aangifteproces om fraude effectiever aan te pakken	• De aanpak coördineert campagnes en initiatieven om burgers en bedrijven beter in staat te stellen fraude te herkennen en zich te weren tegen criminelen, met als doel slachtofferschap voorkomen	• Slachtoffers worden ondersteund met informatie, begeleiding en praktische hulp. Door duidelijke vuistregels en inzicht in meldpunten wordt de meldingsbereidheid vergroot	• Partners delen actuele kennis over trends, daderprofielen en werkwijzen, onderzoeken best practices en slimme samenwerkings-vormen, en brengen wetenschappelijke inzichten samen om de slagkracht van de aanpak te vergroten
Activiteiten					
• Herijking van criminal journeys en barrièremodellen • Bredere bekendheid en implementatie van interventies	• Analyse van juridische kaders inclusief EU-regelgeving • Onderzoek naar noodzaak (cross-)sectorale gegevensdeling • Onderzoek naar technologie voor gegevensdeling • Inventarisatie van oplossingsrichting voor bestuurlijke besluitvorming	• Informeren van partners op strategie op opsporing en vervolging van online criminaliteit • Inrichten van een online aangifteloket voor bedrijfsleven	• Coördineren van weerbaarheidscampagnes en activiteiten • Informeren van burgers en bedrijven	• Verbeteren van informatievoorziening richting slachtoffers • Ontwikkelen van interventie op verminderen herhaald slachtofferschap • Slachtofferhulp meer slachtoffergericht maken (eHelp)	• Creeëren van een integraal beeld van online criminaliteit • Inzicht geven in het functioneren van effectiviteit van anti-fraudecentra • Inzichten uit wetenschappelijk onderzoek naar online fraude samenbrengen

5. IAOF: aanpak, activiteiten en anti-fraudecentra
(4/17)



5.6 Introductie: analyse anti-fraudecentra langs IAOF-pijlers

In de volgende paragrafen worden de initiatieven van de vier onderzochte anti-fraudecentra geanalyseerd aan de hand van de zes pijlers van de IAOF. De opbouw is als volgt:

- Paragraaf 5.7 presenteert een overzicht waarin de anti-fraudecentra zijn gepositioneerd langs de zes pijlers;
- Paragraaf 5.8 werkt geselecteerde initiatieven verdiepend uit, met aandacht voor de beschrijving, het beoogde effect en de doelgroep.

De uitkomsten dienen te worden beschouwd als een verkenning van mogelijk interessante initiatieven, niet als een uitputtende lijst van beste werkwijzen. Genoemde werkwijzen zijn daarbij onderhevig aan veranderingen, zoals de doorontwikkeling van producten en diensten. Bij de interpretatie van dit hoofdstuk is het essentieel om de verschillende nationale contexten, wettelijke kaders en ontwerpkeuzes (zoals beschreven in hoofdstuk 4) mee te wegen.

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(5/17)

5.7 Analyse van de anti-fraudecentra langs de IAOF-pijlers

Pijler	CCB	SSUK	NASC	IKZ
1. Barrières en Interventies Fraude voorkomen door technische barrières en slimme interventies	• Belgian Anti-Phishing Shield (BAPS) • Early Warning System (EWS)-platform • Spear warnings (SW) • CyberFundamentals	• Blocked SIMs programma	• Fusion Cells • Scamwatch	• Fenomeentafels
2. Gegevensdeling Mogelijkheden en noodzaak van persoonsgegevensuitwisseling in kaart brengen en bestuurders in positie stellen voor beleidskeuzes	• NIS2-richtlijn • Early Warning System (EWS)-platform	• Amazon Web Services (AWS)-platform • Datadeling pilots	• Scams Prevention Act 2025 (SPF Act) • Scamwatch • Reportcyber • Fusion Cells • AFCX	• Wbsrz • IKZ-portaal en technische koppelingen • Samengestelde Informatieproducten (SIPs) • Casustafels
3. Opvolging door Politie en Openbaar Ministerie Opsporing en vervolging van online fraude versterken en samenwerking verbeteren	• CERT.be • CyTRIS • SafeOnWeb	• Samenwerking met de National Crime Agency (NCA)	• Joint Policing Cybercrime Coordination Centre (JPC3) • Scamwatch • Fusion Cells	• Fenomeentafels
4. Weerbaarheid van burgers en bedrijven Burgers en bedrijven beter in staat stellen fraude te herkennen en zich te weren	• CERT.be • SafeOnWeb • CyberFundamentals	• 159-lijn • BBC Scam Safe campagne	• Stop. Check. Protect. • Scams Awareness Week • Scamwatch • Little Book of Scams	• Inspiratiesessies en workshops (bedrijven) • Onderzoeksrapporten
5. Hulp aan slachtoffers Ondersteunen met informatie, begeleiding en praktische hulp, herhaald slachtofferschap voorkomen	• SafeOnWeb	• 159-lijn	• IDCARE	
6. Kennis en innovatie Actuele kennis delen, succesvolle initiatieven onderzoeken en innovatieve samenwerkingsvormen ontwikkelen	• CyTRIS en Quarterly Cyber Threat Report	• Blocked SIMs programma • Amazon Web Services (AWS)-platform	• Centrale hub functie • Scamwatch Intelligence • Targeting Scams en Fusion Cells rapporten	• Thematische onderzoeken • Samengestelde informatieproducten (SIPs) • Fenomeentafels

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(6/17) | Pijler 1: Barrières en interventies

5.8 Uitwerking initiatieven anti-fraudecentra

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	Belgian Anti-Phishing Shield (BAPS)	Een nationaal filtersysteem dat op het niveau van het internetverkeer (DNS) de toegang tot bekende malafide domeinen (zoals phishingsites en phishing-kits) proactief blokkeert voor alle gebruikers bij aangesloten providers door omleiding naar een waarschuwingspagina	• *Werking:* Het systeem verzamelt continu verdachte URL's uit meldingen van burgers (suspicious@safeonweb.be) en directe datastromen van vertrouwde partners. Deze URL's worden automatisch onderzocht in een beveiligde testomgeving (sandbox) om met zekerheid vast te stellen of ze malafide zijn. Goedgekeurde malafide domeinen worden direct aan een centrale blokkadelijst toegevoegd. Deelnemende internetproviders (ISPs) passen vervolgens DNS-sinkholing toe. Hierbij wordt het internetverkeer naar de malafide website omgeleid naar een veilige waarschuwingspagina van het CCB • *Effect:* Het Belgian Anti-Phishing Shield (BAPS) blokkeert jaarlijks circa 240 miljoen verbindingen naar malafide websites, waardoor het voor criminelen lastiger wordt om slachtoffers te bereiken. De bescherming werkt op basis van een opt-out principe zonder dat de eindgebruiker zelf iets hoeft te installeren (opt-out principe)	Eindgebruikers (als beschermde partij), Belgische ISPs (als uitvoerende partij), en een netwerk van data-leveranciers
	Early Warning System (EWS)-platform	Een platform dat dreigingsinformatie automatisch vergelijkt met de systemen van aangesloten organisaties om gerichte en direct bruikbare waarschuwingen te sturen	• *Werking:* Organisaties registreren hun externe digitale systemen (IP-reeksen, domeinen) in het EWS. Het platform legt deze lijst continu naast actuele dreigingsdata. Dit omvat technische indicatoren (IoCs), informatie over softwarekwetsbaarheden (CVE's) en beschrijvingen van aanvalsmethoden (TTPs). Het EWS-platform functioneert als een centrale vergelijkingsmotor. Het vergelijkt deze dreigingsinformatie continu met de digitale bezittingen (assets) die de aangesloten organisaties hebben geregistreerd. Bij een 'match' (bijvoorbeeld een bekende kwetsbaarheid op een server van een deelnemer) wordt automatisch een alarm gegenereerd. De getroffen organisatie ontvangt een op maat gemaakte waarschuwing met context, risico-inschatting en concrete stappen voor herstel • *Effect:* Via het EWS-platform werden in 2025 568 rapporten en 14 Flash Alerts gepubliceerd voor aangesloten organisaties. Het systeem zet algemene dreigingsinformatie om in specifieke waarschuwingen, gekoppeld aan de systemen van de ontvanger	Security-teams (SOCs) en IT-beheerders binnen organisaties die vallen onder de NIS2-richtlijn
	Spear Warnings (SW)	Een dienst die bedrijven en overheden proactief informeert over specifieke, van buitenaf zichtbare zwakheden in hun systemen	• *Werking:* Dit is een dienst die de digitale ‘buitenkant’ van de organisatie in kaart brengt. Het CCB scant publieke databronnen op misconfiguraties en gelekte data. Bij een gevalideerde vondst wordt de organisatie direct benaderd met een gedetailleerde beschrijving en een aanbeveling voor herstel • *Effect:* Spear warnings verkleinen de kans op een aanval door 'laaghangend fruit' voor aanvallers te elimineren. In 2025 werden 32.005 spear warnings verzonden. Deze waarschuwingen informeren organisaties over specifieke, geïdentificeerde kwetsbaarheden en bieden aanbevelingen voor herstel	Systeem- en netwerkbeheerders bij elke Belgische organisatie met een publiek identificeerbare zwakheid
	CyberFundamentals	Een praktisch stappenplan met beveiligingsmaatregelen, ontworpen om organisaties te helpen hun niveau van cyberbeveiliging stapsgewijs te verbeteren	• *Werking:* Dit is een praktische gids met bewezen methoden, ingedeeld naar volwassenheidsniveau (Small, Basis, Belangrijk, Essentieel). Een organisatie kan instappen op het niveau dat past bij haar omvang en risico’s • *Effect:* Het CyberFundamentals raamwerk biedt een set concrete maatregelen. De dekking tegen veelvoorkomende aanvalsvectoren is per niveau: Basic (82%), Important (94%), Essential (100%). Het fungeert als gids voor organisaties om te voldoen aan een erkende standaard van cyberbeveiliging	CISO's, IT-managers en compliance-medewerkers van allerlei typen organisaties

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(7/17) | Pijler 1: Barrières en interventies

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
SSUK	Blocked SIMs programma	Een data-uitwisselingsprogramma gericht op het verstoren van de criminele infrastructuur door UK prepaid SIM-kaarten te blokkeren die door fraudeurs worden gebruikt voor eenmalige verificatiecodes om nepaccounts aan te maken	• *Werking:* Telecomproviders identificeren verdachte of geblokkeerde simnummers en delen deze via de beveiligde cloud-omgeving van SSUK met andere sectoren, zoals techplatforms en banken. De data is zo bewerkt dat individuen niet direct herleidbaar zijn (gepseudonimiseerd). Techplatforms kunnen accounts opsporen die met deze nummers zijn aangemaakt; banken gebruiken de signalen om mogelijke fraude of mule-accounts te detecteren. Bij een gevalideerde koppeling vraagt de politie de telecomoperator om de betreffende SIM-kaart te deactiveren, waardoor de crimineel de toegang tot de gekoppelde diensten verliest • *Effect*: Het Blocked SIMs programma heeft als doel deze frauderoute duurder, risicovoller en minder schaalbaar te maken voor criminelen. Het is een van de eerste opgeschaalde pilots van SSUK	Fraudeanalyse-afdelingen bij banken en operationele teams bij telecomoperators
NASC	Fusion Cells	Tijdsgebonden, multidisciplinaire en vaak cross-sectorale projectteams die zich met een operationele focus richten op de technische en tactische ontwrichting van een specifiek type oplichting	• *Werking:* In een 'sprint' van enkele weken bundelt een team data van alle deelnemers, analyseert de infrastructuur (via o.a. on-chain analyse van cryptovaluta) en coördineert de verstoring via takedown-verzoeken en het blokkeren van accounts via directe kanalen bij platforms • *Effect*: De 'Job Scams' cell resulteerde in de verwijdering van >29.000 socialmedia accounts en de verstoring van >800 crypto-wallets. De 'Romance Scams' cell identificeerde >1.000 frauduleuze transacties	Technische specialisten (fraude-analisten, threat researchers, blockchain-experts) van de deelnemende organisaties
	Scamwatch	Het centrale meldplatform in Australië dat data van consumenten verzamelt als startpunt voor gecoördineerde verstoringsacties	• *Werking:* Burgers en organisaties melden oplichting via het Scamwatch formulier. Deze meldingen worden gecategoriseerd, geanalyseerd en gebruikt als input voor intelligence, publiekscampagnes en doorleiding naar partners. Data wordt gebruikt naast data van ReportCyber, AFCX, IDCARE en ASIC • *Effect:* Scamwatch functioneert als de primaire databron voor het nationale dreigingsbeeld. In 2025 leidde de data tot >7.500 verwijderde URLs, >7.000 verwijzingen naar Meta en het doorgeven van >4.200 unieke telefoonnummers aan telecompartners	Australische consumenten en bedrijven
IKZ	Fenomeentafels	Thematische samenwerkingen waarbij partners een specifiek fraudefenomeen analyseren en een gezamenlijk plan van aanpak opstellen	• *Werking:* Dit is primair een analyse- en ontwerpproces. Deelnemers brengen data en expertise in om een 'barrièremodel' te ontwikkelen. Hieruit kunnen voorstellen voor interventies voortkomen, gericht aan organisaties die het betreft • *Effect:* Fenomeentafels leiden tot een gezamenlijke analyse en een gecoördineerd plan van aanpak. In 2025 werden twee fenomeentafels georganiseerd over de onderwerpen diplomafraude en vergewisplicht	Partners van IKZ

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(8/17) | Pijler 2: Gegevensdeling

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	Early Warning System (EWS)-platform	Een platform dat dreigingsinformatie automatisch vergelijkt met de systemen van aangesloten organisaties om gerichte en direct bruikbare waarschuwingen te sturen	• *Werking:* Organisaties registreren hun externe digitale systemen (IP-reeksen, domeinen) in het EWS. Het platform legt deze lijst continu naast actuele dreigingsdata. Dit omvat technische indicatoren (IoCs), informatie over softwarekwetsbaarheden (CVE's) en beschrijvingen van aanvalsmethoden (TTPs). Het EWS-platform functioneert als een centrale vergelijkingsmotor. Het vergelijkt deze dreigingsinformatie continu met de digitale bezittingen (assets) die de aangesloten organisaties hebben geregistreerd. Bij een 'match' (bijvoorbeeld een bekende kwetsbaarheid op een server van een deelnemer) wordt automatisch een alarm gegenereerd. De getroffen organisatie ontvangt een op maat gemaakte waarschuwing met context, risico-inschatting en concrete stappen voor herstel • *Effect:* Via het EWS-platform werden in 2025 568 rapporten en 14 Flash Alerts gepubliceerd voor aangesloten organisaties. Het systeem zet algemene dreigingsinformatie om in specifieke waarschuwingen, gekoppeld aan de systemen van de ontvanger	Security-teams (SOCs) en IT-beheerders binnen organisaties die vallen onder de NIS2-richtlijn
	NIS2-richtlijn	Een Europese richtlijn die een wettelijk kader en een meldplicht voor cyberincidenten creëert, met als doel de algehele cyberweerbaarheid binnen de EU te verhogen en de informatiedeling te harmoniseren	• *Werking:* De richtlijn verplicht organisaties om significante incidenten binnen een vaste termijn (bv. 24 uur voor een eerste melding) te melden bij de nationale autoriteit (het CCB). Dit vereist dat organisaties interne processen en systemen hebben om incidenten te detecteren, te classificeren en te rapporteren via een gestandaardiseerd kanaal • *Effect:* De NIS2-richtlijn maakt het delen van incidentinformatie een verplichte levering. Dit droeg in 2025 bij aan een stijging van het aantal incidentmeldingen bij het CCB tot 635 (+70% t.o.v. 2024), wat leidt tot een rijker nationaal dreigingsbeeld	Organisaties van vitaal belang (OVI's): 4000+ entiteiten in 18 sectoren
SSUK	Amazon Web Services (AWS)-platform	Een centraal, door SSUK beheerd cloud-platform dat functioneert als een neutrale, technische tussenlaag om veilige data-uitwisseling (waaronder persoonlijke en niet-persoonlijke data) tussen private partijen (banken, telecom) mogelijk te maken	• *Werking:* Leden sturen hun data niet naar elkaar, maar naar dit centrale platform. Hier voert het kleine tech-team (ca. 16 medewerkers) van SSUK analyses uit. Alleen de samengevatte resultaten of specifieke alerts worden gedeeld, niet de onderliggende ruwe data van de private partij. Het AWS-platform fungeert als beveiligde cloudomgeving en technische voorziening om data gecontroleerd tussen partners uit te wisselen. • *Effect:* Het AWS-platform maakt samenwerking tussen private partijen technisch haalbaar. Het lost het vertrouwensprobleem op door een 'scheidsrechter' met een beveiligd platform te introduceren, wat de basis vormt voor alle data-pilots	Banken, telecombedrijven, platforms (aangesloten leden van Stop Scams UK)
	Datadeling pilots[1]	Een methodiek van 'start klein, bouw vertrouwen' om technische en juridische barrières voor data-uitwisseling stapsgewijs op te lossen	• *Werking:* In een afgebakende pilot wordt een specifiek data-uitwisselingsscenario getest. De pilot focust op het definiëren van de exacte data-elementen, het formaat, en de juridische (UK GDPR) en technische beveiliging van de overdracht. Data-deling vindt plaats via het AWS-platform. • *Effect:* Oplevering van een schaalbaar recept voor een specifiek type data-uitwisseling	Projectteams met data-analisten, juristen en IT-specialisten van de deelnemende pilot-partners

1) Niet alle pilots van Stop Scams UK zijn openbaar of met ons gedeeld, mede vanwege samenwerking met opsporingsinstanties of de ontwikkelingsfase van de pilots.

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(9/17) | Pijler 2: Gegevensdeling

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
NASC	Scams Prevention Act 2025 (SPF Act)	Een overkoepelende Australische wet die een juridische vrijwaring biedt en een afdwingbare plicht creëert voor het delen van data voor fraudebestrijding	• *Werking:* De wet verplicht aangewezen organisaties (banken, telecom en techbedrijven) om de technische en procesmatige capaciteit te hebben om relevante oplichtingsinformatie te delen. Het specificeert niet de techniek, maar wel de verplichting om deze te hebben • *Effect:* Boetes bij niet-naleving vanuit diverse toezichthouders (ACCC, ASIC, ACMA, AUSTRAC) kan oplopen tot AUD 50 miljoen	Banken, telecombedrijven, tech- en social media platforms
	Scamwatch	Het centrale meldplatform in Australië dat data van consumenten verzamelt als startpunt voor gecoördineerde verstoringsacties	• *Werking:* Burgers en organisaties melden oplichting via het Scamwatch formulier. Deze meldingen worden gecategoriseerd, geanalyseerd en gebruikt als input voor intelligence, publiekscampagnes en doorleiding naar partners. Data wordt gebruikt naast data van ReportCyber, AFCX, IDCARE, ASIC • *Effect: Scamwatch* functioneert als de primaire databron voor het nationale dreigingsbeeld. In 2025 leidde de data tot >7.500 verwijderde URLs, >7.000 verwijzingen naar Meta en het doorgeven van >4.200 unieke telefoonnummers aan telecompartners	Australische consumenten en bedrijven
	ReportCyber	Nationale cybercrime meldingsplatform van het Australian Cyber Security Centre (ACSC)	• *Werking:* Burgers rapporteren cybercrime bij de politie via het ReportCyber formulier. Deze meldingen worden gecategoriseerd, geanalyseerd en gebruikt voor intelligence, publiekcampagnes en doorleiding naar partners. Data wordt gebruikt naast data van Scamwatch, AFCX, IDCARE, ASIC • *Effect:* ReportCyber zorgde samen met Scamwatch voor een dataset van 481.523 meldingen (2025)	Australische burgers (via de lokale politie)
	Fusion Cells	Tijdsgebonden, multidisciplinaire en vaak cross-sectorale projectteams die zich met een operationele focus richten op de technische en tactische ontwrichting van een specifiek type oplichting	• *Werking:* Deelname door geselecteerde organisaties is op vrijwillige basis. Het proces start met een fysieke startworkshop, geleid door het NASC, waarin deelnemers gezamenlijk de projectplanning en doelstellingen vaststellen. De uitwisseling van data volgt een gestructureerd kader: deelnemers delen in principe uitsluitend niet-persoonlijk identificeerbare informatie (Non-PII), zoals frauduleuze URL's en transactiepatronen, via een beveiligd, centraal datadeelportaal dat door het NASC wordt beheerd. NASC laat deelnemende partijen aansluiten op dit datadeelportaal. • *Effect*: Een relatief hoge output in een kort tijdsbestek. De 'Job Scams' cell resulteerde in de verwijdering van >29.000 social-media accounts en de verstoring van >800 crypto-wallets. De 'Romance Scams' cell identificeerde >1.000 frauduleuze transacties	Technische specialisten (fraude-analisten, threat researchers, blockchain-experts) van de deelnemende organisaties
	AFCX	Een onafhankelijk, door de financiële sector geleid platform voor het delen van data over financiële misdrijven	• *Werking:* Banken delen data over frauduleuze transacties met het AFCX-platform. Het NASC is hierop aangesloten en kan deze data gebruiken voor zijn analyses • *Effect:* AFCX geeft het NASC directe toegang tot betrouwbare en gecontroleerde data uit de financiële sector	Fraude-analyseteams van banken en NASC

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(10/17) | Pijler 2: Gegevensdeling

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
IKZ	Wettelijke basis (Wet bevorderen samenwerking en rechtmatige zorg (Wbsrz))	De Wet bevorderen samenwerking en rechtmatige zorg (Wbsrz) is een Nederlandse wet die het IKZ een formele juridische status geeft en de uitwisseling van gegevens tussen negen specifieke zorgpartners reguleert	• *Werking:* De wet is een juridisch raamwerk, geen technisch systeem. Het stelt het IKZ formeel aan als rechtspersoon met een wettelijke taak en geeft de negen aangesloten partners (NZa, IGJ, FIOD, etc.) de juridische grondslag om (persoons)gegevens met elkaar te delen met als doel het bestrijden van zorgfraude • *Effect:* De Wbsrz formaliseert en verruimt de samenwerking die voorheen als een informele taskforce bestond. De wet verplicht partijen om signalen van zorgfraude te delen met IKZ. De wet heeft een verplichtend karakter waardoor partijen in de keten meer prioriteit geven aan het onderwerp en door IKZ kunnen worden aangesproken om hun inspanningen om zorgfraude tegen te gaan. Daarnaast biedt de wet de juridische vrijwaring die essentieel is voor partners omd ata te delen zonder privacywetgeving te schenden	Partners IKZ
	IKZ-portaal en technische koppeling	Een beveiligd platform voor het handmatig delen van signalen; technische koppelingen zijn de volgende stap naar geautomatiseerde uitwisseling	• *Werking:* Momenteel is het portaal een beveiligde webapplicatie. De ontwikkeling van technische koppelingen (API's) met systemen als de Basisregistratie Personen (BRP) moet deze handmatige stap wegnemen • *Effect:* Automatisering van de dataflow zal de snelheid en efficiëntie van het dataverrijkingsproces verhogen. Nu worden 678 signalen per jaar (2025) nog grotendeels handmatig verwerkt	Partners IKZ
	Samengestelde Informatieproducten (SIPs)	Gestructureerde informatieproducten die fraudesignalen verrijken met aanvullende bronnen	• *Werking:* Partners kunnen signalen indienen van vermoedens van zorgfraude via het IKZ-portaal. Deze signalen worden vastgelegd in een centraal systeem: Zaak Informatie Systeem (ZIS-portaal). IKZ verrijkt deze met bronnen (Handelsregister, BRP, publicaties) en met gerichte verrijkingsinformatie van partners en distribueert verrijkte signalen naar de juiste partners voor opvolging • *Effect:* In 2025 heeft IKZ 1710 SIPs verwerkt	Partners IKZ
	Casustafels	Gerichte samenwerkingsbijeenkomsten waar IKZ en partners rond één specifieke, complexe zorgfraudezaak bijeenkomen	• Werking: Voor complexe, multidisciplinaire zorgfraudezaken waar individuele signalen onvoldoende zijn voor besluitvorming, wordt een casustafel georganiseerd. Dit proces omvat het uitnodigen van relevante partners en het faciliteren van de samenwerking. De resulterende verslagen en afspraken worden gedeeld met partners • *Effect:* In 2025 heeft IKZ 11 casustafels georganiseerd	Partners IKZ

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(11/17) | Pijler 3: Opvolging door OM en Politie

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	CERT.be[1]	Het Belgische Cyber Emergency Response Team dat functioneert als de operationele incident-respons-arm van het CCB, ook wel de 'cyber-brandweer' genoemd, die technische ondersteuning levert bij actieve cyberaanvallen	• *Werking:* Op verzoek van een getroffen organisatie of de politie, kan CERT.be ter plaatse komen of indien mogelijk van afstand diensten leveren voor digitale forensische analyse (van systemen, netwerkverkeer) en het indammen en mitigeren van een aanval. De bevindingen kunnen als technisch bewijs dienen in een opsporingsonderzoek • *Effect:* In 2025 zijn er 635 incidenten geregistreerd. CERT.be heeft in 2025 103 keer noodhulp geboden	Organisaties van Vitaal belang (OVI's), politie (België)
	CyTRIS[1]	Het centrale team voor dreigingsanalyse en –informatie binnen het CCB, dat fungeert als het eerste aanspreekpunt voor incidentmeldingen	• Werking: CyTRIS analyseert de binnenkomende meldingen, correleert deze met andere informatie en kan strategische analyses leveren aan de politie over bijvoorbeeld de werkwijze van een specifieke aanvallersgroep. CyTRIS waarschuwt ook potentiële slachtoffers via Spear Warnings. Daarnaast zijn ze verantwoordelijk voor het eerste contact met organisaties die een incident melden bij het CCB • *Effect:* CyTRIS fungeert als de 'voordeur' en het 'brein' dat de ruwe incidentdata omzet in bruikbare intelligence, wat de politie kan helpen om verbanden tussen verschillende zaken te zien	Organisaties van Vitaal belang (OVI's), politie (België), overige Belgische organisaties waarvoor dreigingen worden vastgesteld
	SafeOnWeb	Primaire publiekskanaal dat burgers en bedrijven aanmoedigt om aangifte te doen en hen informeert over de juiste procedures. Daarnaast biedt SafeOnWeb ondersteunende tools voor bedrijven	• *Werking:* Organisaties kunnen via SafeOnWeb een incident melden en gebruik maken van duidelijke, bruikbare aanbevelingen om cyberveiligheid in de dagelijkse werking van hun bedrijf te integreren. Daarnaast verwijzen de website en campagnes van SafeOnWeb slachtoffers actief door naar de politie voor het doen van aangifte. Hoewel het geen directe technische koppeling is, fungeert het als een belangrijke schakel om meldingen om te zetten in officiële aangiftes • *Effect:* Door het hoge bereik (82% bekendheid) speelt SafeOnWeb een rol in het verhogen van de aangiftebereidheid onder de bevolking en bewustzijn door informatiedeling	Consumenten, bedrijven (België)
SSUK	Samenwerking met de National Crime Agency (NCA)	Het afstemmen van de inspanningen van de private sector met de prioriteiten van de nationale wetshandhaving	• *Werking:* De samenwerking is strategisch. SSUK deelt inzichten en trends uit hun data-analyses. De National Crime Agency (NCA) gebruikt deze informatie om hun eigen dreigingsbeeld en opsporingsprioriteiten aan te scherpen • *Effect:* De samenwerking met de NCA creëert een brug tussen de kennis van de industrie en de handhavingsbevoegdheid van de publieke sector	SSUK en NCA

1) CERT.be en CyTRIS zijn twee van de vier departementen van het CCB. Voor een volledige toelichting op de organisatiestructuur wordt verwezen naar pagina 51.

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(12/17) | Pijler 3: Opvolging door OM en Politie

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
NASC	Joint Policing Cybercrime Centre (JPC3)	Een door de Australische Federale Politie (AFP) geleid centrum dat een geïntegreerde samenwerking met het NASC mogelijk maakt, met als doel een directe, operationele link te creëren tussen de intelligence-hub en nationale wetshandhaving	• *Werking:* Een door de Australische Federale Politie (AFP) geleid centrum dat een geïntegreerde samenwerking met het NASC mogelijk maakt, met als doel een directe, operationele link te creëren tussen de intelligence-hub en nationale wetshandhaving • *Effect:* De integratie met JPC3 zorgt voor een extreem korte lijn van detectie naar opsporing. Een voorbeeld is het gezamenlijk waarschuwen van 130 Australiërs die doelwit waren van een specifieke oplichtingsmethode van crypto-oplichters	NASC, JPC3, AFP
	Scamwatch	Het centrale meldplatform in Australië dat data van consumenten verzamelt als startpunt voor gecoördineerde verstoringsacties	• *Werking:* Burgers en organisaties melden oplichting via het Scamwatch formulier. Deze meldingen worden gecategoriseerd, geanalyseerd en gebruikt als input voor intelligence, publiekscampagnes en doorleiding naar partners. Data wordt gebruikt naast data van ReportCyber, AFCX, IDCARE, ASIC. NASC deelt Scamwatch-data met AFP. De AFP kan real-time inlichtingen raadplegen • *Effect: Scamwatch* functioneert als de primaire databron voor het nationale dreigingsbeeld. In 2025 leidde de data tot >7.500 verwijderde URLs, >7.000 verwijzingen naar Meta en het doorgeven van >4.200 unieke telefoonnummers aan telecompartners	Australische consumenten en bedrijven
	Fusion Cells	Tijdgebonden, multidisciplinaire en vaak cross-sectorale projectteams die zich met een operationele focus richten op de technische en tactische ontwrichting van een specifiek type oplichting	• Werking: Politievertegenwoordigers (AFP) zijn actieve deelnemers in de cellen. Zij brengen niet alleen politie-informatie in, maar kunnen ook direct handelen op basis van de bevindingen. Identificeert de cel een belangrijke crimineel, dan kan de politie direct een onderzoek starten in plaats van te wachten op een eindrapport • Effect: De deelname van de politie aan Fusion Cells zorgt voor een vanzelfsprekende overgang van analyse naar actie. De cellen produceren ook "frontline response guides" die direct bruikbaar zijn voor politieagenten ‘in het veld’	NASC, AFP, overige deelnemende partijen aan de Fusion Cell
IKZ	Fenomeentafels	Thematische samenwerkingen waarbij partners een specifiek fraudefenomeen analyseren en een gezamenlijk plan van aanpak opstellen	• Werking: Deelnemers brengen data en expertise in om een barrièremodel te ontwikkelen. In 2025 zijn bijvoorbeeld fenomeentafels georganiseerd rond diplomafraude en de vergewisplicht in de zorg. In deze fenomeentafel participeert ook de politie	Partners IKZ en politie

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(13/17) | Pijler 4: Weerbaarheid van burgers en bedrijven

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	CERT.be	Het Belgische Cyber Emergency Response Team dat functioneert als de operationele incident-respons-arm van het CCB, ook wel de 'cyber-brandweer' genoemd, die technische ondersteuning levert bij actieve cyberaanvallen	• *Werking:* Op verzoek van een getroffen organisatie of de politie, kan CERT.be ter plaatse komen of indien mogelijk diensten van afstand leveren voor digitale forensische analyse (van systemen, netwerkverkeer) en het indammen en mitigeren van een aanval. De bevindingen kunnen als technisch bewijs dienen in een opsporingsonderzoek • *Effect:* In 2025 zijn er 635 incidenten geregistreerd. CERT.be heeft in 2025 103 keer noodhulp geboden	Organisaties van Vitaal belang (OVI's), politie (België)
	SafeOnWeb	Primaire publiekskanaal dat burgers en bedrijven aanmoedigt om aangifte te doen en hen informeert over de juiste procedures. Daarnaast biedt SafeOnWeb ondersteunende tools voor bedrijven, zoals een Quick Scan Rapport en een browserextensie	• *Werking:* De website en campagnes van SafeOnWeb verwijzen slachtoffers actief door naar de politie voor het doen van aangifte. Hoewel het geen directe technische koppeling is, fungeert het als een belangrijke schakel om meldingen om te zetten in officiële aangiftes • *Effect:* Door het hoge bereik (82% bekendheid) speelt SafeOnWeb een rol in het verhogen van de aangiftebereidheid onder de bevolking en bewustzijn door informatiedeling	Consumenten, bedrijven (België)
	CyberFundamentals	Een praktisch stappenplan met beveiligingsmaatregelen, ontworpen om organisaties te helpen hun niveau van cyberbeveiliging stapsgewijs te verbeteren	• *Werking:* Dit is een praktische gids met bewezen methoden, ingedeeld naar volwassenheidsniveau (Small, Basis, Belangrijk, Essentieel). Een organisatie kan instappen op het niveau dat past bij haar omvang en risico's • *Effect:* Het CyberFundamentals raamwerk biedt een set concrete maatregelen. De dekking tegen veelvoorkomende aanvalsvectoren is per niveau: Basic (82%), Important (94%), Essential (100%). Het fungeert als gids voor organisaties om te voldoen aan een erkende standaard van cyberbeveiliging	CISO's, IT-managers en compliance-medewerkers van allerlei typen organisaties
SSUK	159-lijn	Een kort, niet-spoofbaar telefoonnummer dat burgers en bedrijven kunnen bellen bij verdachte communicatie om veilig verbonden te worden met hun bank	• *Werking:* Het is een 'short code' die op netwerkniveau door telecomproviders wordt herkend en gerouteerd naar een centrale telefoondienst. De beller selecteert zijn/haar bank, waarna de oproep wordt doorgeschakeld naar een vooraf gevalideerd, niet-openbaar nummer van die bank • *Effect:* De 159-lijn fungeert als een noodrem die burgers een concrete actie geeft. De dienst verwerkt meer dan 1 miljoen oproepen per jaar en dekt >99% van de particuliere bankrekeningen	Brede publiek in het Verenigd Koninkrijk (burgers)
	BBC Scam Safe Campagne	Een brede publiekscampagne in samenwerking met de BBC ten aanzien van oplichting	• *Werking:* Dit is een mediapartnerschap. SSUK levert de inhoudelijke expertise en casuïstiek, de BBC produceert en verspreidt de content via haar TV-, radio- en online kanalen • *Effect:* De BBC Scam Safe Campagne zorgt voor een massaal bereik	Brede publiek in het Verenigd Koninkrijk (burgers)

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(14/17) | Pijler 4: Weerbaarheid van burgers en bedrijven

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
NASC	Stop. Check. Protect.	Een nationale gedragscampagne vanuit NASC, gericht op het helpen van Australiërs om oplichting te herkennen en te voorkomen. Het is een eenvoudige, concrete gedragsregel (Stop. Check. Protect) voor het publiek om een reflexmatige, veilige reactie op verdachte situaties te creëren	• *Werking:* Dit is een gedragscampagne die via diverse media (TV, radio, online) wordt verspreid. De boodschap wordt consistent herhaald zodat deze goed blijft hangen • *Effect:* De Stop. Check. Protect.-boodschap focust zich op een herhaalbare regel om de kans op gedragsverandering te vergroten. De campagne bereikte via TV al vier miljoen Australiërs	Australische burgers
	Scams Awareness Week	Een jaarlijkse, nationale themaweek die alle communicatie-inspanningen rondom het voorkomen van oplichting bundelt en versterkt	• *Werking:* Gedurende één week wordt een gecoördineerde mediacampagne gevoerd door het NASC en al zijn partners. Elk jaar heeft een specifiek thema • *Effect:* De Scams Awareness Week functioneert als een jaarlijks piekmoment dat zorgt voor maximale media-aandacht en publieke betrokkenheid. In 2025 is het bereik van de campagne geschat op 25 miljoen Australiërs, 1196 social media organisaties, en 16 actief betrokken partnerorganisaties	Australische burgers
	Scamwatch	Het centrale meldplatform in Australië dat data van consumenten verzamelt als startpunt voor gecoördineerde verstoringsacties	• *Werking:* De website van Scamwatch biedt een doorzoekbare database van bekende fraudevormen, waarschuwingen en preventietips. Het is de primaire 'self-service' kennisbank voor consumenten • *Effect:* De Scamwatch website had in 2025 6,5 miljoen bezoeken	Australische burgers en bedrijven
	Little Book of Scams	Een laagdrempelig en toegankelijk naslagwerk (fysiek en digitaal) dat basiskennis over het herkennen en voorkomen van veelvoorkomende oplichting biedt	• *Werking:* Dit is een statisch informatieproduct dat is ontworpen voor brede verspreiding, met name onder minder digitaal vaardige of kwetsbare groepen • *Effect:* In 2025 werden meer dan 158.000 fysieke exemplaren van The Little Book of Scams verspreid in 17 talen, naast ruim 10.000 downloads	Australische burgers, focus op kwetsbare consumenten en ouderen
IKZ	Inspiratiesessies en workshops (bedrijven)	Kennisdelings- en trainingsbijeenkomsten die IKZ organiseert voor partners en externe stakeholders om samenwerking te versterken	• *Werking:* 2-3 keer per jaar organiseert een accountmanager van IKZ inspiratiemiddagen voor partners en externe stakeholders, met als doel samenwerking versterken binnen de zorgketen. De sessies bieden een platform voor diepgaande discussies over een of meerdere onderwerpen, zoals de rollen en taken van partners en voorbeelden van zorgfraude cases • *Effect*: Deze sessies en workshops verhogen het kennisniveau en de alertheid binnen het professionele ecosysteem, wat indirect kan bijdragen aan betere fraudedetectie	Partners IKZ, externe stakeholders
	Onderzoeksrapporten	Het publiceren van diepgaande rapporten over specifieke zorgfraude-fenomenen om partners te informeren en hen in staat te stellen hun eigen processen en controles te verbeteren	• *Werking:* Het onderzoeksteam van het IKZ analyseert data en voert kwalitatief onderzoek uit. De bevindingen worden vastgelegd in rapporten (bv. over turboliquidaties, diplomafraude) en verspreid onder de partners • *Effect:* De onderzoeksrapporten bieden partners concrete handelingsperspectieven om misbruik beter te voorkomen, te herkennen en te bestrijden. Ze dragen bij aan de weerbaarheid van de sector als geheel	Partners IKZ

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(15/17) | Pijler 5: Hulp aan slachtoffers

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	SafeOnWeb	Primaire publiekskanaal dat burgers en bedrijven aanmoedigt om aangifte te doen en hen informeert over de juiste procedures. Daarnaast biedt SafeOnWeb ondersteunende tools voor bedrijven	• *Werking:* Via de website vinden slachtoffers een checklist met concrete, technische stappen die ze onmiddellijk moeten nemen om verdere schade te beperken (bv. apparaat loskoppelen van het netwerk, bewijsmateriaal veiligstellen, wachtwoorden wijzigen). De informatievoorziening is eenzijdig, van de website naar het slachtoffer • *Effect*: SafeOnWeb geeft slachtoffers een duidelijk en direct uitvoerbaar stappenplan. Het is een vorm van zelfhulp die is gericht op het beperken van de technische schade, niet op emotionele of financiële nazorg	Belgische burgers en bedrijven
SSUK	159-lijn	Een kort, niet-spoofbaar telefoonnummer dat burgers en bedrijven kunnen bellen bij verdachte communicatie om veilig verbonden te worden met hun bank	• *Werking:* Het is een 'short code' die op netwerkniveau door telecomproviders wordt herkend en gerouteerd naar een centrale telefoondienst. De beller selecteert zijn/haar bank, waarna de oproep wordt doorgeschakeld naar een vooraf gevalideerd, niet-openbaar nummer van die bank. De 159-lijn biedt beperkt directe slachtofferhulp. De primaire functie van de 159-lijn is preventie en niet de nazorg of de psychosociale ondersteuning. Deze functie vervult de bank • *Effect:* De 159-lijn fungeert als een noodrem die burgers een concrete actie geeft. De dienst verwerkt meer dan 1 miljoen oproepen per jaar en dekt >99% van de particuliere bankrekeningen	Brede publiek in het Verenigd Koninkrijk (burgers)
NASC	IDCARE	Australische non-profit organisatie voor slachtofferhulp, NASC verwijst slachtoffers automatisch door naar IDCARE voor emotionele en financiële ondersteuning	• *Werking:* IDCARE biedt slachtofferhulp na oplichting en cyberincidenten. Via automatische doorverwijzing vanuit NASC/Scamwatch krijgen slachtoffers gericht hersteladvies en praktische ondersteuning om verdere schade te voorkomen. IDCARE biedt ondersteuning voor: scam-slachtoffers, identiteitsdiefstal, verloren/gesloten inloggegevens, datalekken, en hackincidenten/cyberaanvallen • *Effect:* In 2025 heeft Scamwatch 8.536 slachtoffers doorverwezen naar IDCARE. Bij IDCARE zijn 47.589 rapporten in totaal binnen gekomen, met een totaal van $535,8 miljoen gerapporteerde verliezen	Australische burgers

5. IAOF: aanpak, activiteiten en anti-fraudecentra

(16/17) | Pijler 6: Kennis en Innovatie

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
CCB	CyTRIS en Quarterly Cyber Threat Report	Het centrale team voor dreigingsanalyse en –informatie binnen het CCB, dat fungeert als het eerste aanspreekpunt voor incidentmeldingen. Het CyTRIS team stelt het kwartaalrapport (Quarterly Cyber Threat Report) op	• *Werking:* CyTRIS is de analyse-eenheid die data uit alle CCB-operaties verzamelt. Voor het kwartaalrapport (Quarterly Cyber Threat Report) wordt deze data geaggregeerd, geanonimiseerd en geanalyseerd om patronen op macroniveau te identificeren. Het rapport is de gestructureerde output van dit analyseproces. Naast deze publicatie, organiseert het CyTRIS teams ook webinars en events om deelnemers te informeren over cyberdreigingen • *Effect:* Het Quarterly Cyber Threat Report biedt een overzicht van het dreigingslandschap	Organisaties van Vitaal belang (OVI's), webinars voor organisaties in het algemeen
SSUK	Blocked SIMs programma	Een data-uitwisselingsprogramma gericht op het verstoren van de criminele infrastructuur door UK prepaid SIM-kaarten te blokkeren die door fraudeurs worden gebruikt voor eenmalige verificatiecodes om nepaccounts aan te maken	• *Werking:* Telecomproviders identificeren verdachte of geblokkeerde simnummers en delen deze via de beveiligde cloud-omgeving van SSUK met andere sectoren, zoals techplatforms en banken. De data is zo bewerkt dat individuen niet direct herleidbaar zijn (gepseudonimiseerd). Techplatforms kunnen accounts opsporen die met deze nummers zijn aangemaakt; banken gebruiken de signalen om mogelijke fraude of mule-accounts te detecteren. Bij een gevalideerde koppeling vraagt de politie de telecomoperator om de betreffende SIM-kaart te deactiveren, waardoor de crimineel de toegang tot de gekoppelde diensten verliest • *Effect:* Het Blocked SIMs programma heeft als doel deze frauderoute duurder, risicovoller en minder schaalbaar te maken voor criminelen. Het is een van de eerste opgeschaalde pilots van SSUK	Fraudeanalyse-afdelingen bij banken en operationele teams bij telecomoperators
	Amazon Web Services (AWS)-platform	Een centraal, door SSUK beheerd cloud-platform dat functioneert als een neutrale, technische tussenlaag om veilige data-uitwisseling (waaronder persoonlijke en niet-persoonlijke data) tussen private partijen (banken, telecom) mogelijk te maken	• *Werking:* Leden sturen hun data niet naar elkaar, maar naar dit centrale platform. Hier voert het kleine tech-team (ca. 16 medewerkers) van SSUK analyses uit. Alleen de samengevatte resultaten of specifieke alerts worden gedeeld, niet de onderliggende ruwe data van de private partij. Het AWS-platform fungeert als beveiligde cloudomgeving en technische voorziening om data gecontroleerd tussen partners uit te wisselen. • *Effect:* Het AWS-platform maakt samenwerking tussen private partijen technisch haalbaar. Het lost het vertrouwensprobleem op door een 'scheidsrechter' met een beveiligd platform te introduceren, wat de basis vormt voor alle data-pilots	Banken, telecombedrijven, platforms (aangesloten leden van Stop Scams UK)

5. IAOF: aanpak, activiteiten en anti-fraudecentra

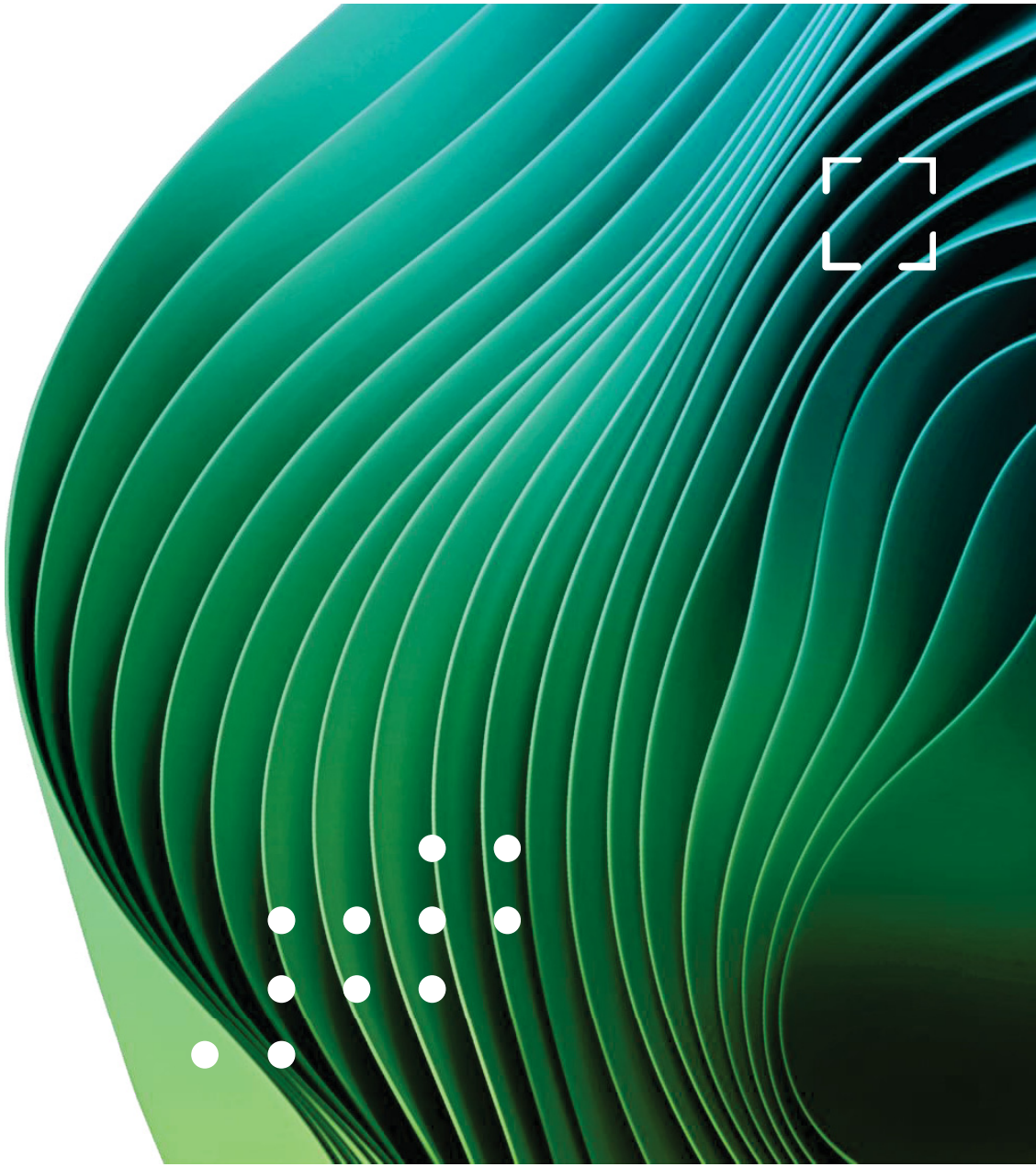
(17/17) | Pijler 6: Kennis en Innovatie

5.8 Uitwerking initiatieven anti-fraudecentra *(vervolg)*

Organisatie	Initiatief	Beschrijving		
		Beschrijving	*Werking en effect*	*Doelgroep*
NASC	Centrale hub functie	Het operationaliseren van een 'virtueel' model waarbij het NASC functioneert als het centrale zenuwstelsel voor het centraliseren van fraudedata en acties van verschillende publieke en private partners in Australië. NASC brengt daarbij de overheid, handhaving, opsporing en de private sector samen	• *Werking:* Het NASC is organisatorisch ingericht als de centrale hub waar verschillende datastromen (Scamwatch, ReportCyber, AFCX, IDCARE, etc.) samenkomen. Het is de plek waar de data wordt geanalyseerd, verrijkt en vervolgens gedistribueerd naar de juiste partij voor actie • *Effect:* De centrale hub functie zorgt voor een gecoördineerde, ecosysteembrede aanpak	Overheid, handhaving, opsporing, private partijen (Australië)
	Scamwatch Intelligence	Het centrale informatiesysteem dat de vijf primaire databronnen (Scamwatch, ReportCyber, IDCARE, AFCX en ASIC) integreert	• *Werking*: Scamwatch intelligence combineert data uit vijf bronnen: Scamwatch (consumentenmeldingen, platform van NASC), ReportCyber (cybercrime meldingen, gedeeld met politie en inlichtingendiensten), AFCX (data vanuit banken), IDCARE (informatie/casussen vanuit slachtofferhulp) en ASIC (meldingen op gebied van investeringsfraude). Technische indicatoren worden geëxtraheerd, meldingen worden geclusterd en patronen worden geïdentificeerd. Het resultaat is een dataset met 'intelligence' die bruikbaar is voor operationele partners • *Effect:* Scamwatch Intelligence is het concrete product dat wordt gedeeld met partners. Dit leidde in 2025 tot het doorgeven van bv. >4.200 telefoonnummers aan telecomproviders voor disruptie; 4 keer zo veel als in 2024	Overheid, handhaving, opsporing, private partijen (Australië)
	Targeting Scams en Fusion Cells rapporten	Het publiceren en delen van rapportages om strategische kennis en operationele lessen te delen met een breed publiek	• Werking: Het NASC analyseert de geaggregeerde data over een heel jaar voor het jaarlijkse 'Targeting Scams' rapport. Daarnaast worden na afloop van elke Fusion Cell specifieke eindrapporten geschreven met de bevindingen en resultaten • Effect: De rapporten maken de omvang, trends en resultaten van de fraudebestrijding inzichtelijk. De publicaties worden gebruikt voor beleidsvorming, publieke verantwoording en internationale kennisdeling	Overheid, handhaving, opsporing, private partijen (Australië) en overige geïnteresseerden
IKZ	Thematische onderzoeken	Het uitvoeren van diepgaand, kwalitatief onderzoek naar specifieke zorgfraude-fenomenen om de werkwijze en onderliggende oorzaken te begrijpen	• *Werking:* Het onderzoeksteam van het IKZ verzamelt data, houdt interviews en analyseert casuïstiek rondom een thema (bv. misbruik van turboliquidaties). De output is een publiek rapport met een gedetailleerde analyse en aanbevelingen • *Effect:* Thematische onderzoeken bieden partners en beleidsmakers een diepgaand inzicht in complexe fraudevormen, wat kan leiden tot aanpassingen in wetgeving of toezicht	Partners IKZ
	Samengestelde Informatieproducten (SIPs)	Gestructureerde informatieproducten die fraudesignalen verrijken met aanvullende bronnen	• *Werking:* Partners kunnen signalen indienen van vermoedens van zorgfraude via het IKZ-portaal. Deze signalen worden vastgelegd in een centraal systeem: Zaak Informatie Systeem (ZIS-portaal). IKZ verrijkt deze met bronnen (Handelsregister, BRP, publicaties) en distribueert verrijkte signalen naar de juiste partners voor opvolging • *Effect:* In 2025 heeft IKZ 1710 SIPs verwerkt	Partners IKZ
	Fenomeentafels	Thematische samenwerkingen waarbij partners een specifiek fraudefenomeen analyseren en een gezamenlijk plan van aanpak opstellen	• *Werking:* Dit is primair een analyse- en ontwerpproces. Deelnemers brengen data en expertise in om een 'barrièremodel' te ontwikkelen. Hieruit kunnen voorstellen voor interventies voortkomen, gericht aan organisaties die het betreft • *Effect:* Fenomeentafels leiden tot een gezamenlijke analyse en een gecoördineerd plan van aanpak. In 2025 werden 11 van deze tafels georganiseerd	Partners IKZ

Bijlagen

I. Factsheet
II. Begrippenlijst
III. Bronnenlijst



I. Factsheet

(1/13)

Inleiding

Het onderstaande factsheet vat de belangrijkste kenmerken van de vier onderzochte anti-fraudecentra samen. De opbouw volgt het vergelijkende analysekader, met een onderwerpvolgorde die aansluit bij de opdrachtomschrijving. Voor een gedetailleerde analyse van de werking, effecten en doelgroep wordt verwezen naar hoofdstuk 5. Specifieke termen worden gedefinieerd in *Bijlage II. Begrippenlijst*.

	CCB	SSUK	NASC	IKZ
Doel	• Beschermen van de aanbieders van essentiële diensten of organisaties van vitaal belang (OVI's), burgers en bedrijven tegen toenemende cyberdreigingen door middel van een gecoördineerde, geïntegreerde nationale aanpak	• Stoppen van oplichting bij de bron door een cross-sectorale samenwerking te bevorderen tussen banken, technologie-bedrijven en telecommunicatie-aanbieders	• Beschermen van burgers en bedrijven tegen steeds geavanceerdere oplichting door de samenwerking tussen de overheid en het bedrijfsleven te versterken	• Voorkomen en het aanpakken van misbruik van zorggelden en zorgcriminaliteit in Nederland
Strategie	• Vergroten van het bewustzijn ten aanzien van fraude (o.a. via SafeOnWeb) • Opsporen en verstoren van criminele infrastructuur (o.a. via Belgian Anti-Phishing Shield - BAPS) • Signaleren van dreigingen via monitoring en gerichte waarschuwingen (o.a. via Early Warning System (EWS) en Spear Warnings) • Versterken van cyberweerbaarheid (o.a. via CyberFundamentals) • Coördineren van beleid voor een betrouwbare digitale omgeving	• Bevorderen van de cross-sectorale samenwerking en datadeling (Amazon Web Services (AWS)-platform en datadeling overeenkomsten) • Beschermen van slachtoffers aan de hand van directe interventies (o.a. via 159-lijn) • Uitoefenen van invloed op publieke bewustwording door actieve betrokkenheid bij nationaal beleid op het gebied van fraude	• Bevorderen van publiek-private samenwerking en het uitoefenen van invloed op de formulering van technische maatregelen • Verhogen van publieke bewustwording en het vereenvoudigen van meldingen met campagnes en nieuwe tools • Bieden van directe slachtofferondersteuning om herstel te bevorderen	• Centraliseren, verrijken en doorgeleiden van fraudesignalen naar partners voor effectieve opvolging • Analyseren van trends en datastromen om opkomende fraudefenomenen en structurele risico's vroegtijdig te identificeren • Organiseren van multi-disciplinaire samenwerking via thematische platforms om kennis te delen en gezamelijke barrièremodellen te ontwikkelen
Kerntaken	• Coördineren van het nationaal cyberbeleid • Creëeren van bewustwording bij burgers en bedrijven • Verrichten van incidentrespons (CERT.be) • Uitvoeren van dreigingsanalyses (CyTRIS) • Vervullen van de rol als Nationale Cyber Certificerings Autoriteit (NCCA) en Nationaal Coördinatie Centrum (NCC-BE)	• Faciliteren van cross-sectorale samenwerking door middel van operationele pilots (159-lijn, Blocked SIMs programma) • Testen en implementeren van fraude-interventies • Coördineren van campagnes en partnerschappen	• Faciliteren van cross-sectorale samenwerking en samenwerking tussen overheid en bedrijfsleven • Informeren en beschermen van het publiek door middel van campagnes (Stop. Check. Protect, Scams Week) • Verwijzen van melders naar gespecialiseerde hulpdiensten (IDCARE) • Bieden van hulp en ondersteuning bij de afwikkeling van een fraude-incident (melder, hulpverlener)	• Centraliseren en gericht delen van fraudesignalen naar partners • Faciliteren van de operationele aanpak op casusniveau • Analyseren van trends en statistieken • Bevorderen van kennisdeling over de aanpak van fraude binnen het zorgdomein

I. Factsheet

(2/13)

	CCB	SSUK	NASC	IKZ
Taken en producten	• CCB produceert jaarverslagen, Quarterly Cyber Threat Reports en technische adviezen • Daarnaast levert CCB tools en raamwerken, waaronder het SafeOnWeb-platform (incidentenmeldpunt voor burgers en bedrijven), het Early Warnings Systeem (EWS) en het CyberFundamentals raamwerk • Ook levert CCB direct hulp bij incidentenherstel (via CERT.be), forensische ondersteuning en de coördinatie bij nationale cybercrises • Oprichting van de Belgian Anti-Fraud Coordination Board 1.5 jaar geleden om initiatieven rond online fraude strategisch te coördineren en informatie te delen	• SSUK beheert de 159-lijn • Daarnaast beheert SSUK een datadeling platform (op AWS) wat de veilige uitwisseling van data tussen leden faciliteert • Ook ontwikkelt en test SSUK nieuwe oplossingen via kleinschalige projecten (bijv. het Blocked SIMs programma) • Tot slot publiceert SSUK strategische rapporten en onderzoek om beleid en praktijk te informeren (rapporten zoals The Future of Fraud en onderzoek in samenwerking met instituten zoals RUSI)	• NASC publiceert jaarlijks het Targeting Scams Report, de Fusion Cells rapporten en The Little Book of Scams • Daarnaast beheert NASC het Scamwatch platform • Ook coördineert NASC de publiekscampagnes en verstoringsactiviteiten	• IKZ stelt Samengestelde Informatieproducten (SIPs) op om fraudesignalen te verrijken • IKZ publiceert thematische onderzoeken (bijvoorbeeld over turboliquidaties, diplomafraude) • IKZ organiseert fenomeentafels, casustafels en inspiratiesessies om samenwerking en kennisdeling over de aanpak van fraude in de zorg te faciliteren
Invulling maatschappelijke behoefte	• Invulling vanuit CCB is het bewaken, coördineren en versterken van de nationale cyberweerbaarheid, met de ambitie om België tot de minst kwetsbare landen van Europa te maken • Maatschappelijk effect (2025): ➢ 635 incidenten geregistreerd vanuit CCB (+70% t.o.v. 2024), o.a. door NIS2-richtlijn en verbeterde detectiemogelijkheden; ➢ SafeOnWeb verwerkte 10 miljoen verdachte e-mails; ➢ 82% van de Belgische bevolking heeft aangegeven SafeOnWeb te kennen	• 2025: Fraude meest voorkomende misdrijf in Engeland en Wales (41%); veroorzaakt 1,2 miljard economische schade en ernstig psychologische gevolgen (70% van de slachtoffers heeft aangegeven mentale schade te ervaren) • SSUK verzorgt praktijkgerichte interventies, veilige datadeling, en gerichte samenwerking met beleidsmakers • De ledenorganisatie van aangesloten private partijen dekt meer dan 99% van de particuliere bankrekeningen, 100% van de mobiele netwerkoperatoren en de meeste grote tech-platforms in het Verenigd Koninkrijk	• 2025: Australische bevolking verliest 2,18 miljard AUD aan oplichting (+7,8% t.o.v. 2024) • NASC speelt in op kernbehoefte in het voorkomen en beperken van financiële en emotionele schade door oplichting, beschermen van kwetsbare groepen, snelle hulp aan slachtoffers en herstel van vertrouwen in systemen	• IKZ heeft tot taak bij te dragen aan het versterken van de integriteit van de zorgsector door het ontvangen, analyseren en doorgeleiden van signalen over mogelijke fraude en misbruik van zorggelden • 2025: 678 signalen ontvangen (139% meer t.o.v. 2024 – 200 signalen)

I. Factsheet

(3/13)

	CCB	SSUK	NASC	IKZ
Doel op (online)fraudepreventie en –bestrijding	• Preventief aanpakken van online fraude door gebruikers om te leiden naar een waarschuwingspagina bij bezoek aan malafide websites (Belgian Anti-Phishing Shield - BAPS), bewustwording te creëeren (SafeOnWeb • Detecteren van cyberfraude via o.a. EWS en Spear Warnings (kwetsbare systemen) en online fraude via SafeOnWeb (meldingen) • Specifiek op cyberfraude: respons bieden op gedetecteerde cyberaanvallen door de inzet van het Emergency Response Team (CERT.be) en preventive door cybersecuritykaders zoals CyberFundamentals beschikbaar te stellen	• Preventief aanpakken van fraude door de cross-sectorale samenwerking verder te stimuleren • Detecteren van fraude via real-time identificatie van fraudeurs en patronen via datadeling (Blocked SIMs programma, AWS data platform) • Respons te bieden op gedetecteerde fraude door actieve scamtrajecten te onderbreken door de inzet van de 159-lijn	• Preventief aanpakken van fraude door de cross-sectorale samenwerking verder te stimuleren (Fusion Cells) en bewustwording te creëren via campagnes • Detecteren van fraude via real-time identificatie van fraudeurs en patronen te delen met banken (AFCX) en burgers en organisaties (Scamwatch) • Respons te bieden op gedetecteerde fraude door signalen te delen met banken (AFCX) en burgers en bedrijven (Scamwatch), meldkanalen aan te bieden (ReportCyber) en slachtofferondersteuning te bieden (IDCARE)	• Signaleren en communiceren ten aanzien van potentiële zorgfraude naar partners • Faciliteren van de samenwerking tussen partners
Aansluiting organisatie bij nationale context - ecosysteem van samenwerkingsverbanden	• CCB vervult de rol als nationale coördinatieautoriteit die de implementatie van EU-regels (o.a. NIS2) bewaakt en nationale cyberinitiatieven aanstuurt	• SSUK vervult de rol als facilitator die private banken, telecommunicatie-aanbieders en technologie-bedrijven bij elkaar brengt	• NASC vervult de rol als facilitator die publieke en private partijen samenbrengt. NASC centraliseert meld- en operationele data om trends te detecteren, oplichting vroegtijdig te verstoren en gerichte acties te coördineren	• IKZ vervult de rol van facilitator die de partners[1] – op verzoek – samenbrengt en fenomeentafels en inspiratiesessies met de partners en andere betrokken instanties, zoals DUO of de politie, organiseert
Ontvangen en registreren van meldingen van burgers en bedrijven	• CCB maakt gebruik van het nationale meldpunt SafeOnWeb (suspicious@safeonweb.be), dat beschikbaar is in vier talen en waar burgers en bedrijven verdachte fraude-incidenten rondom phishing (malafide berichten, mails en domeinen) kunnen melden • Cyberincidenten worden gemeld bij CERT.be en vereisen meer technische context • Verdachte berichten worden automatisch geanalyseerd, geregistreerd en waar nodig actie op ondernomen, zoals het BAPS (blokkering van toegang naar frauduleuze websites), Spear Warnings, of manuele escalatie uitgevoerd door een CyTRIS analist	• SSUK maakt gebruik van een 159-lijn: een kort, niet spoofbaar telefoonnummer dat burgers en bedrijven kunnen bellen bij verdachte communicatie om veilig verbonden te worden met hun bank	• NASC maakt gebruik van meerdere meldkanalen, o.a.: ReportCyber (een nationaal cybermeldpunt voor burgers) en Scamwatch (meldpunt waar burgers en bedrijven een melding kunnen doen van oplichting) • Beide platforms leggen de gegevens vast, classificeren deze en delen actiegerichte intelligence met NASC via beveiligde kanalen	• Burgers kunnen een melding doen over een ‘vermoeden van zorgfraude’ bij de NZa, gemeente of zorgverzekeraar • De partners beoordelen de meldingen van burgers en bedrijven. Indien zij een aanleiding zien tot een vermoeden van zorgfraude, dienen zij hierover een signaal in bij IKZ • Burgers kunnen geen rechtstreekse melding doen bij IKZ • 2025: 678 signalen vanuit partners (2024: 200 signalen)

1) Partners: Nederlandse Zorgautoriteit (Nza), Inspectie Gezondheidszorg en Jeugd (IGJ), Belastingdienst, FIOD, Centrum Indicatiestelling Zorg (CIZ), Sociale Verzekeringsbank (SVB), Nederlandse Arbeidsinspectie (NLA), Gemeenten (VNG), Zorgverzekeraars en zorgkantoren (ZN)

I. Factsheet

(4/13)

	CCB	SSUK	NASC	IKZ
Informatiedeling met burgers	• CCB waarschuwt en informeert burgers via SafeOnWeb (site, app, browserextentie), social media en publieke campagnes (EU Cybersecurity Month, themacampagnes rond feestdagen)	• SSUK informeert burgers via bewustwordingcampagnes (BBC Scam Week, BBC Scam Safe), hun website en social media	• NASC informeert burgers via brede publiekscampagnes (Stop. Check. Protect) en via hun website, social media, radio en gidsen • Daarnaast investeert NASC in openbare fraudedata en dashboards (o.a. in Scamwatch), zodat burgers, bedrijven en toezichthouders in staat worden gesteld om trends zelf te analyseren	• IKZ is niet gericht op informatiedeling met burgers. Informatiedeling vindt plaats via de partners • Er vindt indirect informatiedeling plaats via publicatie van jaarrapporten, onderzoeksrapporten en fenomeenanalyses
Informatiedeling met partners in de fraudeketen	• Het CCB werkt binnen BAPS met vertrouwde partners. Deze partners kunnen vastgestelde malafide domeinnamen rechtstreeks in het BAPS-systeem invoeren. Belgische internetproviders kunnen die domeinen vervolgens op nationaal DNS-niveau omleiden naar een waarschuwingspagina. • Het CCB werkt met opsporingspartners via PhishNemo, een detectietool die door de Federale Gerechtelijke Politie is ontwikkeld en later door het CCB is overgenomen. In het Nationaal Protocol voor Detectie en Disruptie van Phishingdreigingen werkt het CCB samen met de federale politie en Secutec om phishingwebsites en -toolkits sneller te detecteren en verstoren.	• SSUK faciliteert informatiedeling niet als een centrale datahub, maar als een neutrale bemiddelaar die de voorwaarden voor samenwerking creëert. Via kleinschalige datadeling pilots onderzoekt SSUK eerst praktische, culturele en regulatie barrières, waarna succesvolle inzichten worden opgeschaald. De aanpak rust op twee pijlers: ➢ SSUK werkt actief samen met partners om te onderzoeken hoe data – met name afkomstig uit de 159-lijn – veilig en doelgericht kan worden gedeeld met partijen in de fraudeketen. In pilotprogramma's delen leden bijvoorbeeld data met elkaar om beter te begrijpen welke data beschikbaar is; ➢ Door expliciete steun en erkenning te verkrijgen van cruciale toezichthouders (zoals Ofcom, de FCA en ICO), biedt SSUK haar leden het vertrouwen dat deelname aan data-uitwisseling binnen een goedgekeurd kader plaatsvindt. Daarnaast heeft SSUK meer dan 40 datadelingsovereenkomsten opgezet en vindt datadeling plaats via een beveiligd AWS-platform	• NASC fungeert als centraal knooppunt: het verzamelt en analyseert meldingen van verschillende bronnen (bijv. AFCX, ReportCyber, Scamwatch) en deelt via beveiligde kanalen gerichte, uitvoerbare intelligence met platforms, banken, telecomproviders en opsporingsinstanties	• Algemene samenwerking met partners (Nederlandse Zorgautoriteit (Nza), Inspectie Gezondheidszorg en Jeugd (IGJ), Belastingdienst, FIOD, Centrum Indicatiestelling Zorg (CIZ), Sociale Verzekeringsbank (SVB), Nederlandse Arbeidsinspectie (NLA), Gemeenten, Zorgverzekeraars en zorgkantoren • Samenwerking met politie op bepaalde fenomeenonderzoeken (zoals valse diploma's)

I. Factsheet

(5/13)

	CCB	SSUK	NASC	IKZ
Verwerking van persoonsgegevens	• CCB verwerkt persoonsgegevens alleen waar nodig voor wettelijke taken of verplichtingen van algemeen belang, monitoring, waarschuwingen, incidentrespons, certificering en contactmomenten. Het gaat vooral om identificatie-, contact-, organisatie-, werkgerelateerde en technische gegevens • CCB verwerkt geen persoonsgegevens specifiek voor fraudebestrijding, waar nodig worden gegevens gedeeld met dienstverleners of bevoegde overheden	• SSUK focust in pilotprojecten op het classificeren van bepaalde (telecom)data als Niet-Persoonlijke Informatie, wat een snellere en minder privacy-gevoelige gegevensuitwisseling mogelijk maakt. Alle data wordt opgeslagen op een beveiligde infrastructuur en uitsluitend met partners gedeeld indien dit strikt noodzakelijk is voor het realiseren van het vastgestelde doel	• De Scams Prevention Framework 2025 (SPF Act) staat toe dat gegevens uit één onderzoek mogen worden gebruikt voor andere relevante zaken, dat gegevens kunnen worden ingezet voor geaggregeerde trendanalyses en dat persoonsgegevens mogen worden gedeeld met een afgebakende kring van partners, waaronder andere toezichthouders, opsporingsdiensten, betrokken bedrijven en internationale instanties • Verwerking van persoonsgegevens valt onder het privacyregime van ACCC, die de Australische privacyprincipes volgt	• IKZ ontvangt signalen van partners en verrijkt deze met gegevens uit drie bronnen: ➢ Handelsregister; ➢ Dashboard Zicht op Zorgaanbieders; ➢ Basisregistratie Personen (BRP). • Verrijking vindt eveneens plaats met gegevens van partners, die zij op verzoek van IKZ moeten leveren. Dit is voor IKZ de voornaamste vorm van verrijking. In Wbsrz is vermeld welke partner welke informatie moet leveren • Verwerking vindt plaats op basis van een wettelijke taak (art. 6 lid 1 sub c AVG) • De gegevens worden gebruikt voor twee doelen: signaalverrijking (bewaartermijn 5 jaar) en strategische analyse (bewaartermijn 10 jaar) • Verrijkte signalen worden gedeeld met aangesloten partners voor opvolging. De rechten van betrokkenen (AVG) zijn van toepassing
Ondersteuning en samenwerking partners	• Als lid van het Coördinatiecomité voor Inlichtingen en Veiligheid (CCIV) werkt het CCB nauw samen met Belgische inlichtingen-, veiligheids-, en politiediensten op gebied van het veiligheidsbeleid • Het CCB heeft met nationale partners, waaronder het Nationaal Crisiscentrum (NCCN), een cybernoodplan opgesteld. Dit plan verdeelt taken en verantwoordelijkheden bij nationale cyberincidenten en –crises en is ter goedkeuring voorgelegd aan het CCIV. • Als Nationaal Coördinatiecentrum (NCC-BE) binnen het EU-netwerk bevordert het CCB innovatie en de opbouw van cybersecurity-capaciteit, coördinatie van cybersecurity-investeringen en ondersteunt het bij het verkrijgen van EU-financiering, in samenwerking met Europese en nationale partners uit de academische en private sector	• SSUK biedt een neutrale ruimte waar leden (uit financiële, telecom- en techsector) veilig problemen kunnen delen en gezamenlijke projecten kunnen ontwikkelen • SSUK initieert en coördineert cross-sectorale pilotprogramma's die gericht zijn op het verstoren van oplichting (waaronder het Blocked SIMs programma) • SSUK heeft een eigen, veilig datadelingsplatform op Amazon Web Services (AWS) ontwikkeld en schaalt dit op om grote hoeveelheden data snel en veilig met partners te wisselen. Of het om persoonsgegevens of niet-persoonsgegevens gaat, wordt bepaald door datadelingsovereenkomsten tussen de betrokken partners.	• Samenwerking en ondersteuning van partners wordt door NASC vormgegeven via Fusion Cells: tijdsgebonden, publiek-private taskforces die een breed scala aan experts (industrie, overheid, opsporing en maatschappelijke organisaties) bijeenbrengen om een specifiek, hardnekkig oplichtingstype aan te pakken • Samenwerking omvat directe verstoring (zoals het verwijderen van 29.000+ accounts en 800+ crypto-wallets bij vacaturefraude) als het ontwikkelen van structurele oplossingen	• IKZ organiseert thematische bijeenkomsten waar relevante partners samenwerken om een specifiek, complex fraudefenomeen te analyseren en een gezamenlijke aanpak te ontwikkelen • IKZ fungeert als operationeel knooppunt door signalen te bundelen, te verrijken en gericht te delen. Voor complexe zaken vindt afstemming plaats in casustafels

I. Factsheet

(6/13)

	CCB	SSUK	NASC	IKZ
Ondersteuning van slachtoffers	• CCB verleent zelf geen psychosociale of financiële slachtofferzorg, maar biedt wel technische (CERT.be) en coördinerende (SafeOnWeb) ondersteuning na een incidentmelding • CERT.be biedt ondersteuning aan organisaties van vital belang (OVI's) en administratieve overheden. SafeOnWeb biedt ondersteuning aan bedrijven, overheden en burgers. De focus ligt op het adviseren over directe acties om schade te beperken en het aanmoedigen van aangifte	• SSUK biedt zelf geen directe slachtofferondersteuning • De ondersteuning is indirect en wordt primair gefaciliteerd via de 159-lijn, die slachtoffers direct en veilig doorverbindt met de fraude-afdeling van hun eigen bank	• NASC faciliteert snelle, gerichte slachtofferhulp door automatische doorverwijzing van Scamwatch naar specialistische instantie (IDCARE)	• Slachtofferhulp is geen taak van IKZ. Deze wordt evenmin verzorgd door de negen partners, aangezien zij vooral gericht zijn op het voorkomen, stoppen en straffen van fraude in de zorg. Bovendien zijn gemeenten, zorgverzekeraars en zorgkantoren veelal zelf slachtoffer van de gepleegde frauds in de zorg
Preventie-activiteiten	• CCB biedt organisaties die onder NIS2 als vitaal zijn aangewezen toegang tot het Early Warning System (EWS)-portaal. Hier kunnen organisaties relevante CTI-informatie aanleveren. CCB-analisten verrijken deze data met informatie van partners en sturen actiegerichte waarschuwingen uit (Spear Warnings) over o.a. kwetsbare systemen. Daarnaast biedt het portaal rapporten, alerts, en inzicht in het strategische beveiligingsniveau en kwetsbaarheden • Het actief op zoek gaan naar kwetsbaarheden en dreigingen gericht op specifieke Belgische organisaties, zoals gelekte inloggegevens • Voor specifieke dreigingen, zoals DDoS-aanvallen, heeft het CCB procedures zoals de 'red-button procedure' ontwikkeld. Dit omvat geautomatiseerde, real-time monitoring en een snelle, gecoördineerde respons in samenwerking met internet service providers en hostingproviders om aanvallen te mitigeren	• SSUK richt zich op het direct onschadelijk maken van de middelen van oplichters, door het op grote schaal blokkeren van van schadelijke domeinen (>50.000 tot nu toe) en het uitvoeren van operationele takedowns van websites, accounts en advertenties • Daarnaast ontwikkelt SSUK geavanceerde detectiemechanismen om oplichting tijdens de uitvoering te signaleren. Dit omvat het monitoren van 'remote access'-software (zoals TeamViewer en AnyDesk), de inzet van stembiometrie voor verificatie en het gebruik van machine-learning-modellen voor geautomatiseerde detectie	• NASC richt zich op het direct onschadelijk maken van de middelen van oplichters. Dit omvat het offline halen van websites, verwijderen van advertenties, delen van verdachte bankgegevens met financiële partners en doorgeven van telefoonnummers voor blokkering • In samenwerking met telecombedrijven worden systeembrede maatregelen genomen, zoals het blokkeren van oplichtingsverkeer op netwerkniveau en het tegengaan van 'spoofing' Daarnaast worden nieuwe barrières geïmplementeerd, zoals betaalvertragingen en waarschuwingen bij transacties • Via doorlopende voorlichtingscampagnes informeert NASC consumenten over hoe zij oplichting kunnen herkennen en welk beschermend gedrag zij kunnen vertonen om te voorkomen dat zij slachtoffer worden	• Verrijken, analyseren en doorgeleiden van signalen van verschillende partners om nieuwe fraudepatronen in een vroeg stadium te kunnen herkennen • Uitvoeren van onderzoek naar specifieke fraudefenomenen en het continu monitoren van nieuwe trends. Vanuit deze onderzoeken biedt IKZ partners handelingsperspectieven voor het voorkomen, detecteren of aanpakken van fraude in de zorg • Organiseren van actieve kennisuitwisseling via thematische fenomeentafels en inspiratiesessies

I. Factsheet
(7/13)

	CCB	SSUK	NASC	IKZ
Overige activiteiten	• Coördineren van de Belgische aanpak en vertegenwoordigen van het land in diverse EU-netwerken en internationale fora (o.a. NIS Cooperation Group) en vertegenwoordiging in Europese bestuursraden (o.a. ENISA raad, ENISA Liasions Office en EU-CyCLONe) • Aanbieden van het CyberFundamentals raamwerk om organisaties te helpen hun digitale bescherming te verbeteren • Samenwerken met de academische en private sector aan opleidingen en ondersteunen van initiatieven (zoals de Cyber Security Challenge) om nieuw talent aan te trekken	• Bijdragen aan de *UK Fraud Strategy 2026-2029* om de cross-sectorale discussie over de toekomst van fraudebestrijding te stimuleren • Produceren en publiceren van strategisch onderzoek (bijv. over AI en fraude), casestudies en rapporten om beleid en praktijk te informeren • Deelname aan internationale fora zoals de Global Fraud Summit om kennis uit te wisselen	• Publicatie van jaarlijkse trendrapporten en gedetailleerde verslagen van Fusion Cell-operaties • Delen van inzichten en praktijkvoorbeelden door actieve deelname aan mondiale platforms zoals de Global Anti-Scam Summit en de International Consumer Protection and Enforcement Network (ICPEN) • Geven van anti-scam workshops aan internationale partners, met een focus op de Associatie van Zuidoost-Aziatische Naties (de ASEAN-regio) • Ondersteunen van wereldwijde samenwerking via een actieve rol in de adviesraad van de Global Anti-Scam Alliance (GASA)	• Actieve deelname aan het Fieldlab Ondermijning in de Zorg voor de ontwikkeling van nieuwe, multi-disciplinaire interventies • Deelname aan het European Healthcare Fraud and Corruption Network (EHFCN) om praktijkvoorbeelden uit te wisselen en expertise op dit gebied vanuit Nederland te delen
Effectiviteit organisatie in buitenland	• Actieve rol in EU-, NAVO- en VN-fora om beleid af te stemmen en een gecoördineerde respons te organiseren • Uitvoeren van internationale projecten (bijv. in Senegal) om expertise en kennis te delen • De door het CCB ontwikkelde modellen (Active Cyber Protection (ACP), CyberFundamentals, Belgian Anti-Phishing Shield - BAPS) worden erkend als praktijkvoorbeelden en zijn overgenomen door andere landen • Bevestiging van de effectiviteit door een top-10-positie in de National Cybersecurity Index (NSCI) en een ‘Tier-1 rolmodel’ status in de International Telecommunication Union (ITU) Global Cybersecurity Index (GCI)	• Uitwisselen van kennis op internationale fora en delen van praktijkvoorbeelden van operationele modellen en pilots	• Actieve deelname aan mondiale fora zoals de Global Anti-Scam Summit en ICPEN om inzichten te delen • Geven van workshops aan internationale partners, zoals de ASEAN-lidstaten, om hun anti-scam capaciteiten te versterken • Onderhouden van sterke banden met sleutelpartners via lidmaatschap van de International Fraud Council (met o.a. Britse instanties)	• De internationale effectiviteit van IKZ richt zich op strategische kennisuitwisseling via actieve deelname aan het EHFCN • Het doel is het uitwisselen van succesvolle initiatieven en het opdoen van nieuwe inzichten om de nationale aanpak van zorgfraude te versterken

I. Factsheet

(8/13)

	CCB	SSUK	NASC	IKZ
Effectiviteit organisatie in binnenland	• Geautomatiseerde preventie: ➢ Belgian Anti-Phishing Shield (BAPS): Voorkomt jaarlijks ~240 miljoen bezoeken aan frauduleuze websites; ➢ SafeOnWeb: Verwerkte in 2025 bijna 10 miljoen verdachte e-mails • Proactieve waarschuwingen: ➢ 32.005 gerichte 'spear-waarschuwingen' verzonden in 2025 (+42%); ➢ Tienduizenden waarschuwingen per jaar via het Early Warning System (EWS) • Publieksbereik en -betrokkenheid: ➢ 82% van de bevolking kent SafeOnWeb; ➢ 44% van de Belgen heeft de dienst ooit gebruikt om een melding te doen • Incidentherstel: ➢ 635 incidenten gemeld en behandeld in 2025 (+70%); ➢ 103 organisaties ondersteund, inclusief forensische hulp	• Bereik van de 159-lijn: >1 miljoen oproepen verwerkt; dekt >99% van de Britse betaalrekeningen • Leden dekken samen o.a. >95% van online zoekopdrachten en 90% van privé e-mailaccounts • Winnaar van de PAY360 Award for Best Financial Crime Prevention Initiative, geprezen om de cross-sectorale samenwerking en het innovatieve data-gebruik • De National Crime Agency erkent SSUK als een sleutelinnovator in data-uitwisseling om criminaliteit te voorkomen	• Verstoring: ➢ >7.500 scam-URLS verwijderd (+30% t.o.v. 2024); ➢ 4x meer telefoonnummers doorverwezen naar telecompartners voor blokkering (4.246); ➢ Handhaving door ACMA resulteerde in >AUD 4 miljoen aan boetes voor telecombedrijven • Publieksbereik (2025): ➢ Scamwatch-site bezocht door 6.5 miljoen mensen; ➢ TV-campagnes bereikten circa 4 miljoen Australiërs • Slachtofferhulp: ➢ 8.536 melders doorverwezen naar de gespecialiseerde hulpdienst IDCARE; ➢ ~2.700 slachtoffers direct benaderd voor advies en ondersteuning	• In 2023 werden 338 signalen 696 keer gedeeld met partners • Aantal verwerkte signalen steeg van ~200 in 2024 naar 678 in 2025 door de wettelijke verplichting en gerichte voorlichting • Producten en output uit jaarverslag (2025): ➢ 372 unieke, verrijkte SIPs (1710 SIP-records in totaal); ➢ 678 signalen verwerkt (2024: ~200 signalen). Stijging door wettelijke verplichting en gerichte voorlichting; ➢ 11 casustafels afgerond; ➢ Gemiddeld 3 onderzoeksrapporten per jaar; ➢ Fenomeentafels organiseren. Voorbeelden: diplomafraude in de zorg, omgang met de vergewisplicht
Factoren die bijdragen aan effectiviteit organisatie	• Proactieve, geautomatiseerde en op maat gemaakte aanpak (ACP) • Samenwerkingsverbanden met 100+ internetproviders en internationale partners • Massale bewustwording doordat 600+ organisaties nauw aangesloten zijn bij de verspreiding van de jaarlijks terugkerende campagne in oktober	• Tri-sector governance met gebalanceerde vertegenwoordiging • Flexibel lidmaatschapsmodel dat deelname laagdrempelig maakt • C-suite betrokkenheid en mandaten • Publieke zichtbaarheid van SSUK-leden creëert een strategisch draagvlak	• Een ecosysteembrede aanpak die publieke en private partijen structureel (via het Joint Policing Cybercrime Coordination Centre (JPC3) met de politie) en flexibel (via Fusion Cells) samenbrengt • Formele partnerschappen en een wettelijk kader zorgen voor een betrouwbare uitwisseling van bruikbare 'intelligence' • Juridische zekerheid bij private partijen versterkt een betrouwbare en proactieve uitwisseling van data	• IKZ bundelt en verrijkt signalen van negen partners die elkaar kunnen aanvullen vanuit hun eigen kennis en expertise • IKZ faciliteert fenomeentafels om, naast de casuïstiek, ook opkomende fraudefenomenen in de zorg gezamenlijk te analyseren

I. Factsheet
(9/13)

	CCB	SSUK	NASC	IKZ
Factoren die effectiviteit organisatie afzwakken	• Talent-schaarste • Regelgevingsuitdagingen (NIS2-complexiteit, fragmentatie tussen sectoren en vrije invulling van regels binnen lidstaten)	• Er is geen wet die systematische, sector-overstijgende informatiedeling verplicht, wat leidt tot juridische onduidelijkheid en een gebrek aan standaardisatie • Het vrijwillige karakter kan leiden tot een onvolledige dekking en inconsistente deelname aan projecten, waardoor een volledig ecosysteem-breed beeld uitblijft • Zowel de Britse AVG als technische en operationele beperkingen (zoals een gebrek aan standaarden) vormen een barrière voor snelle, grootschalige gegevensuitwisseling	• Consumenten zijn overweldigd door tegenstrijdige adviezen en hebben behoefte aan heldere, consistente richtlijnen vanuit de overheid om zichzelf effectief te beschermen	• De effectiviteit wordt ondermijnd doordat handhavingspartners (zoals de NLA en OM) over beperkte capaciteit beschikken voor het strafrechtelijk vervolgen van de plegers van fraude in de zorg • Een aantal organisaties dat wel over waardevolle informatie beschikt (politie, Kamer van Koophandel), is nog geen partner van het IKZ • De mogelijkheden voor IKZ om zelf informatie te toetsen of verzamelen is zeer beperkt • Het IT-systeem voor signaalverwerking is nog niet optimaal ingericht, wat een efficiënte verwerking van signalen belemmert
Structuur	• CCB is een federale overheidsinstantie onder de bevoegdheid van de Eerste Minister • CCB heeft vier departementen met elk hun eigen operationaliteit en taken: NCCA (cybercertificering), CERT.be (incidentenrespons), CyTRIS (dreigingsanalyse) en NCC-BE (ecosysteem-verbinder) • Teams worden ondersteund door centrale managementsdiensten en specifieke klantgerichte SafeOnWeb-teams	• SSUK is een door de private sector geleide ledenorganisatie die bedrijven uit de financiële, technologie- en telecomsector verenigt • De organisatie wordt geleid door een compact leiderschapsteam van vijf personen • SSUK ontvangt pro bono juridische ondersteuning van advocatenkantoor Mishcon de Reya LLP • De governance wordt gewaarborgd door een adviesraad van negen leden, gelijk verdeeld over de drie aangesloten sectoren (3 leden per sector)	• NASC heeft de structuur van een virtueel centrum, gepositioneerd als een operationeel knooppunt binnen de ACCC (de Australische mededingings- en consumentenautoriteit). Het functioneert niet als een zelfstandige entiteit, maar als een coördinerend netwerk dat een systeem-brede respons op oplichting organiseert • De governance wordt gewaarborgd door een adviesraad (Advisory Board) bestaande uit 12 leden. Deze raad weerspiegelt de ecosysteem-brede aanpak en omvat senior vertegenwoordigers uit de belangrijkste sectoren: financiën, rechtshandhaving, digitale platforms, telecom, slachtofferhulp en consumentenbelangen	• De Raad van Bestuur is eindverantwoordelijk, met de dagelijkse leiding in handen van een directeur • De organisatie is opgebouwd uit twee kernteams: Onderzoek & Analyse en Casuïstiek, ondersteund door staff-functies

I. Factsheet

(10/13)

	CCB	SSUK	NASC	IKZ
Type organisatie (publiek, privaat, combinatie)	• CCB is een publieke, federale overheidinstelling, opgericht bij Koninklijk Besluit • CCB staat onder de directe bevoegdheid van de Eerste Minister	• SSUK is een private non-profit en industrie-geleide lidmaatschaporganisatie zonder overheidsfinanciering. SSUK bestaat uit +-40 leden vanuit de banken, telecommunicatie en technologiesector	• NASC is een publieke organisatie binnen een overheidsinstantie (ACCC), dat zijn taken uitvoert in nauwe operationele samenwerking met private partners (banken, telecom, socialmediaplatforms)	• IKZ is een onafhankelijke, privaatrechtelijke organisatie in de vorm van een Stichting met een Wettelijke Taak (Rechtspersoon met een Wettelijke Taak - RWT) • Deze juridische status, vastgelegd in de Wet bevorderen samenwerking en rechtmatige zorg, geeft de organisatie een formeel mandaat om haar specifieke taken uit te voeren • Als RWT is de stichting een zelfstandige rechtspersoon, ingeschreven bij de Kamer van Koophandel
Inrichting afdelingen	• Daarnaast beschikt CCB over vier departementen primair gericht op cybersecurity diensten: 1) NCCA (voor certificering en standaarden), 2) NCC-BE (voor coördinatie cybersecurity-investeringen, innovatie stimulatie, ondersteuning van organisaties bij EU-financiering), en de operationele afdelingen: 3) CERT.be (voor technische expertise en bijstand bij cyberaanvallen), 4) CyTRIS (als contactpunt bij incidentmeldingen, verzenden van waarschuwingen en uitvoeren van analyses). Daarnaast: SafeOnWeb (voor publieke bewustwording) en Capacity Building (voor talentontwikkeling) • Daarnaast zijn er nog ondersteunende teams, waaronder HR en Financiën	• SSUK beschikt over een leiderschapsteam van vijf personen dat de strategische domeinen dekt (voorzitter, algemeen directeur, en directeuren voor beleid, product en operaties) • Daarnaast heeft SSUK een groeiend team van technische analisten en data-engineers dat zich richt op het bouwen en opschalen van de pilots en het dataplatform	• NASC is ingericht met drie thematische werkgroepen: ➢ Data Integration & Technology: verantwoordelijk voor de technische infrastructuur en het faciliteren van data-uitwisseling ➢ Emerging Trends & Responses: monitort dreigingen, analyseert patronen en ontwerpt operationele reacties (incl. Fusion Cells) ➢ Communications & Awareness: leidt publiekcampagnes en stakeholdermanagement	• Bestuur: Raad van Bestuur en directeur • Staf: ondersteunende functies voor o.a. HR, Financiën en Communicatie • Operationele units: ➢ Onderzoek & Analyse: focust op strategische analyse, trends en thematische onderzoeken; ➢ Casuïstiek: beheert de operationele 'workflow' van fraudemeldingen
Wijze van bemensing (allocatie)	• Totaal: 135 fte (2026), die verdeeld zijn over: • CERT.be • CyTRIS • NNCA • NCC-BE • SafeOnWeb • Capacity Building • Ondersteunende diensten (HR en Financiën)	• SSUK beschikt over een vast en 5-koppig leiderschapsteam en een gespecialiseerd tech-team van 16 personen • Het merendeel van het operationele werk wordt uitgevoerd door de technische experts van de lidbedrijven zelf • Het interne team van SSUK fungeert als coördinator en facilitator	• De dagelijkse, operationele staff wordt geleverd door de moederorganisatie ACCC: 31 fte in operationele teams van NASC (datadeling; intelligence; verstoring; fusion cells; educatie en outreach). Dit is exclusief personeel dat werk doet op gebied van IT, strategische communicatie en handhaving • Experts van partnerorganisaties (banken, tech, politie) worden tijdelijk samengebracht in Fusion Cells • De adviesraad en stuurgroepen bestaan uit externe vertegenwoordigers die toezicht en advies geven, maar niet tot de operationele staff behoren	• Totaal: 16,5 fte (eind 2025) • Wijze van bemensing: ➢ Raad van Bestuur: 0,44 fte; ➢ Directeur: 0,94 fte; ➢ Staf: 4,45 fte; ➢ Team Onderzoek & Analyse: 3 fte; ➢ Team Casuïstiek: 7,67 fte

I. Factsheet
(11/13)

	CCB	SSUK	NASC	IKZ
Juridische grondslag	• CCB is een federale overheidsinstelling dat is opgericht bij Koninklijk Besluit, direct onder de bevoegdheid van de Eerste Minister • De operationele taken en bevoegdheden zijn primair vastgelegd in de EU NIS2-richtlijn • CCB functioneert als de officieel aangewezen nationale coördinatie-autoriteit en nationaal CSIRT	• SSUK is een private rechtspersoon (‘company limited by guarantee’) • SSUK functioneert op basis van een vrijwillige lidmaatschapsovereenkomst tussen private partijen • SSUK opereert niet onder een wettelijk mandaat	• NASC is een coördinerend centrum binnen een bestaande federale overheidsinstantie (ACCC) • De SPF Act legt de specifieke rollen en verantwoordelijkheden voor toezichthouders vast. Het framework is flexibel ingericht zodat verplichtingen kunnen worden aangepast aan veranderende frauderisico’s	• IKZ is een Rechtspersoon (Stichting) met een Wettelijke Taak (RWT) door de inwerktreding van de Wet bevorderen samenwerking en rechtmatige zorg (Wbsrz) • Deze wet is op 1 januari 2025 in werking getreden
Juridische bevoegdheden	• CCB is bevoegd om toezicht te houden op de naleving van beveiligingseisen bij meer dan 4.000 entiteiten in 18 sectoren (NIS2-verplichtingen) • Daarnaast heeft het CCB bevoegdheden onder de Cyber Solidarity Act, Cyber Resilience Act en Cybersecurity Act • Ook is het CCB bevoegd om incidenten te analyseren, technische bijstand te verlenen en de gecoördineerde bekendmaking van kwetsbaarheden (CVD) te bemiddelen • Bovendien is het CCB bevoegd om richtlijnen en aanbevelingen uit te vaardigen en praktische instrumenten (zoals het CyberFundamentals raamwerk) aan te bieden ter ondersteuning van de naleving	• SSUK heeft geen wettelijk mandaat of handhavingsmacht om datadeling af te dwingen • SSUK opereert binnen de grenzen van bestaande wetten (zoals de Britse AVG) en het toezicht van verschillende regulatoren, zonder eigen wettelijke basis • Deelname en datadeling door leden is gebaseerd op vrijwilligheid, niet op een wettelijke plicht	• De SPF Act verplicht aangewezen sectoren (banken, telcoms, platforms) tot het delen van intelligence en het rapporteren van incidenten • De ACCC kan de naleving afdwingen met boetes die kunnen oplopen tot AUD 50 miljoen • De ACCC handhaaft de SPF Act en houdt toezicht op digitale platforms, de Australian Securities and Investments Commission (ASIC) houdt toezicht op de financiële sector en de Australian Communications and Media Authority (ACMA) op de telecomsector	• Partners zijn onder de Wbsrz wettelijk verplicht om vermoedens van zorgfraude te melden aan IKZ • De Wbsrz biedt de juridische basis die de uitwisseling van signalen en persoonsgegevens tussen partijen mogelijk maakt • IKZ heeft de wettelijke taak om data te bundelen, te verrijken en te delen
Relaties met overheid	• Het CCB werkt operationeel samen met de FOD economie om te testen hoe malafide online advertenties sneller offline gezet kunnen worden • Daarnaast heeft het CCB een strategische samenwerking via formele overlegplatforms (zoals het Coördinatiecomité CCIV) met veiligheids- en inlichtingendiensten, politie en Defensie	• SSUK werkt in lijn met de nationale Fraudestrategie en onderhoudt nauwe banden met partners zoals het National Cyber Security Centre (NCSC), de Financial Conduct Authority (FCA), de Information Commissioner’s Office (ICO) en de National Crime Agency (NCA)	• NASC is onderdeel van de ACCC • Daarnaast heeft NASC nauwe banden met sectorspecifieke toezichthouders zoals de Australian Securities and Investments Commission (ASIC – financiële sector), Australian Communications and Media Authority (ACMA – telecom), Australian Transaction Reports and Analysis Centre (AUSTRAC – anti-witwassen) • Bovendien heeft de NASC een operationele samenwerking met de Politie (AFP) via het JPC3	• Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) functioneert als de directe opdrachtgever en financierder voor IKZ • Daarnaast fungeert de Nederlandse Zorgautoriteit (NZa) als het landelijke meldpunt voor zorgfraude en daarmee als één van de hoofdleveranciers van signalen aan het IKZ • IKZ is tevens lid van de Taskforce Integriteit Zorg (TIZ)

I. Factsheet

(12/13)

	CCB	SSUK	NASC	IKZ
Relaties met banken	• CCB werkt samen met de sectorfederatie Febelfin binnen de BAC-board (Belgian Anti-Fraud Coordination Board) waarvan CCB de voorzitter is. Deze board coördineert de nationale aanpak van online fraude in België en stemt de opzet van het nationale antifraudeplan af met publieke en private partijen. • Het CCB werkt samen met individuele banken en toezichthouders, waaronder de Financial Services and Markets Authority (FSMA), om als 'trusted partners' informatie uit te wisselen voor het Belgian Anti-Phishing Shield (BAPS) • Daarnaast voorziet het CCB banken via het Early Warning Systeem (EWS) van gerichte cyberdreigingsinformatie en waarschuwingen, en biedt het ondersteuning bij de naleving van de NIS2-richtlijn	• SSUK heeft relaties met bijna alle UK retail-banken (99.7% van alle banken, 26 banken totaal), waaronder: Visa, Revolut, NatWest, Lloyds, HSBC • Banken participeren actief in datadeling, 159-lijn en in diverse pilots zoals het Blocked SIMs programma	• Banken leveren transactiedata en verdachte rekeninginformatie (o.a. via het AFCX-kanaal) en ontvangen in ruil daarvoor geanalyseerde 'intelligence' van NASC • Banken voeren concrete verstoringsacties uit, zoals het blokkeren van rekeningen en betalingen, en nemen deel aan 'Fusion Cells' om nieuwe tegenmaatregelen te ontwikkelen • Banken dragen bij aan slachtofferhulp door het coördineren van herstelacties na een oplichting	• IKZ heeft momenteel geen relaties met banken
Relaties met socialmediaplatforms	• Social media platforms, zoals Meta, worden gebruikt als distributiekanaal om met preventiecampagnes een groot publiek te bereiken. Een campagne tegen beleggingsfraude bereikte via Facebook en Instagram >446.000 mensen en leidde tot 36.754 klikken naar SafeOnWeb.be • Het CCB werkt samen met grote techbedrijven zoals Google en Microsoft voor het uitwisselen van technische data, bijvoorbeeld over malware	• Grote techplatforms zoals Meta, Google en Microsoft zijn volwaardige, betalende leden van SSUK • De platforms nemen direct deel aan de kernactivteiten van SSUK, waaronder datadelingsprojecten en gezamenlijke scam detectie-initiatieven	• NASC werkt samen met DIGI en rechtstreeks met enkele platforms die deelnemen aan fora en fusion cells. Platforms hanteren een vrijwillige gedragscode, beheerd door brancheorganisatie Digital Industry Group Inc. (DIGI) en ondertekend door grote platforms zoals Meta, Google, Apple, Snap, TikTok, Twitch, X en Yahoo • De code bevordert gezamenlijke acties op het gebied van gebied van 'takedowns', het verbeteren van meldmechanismen en het implementeren van waarborgen voor advertenties • De code bevat ook afspraken over het delen van 'intelligence' en de samenwerking met rechtshandhavingsinstanties	• IKZ heeft momenteel geen relaties met social media platforms
Relaties met klanten	• CCB heeft contact met burgers via SafeOnWeb@Home voor bewustwording, preventie en meldingen • Via SafeOnWeb@Work heeft CCB contact met bedrijven voor specifieke richtlijnen en tools • Via het Early Warning Systeem (EWS) biedt CCB diepgaande ondersteuning aan vitale organisaties (OVI's) en biedt CCB via CERT.be directe incidentrespons • Daarnaast onderhoudt CCB relaties met de academische wereld en Europese netwerken voor advies, onderzoek en internationale coördinatie	• De primaire relatie verloopt via de 159-dienst als direct contactpunt in geval van (vermoedelijke) oplichting. Daarnaast via publiekscampagnes, zoals de samenwerking met de BBC (Scam Safe) • SSUK biedt een "vertrouwde ruimte" en de middelen voor leden om problemen te delen, kansen te identificeren en gezamenlijke projecten te leiden	• Het NASC heeft toegang tot meldingen via meerdere kanalen, waaronder ReportCyber als nationaal cybermeldpunt voor burgers, Scamwatch als meldpunt waar burgers en bedrijven oplichting kunnen rapporteren, en relevante systemen zoals AUSTRAC voor financiële en transactiegerelateerde signalen • Daarnaast benadert NASC slachtoffers direct voor advies en informeert NASC het publiek via campagnes	• Burgers kunnen niet bij IKZ terecht met vermoedens van fraude in de zorg. Meldingen lopen via de aangesloten partners (zoals NZa, gemeenten of zorgverzekeraars) • De relatie met het publiek is indirect, voornamelijk via de publicatie van (geanonimiseerde) rapporten en factsheets

I. Factsheet
(13/13)

	CCB	SSUK	NASC	IKZ
Kostenopbouw (begroting)	• Totale begroting: €36.000.000 (2025) • Het jaarlijkse budget is gegroeid van circa €15 miljoen (2020) naar €36 miljoen (2025) • Een gedetailleerde, openbare begroting van CCB is niet beschikbaar	• Een gedetailleerde, openbare begroting van SSUK is niet beschikbaar	• Een gedetailleerde, openbare begroting van NASC is niet beschikbaar	• Totale begroting: €3.991.464 (2025, goedgekeurd door het ministerie van Volksgezondheid, Sport en Welzijn – VWS) • Kostenopbouw 2025 is terug te vinden op pagina 8 van het openbare jaarverslag, via: https://www.ikz.nl/wp-content/uploads/2026/03/2025-133-IKZ-jaarverslag_07.pdf
Wijze van financiering	• CCB wordt volledig gefinancieerd door de Belgische federale overheid	• SSUK wordt gefinancieerd door jaarlijkse abbonnementsgelden van leden, variërend van £20k tot £120k per lid, afhankelijk van de organisatiegrootte • Aanvullende financiering vindt plaats via donaties en sponsoring voor specifieke projecten • Gedetailleerde budgetcijfers zijn niet openbaar	• NASC wordt gefinancieerd door de Australische overheid via de ACCC • NASC heeft bij oprichting AUD 58 miljoen ontvangen voor een 3-jarig programma om de organisatie op te zetten: AUD 44 miljoen is bestemd voor de technologie-infrastructuur en real-time datadeling. AUD 14 miljoen is bestemd voor operationele capaciteit (waaronder de Fusion Cells, communicatie en doorlopende analyses) • De overheid heeft de financiering van het NASC met één jaar verlengd voor 2026-2027. hiervoor is AUD 12,7 miljoen beschikbaar gesteld aan de ACCC om de activiteiten van NASC voort te zetten	• IKZ wordt primair gefinancieerd via een jaarlijkse toekenning van financiële bijdrage van het ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Mate van afdwingbaarheid vanuit organisatie	• CCB is bevoegd om toezicht te houden op de naleving van de NIS2-richtlijn, inclusief het uitvoeren van inspecties en controles • CCB is daarbij ook bevoegd om toezicht te houden op de certificering van producten en diensten onder de EU Cybersecurity Act • Voor opsporing en vervolging is CCB afhankelijk van de politie en justitie	• Er is geen wet die systematische, sector-overstijgende informatiedeling verplicht of eenduidig faciliteert • De afdwinging is gebaseerd op de formele toezegging van de leden zelf, niet op wettelijke sancties	• De SPF Act legt verplichtingen op aan banken, platforms en telecombedrijven. Niet naleving kan worden bestraft met boetes die oplopen tot AUD 50 miljoen • Concrete verplichtingen die uit het SPF Act volgen zijn een gedocumenteerde anti-scam strategie, verplichte informatiedeling en versterkte consumentenbescherming	• Partners zijn in het kader van de Wbsrz wettelijk verplicht om vermoedens van zorgfraude te melden aan IKZ • IKZ's rol is beperkt tot het verzamelen, verrijken en doorgeven van informatie om de effectiviteit van de bevoegde handhavingspartners te vergroten • IKZ heeft zelf geen handhavings-, toezicht- of opsporingsbevoegdheden • Daadwerkelijke opvolging en afdwinging is afhankelijk van de capaciteit en prioritering van partners in de keten

II. Begrippenlijst

(1/5)

Begrip	Definitie
159-lijn	Een kort, niet-spoofbaar telefoonnummer dat burgers en bedrijven in het Verenigd Koninkrijk kunnen bellen bij verdachte communicatie van banken om veilig verbonden te worden met hun bank
ACP (Active Cyber Protection)	Een proactieve, op maat gemaakte, geautomatiseerde en participatieve aanpak; het centrale raamwerk van het CCB die proactieve detectie en gerichte respons combineert
ACCC (Australian Competition & Consumer Commission)	De Australische mededingings- en consumentenautoriteit, de overheidsinstantie waaronder het NASC is gepositioneerd
ACMA (Australian Communications and Media Authority)	De Australische toezichthouder voor communicatie- en mediadiensten
AFCX (Australian Financial Crimes Exchange)	Een onafhankelijk, door de financiële industrie geleid platform voor het delen van data over financiële misdrijven in Australië
Amazon Web Services (AWS)-platform	Een centraal, door SSUK beheerd cloud-platform dat functioneert als een neutrale, technische tussenlaag om veilige data-uitwisseling tussen private partijen (banken, telecom, tech) mogelijk te maken
ASIC (Australian Securities and Investments Commission)	Australische toezichthouder voor financiële dienstverlening en financiële markten
BBC Scam Safe Campagne	Een brede publiekscampagne in het Verenigd Koninkrijk, in samenwerking met de BBC, gericht op het verhogen van de weerbaarheid van burgers tegen oplichting
Belgian Anti-Phishing Shield (BAPS)	Een nationaal filtersysteem dat op het niveau van het internetverkeer (DNS) de toegang tot bekende malafide domeinen (zoals phishingsites en phishing-kits) proactief blokkeert voor alle gebruikers bij aangesloten providers door omleiding naar een waarschuwingspagina (opt-out principe)
Blocked SIMs programma	Een data-uitwisselingsprogramma van SSUK tussen telecom, banken en techbedrijven gericht op het verstoren van de criminele infrastructuur door prepaid SIM-kaarten van Britse telecombedrijven te blokkeren die door fraudeurs worden gebruikt voor eenmalige verificatiecodes om nepaccounts aan te maken
Casustafels	Gerichte samenwerkingsbijeenkomsten waar IKZ en partners rond één specifieke, complexe zorgfraudezaak bijeenkomen

II. Begrippenlijst

(2/5)

Begrip	Definitie
CCB (Centre for Cybersecurity Belgium)	De Belgische federale autoriteit, opgericht in 2014, met als doel het bewaken, coördineren en versterken van de nationale cyberweerbaarheid. Het CCB speelt een centrale rol in de implementatie van EU-regelgeving zoals de NIS2-richtlijn
CCIV (Coördinatiecomité voor Inlichtingen en Veiligheid)	Belgisch overleg- en coördinatieorgaan waar het CCB als permanent lid samenwerkt met inlichtingen-, veiligheids-, en politiediensten op strategisch niveau over het nationale veiligheidsbeeld
CERT.be	Het Belgische Cyber Emergency Response Team dat functioneert als de operationele incident-respons-arm van het CCB, ook wel de 'cyber-brandweer' genoemd, die technische ondersteuning levert bij actieve cyberaanvallen
CyberFundamentals	Een praktisch stappenplan met beveiligingsmaatregelen opgesplitst in volwassenheidsniveau , ontworpen door het CCB, om organisaties te helpen hun niveau van cyberbeveiliging stapsgewijs te verbeteren
CyTRIS (Cyber Threat Research & Intelligence Sharing)	Het centrale team voor dreigingsanalyse en –informatie binnen het CCB, dat fungeert als het eerste aanspreekpunt voor incidentmeldingen en strategische analyses levert
Datadeling pilots (SSUK)	Een methodiek van 'start klein, bouw vertrouwen' om technische en juridische barrières voor data-uitwisseling stapsgewijs op te lossen in afgebakende projecten
Early Warning System (EWS)-platform	Een platform van het CCB dat dreigingsinformatie automatisch vergelijkt met de systemen van aangesloten organisaties om gerichte en directe waarschuwingen te sturen
Fenomeentafels	Thematische samenwerkingen georganiseerd door het IKZ waarbij partners een specifiek fraudefenomeen analyseren en een gezamenlijk plan van aanpak (barrièremodel) opstellen
Fusion Cells	Tijdsgebonden, multidisciplinaire en vaak cross-sectorale projectteams van het NASC die zich met een operationele focus richten op de technische en tactische ontwrichting van een specifiek type oplichting
IAOF (Integrale Aanpak tegen Online Fraude)	Een samenwerkingsverband van publieke en private partijen in Nederland, gestart in 2022, met als doel het aantal slachtoffers en de maatschappelijke schade van online fraude terug te dringen door sneller en gerichter op te treden in de gehele fraudeketen
IDCARE	Een Australische non-profit organisatie voor slachtofferhulp, waar het NASC slachtoffers automatisch naar doorverwijst voor emotionele en financiële ondersteuning na oplichting en cyberincidenten

II. Begrippenlijst

(3/5)

Begrip	Definitie
IKZ (Stichting Informatieknooppunt Zorgfraude)	Een Nederlandse onafhankelijke, privaatrechtelijke stichting, opgericht in 2025, om signalen over vermoedens van zorgfraude te bundelen, te verrijken en door te leiden naar partners, met als doel misbruik van zorggelden te voorkomen en aan te pakken
Inspiratiesessies en workshops (IKZ)	Kennisdelings- en trainingsbijeenkomsten die het IKZ organiseert voor partners en externe stakeholders om de verbinding tussen uitvoering, beleid en bestuur te versterken
Ministerie van JenV	Afkorting voor het Ministerie van Justitie en Veiligheid
Joint Policing Cybercrime Centre (JPC3)	Een door de Australische Federale Politie (AFP) geleid centrum dat een geïntegreerde samenwerking met het NASC mogelijk maakt, met als doel een directe, operationele link te creëren tussen de intelligence-hub en nationale wetshandhaving
Little Book of Scams	Een laagdrempelig naslagwerk (fysiek en digitaal) van het NASC dat basiskennis biedt over het herkennen en voorkomen van veelvoorkomende oplichting, met name gericht op minder digitaal vaardige of kwetsbare groepen
NASC (National Anti-Scam Centre)	Een Australisch publiek knooppunt, ingesteld in 2023 onder de ACCC, met als doel de samenwerking tussen overheid, opsporing en private partijen te versterken en gecoördineerde acties tegen oplichting te organiseren
NCCA (National Cybersecurity Certification Authority)	Een nationale autoriteit verantwoordelijk voor de uitvoering en handhaving van het nationale certificeringsschema voor cybersecurity. NCCA controleert naleving en kan indien nodig optreden om de naleving van regelgeving te garanderen
NCCN (Nationaal Crisiscentrum)	Belgische nationaal crisiscentrum dat de algemene noodplanning en crisisbeheer coördineert en overheden en hulpdiensten ondersteunt via permanente 24/7-waakzaamheid
NIS2-richtlijn (Network and Information Security Directive)	Een Europese richtlijn die een wettelijk kader en een meldplicht voor cyberincidenten creëert, met als doel de algehele cyberweerbaarheid binnen de EU te verhogen en de informatiedeling te harmoniseren
Organisaties van Vitaal Belang (OVI's)	Cruciale sectoren voor de veiligheid van de Belgische bevolking: de energie-, mobiliteits-, telecom-, en financiële sectoren, drinkwater, volksgezondheid en de overheid
PSR (Payment Service Regulation)	Een (EU-)kader voor digitale veiligheid dat eisen stelt aan detectie en gegevensdeling

II. Begrippenlijst

(4/5)

Begrip	Definitie
PhishNemo	Een detectietool ontwikkeld binnen de Federale Gerechtelijke Politie (FGP), overgenomen door het CCB. CCB werkt binnen dit project samen met de FGP en Secutec (private beveiligingspartner) om phishingwebsites en phishingtoolkits sneller te detecteren en te verstoren
Samengestelde Informatieproducten (SIPs)	Gestructureerde informatieproducten van IKZ die fraudesignalen, ingediend door partners, verrijken met aanvullende gegevens uit drie bronnen: het Handelsregister, het dashboard Zicht op Zorgaanbieders, en het BRP en met gegevens van partners die zij op verzoek van IKZ moeten leveren
Remote Access Detectie	Een pilot van SSUK om banken te waarschuwen wanneer een klant mogelijk slachtoffer is van 'hulp-op-afstandfraude', door te signaleren of software als AnyDesk of TeamViewer actief is tijdens een online banksessie
ReportCyber	Het nationale cybercrime meldingsplatform van het Australian Cyber Security Centre (ASCC), waar Australische burgers cybercriminaliteit kunnen rapporteren bij de politie
RWT (Rechtspersoon met een Wettelijke Taak)	Een juridische status die een organisatie een formeel mandaat geeft om specifieke wettelijke taken uit te voeren. Het IKZ is een voorbeeld van een RWT
SafeOnWeb	Het primaire publiekskanaal van het CCB in België, bestaande uit een website, app en campagnes, dat burgers en bedrijven informeert over cyberveiligheid, hen aanmoedigt aangifte te doen en ondersteuning biedt na een incident
Scams Awareness Week	Een jaarlijkse, nationale themaweek in Australië, gecoördineerd door het NASC, die alle communicatie-inspanningen rondom het voorkomen van oplichting bundelt en versterkt
Scams Prevention Act 2025 (SPF Act)	Een overkoepelende Australische wet die een juridische vrijwaring biedt en een afdwingbare plicht creëert voor het delen van data voor fraudebestrijding door aangewezen sectoren (banken, telecom, platforms)
Scamwatch	Het centrale meldplatform in Australië, beheerd door het NASC, dat data van consumenten over oplichting verzamelt als startpunt voor gecoördineerde verstoringsacties, publiekscampagnes en intelligence-ontwikkeling
Spear Warnings (SW)	Een dienst van het CCB die organisaties proactief informeert over specifieke, van buitenaf zichtbare zwakheden in hun systemen, zoals misconfiguraties of gelekte data

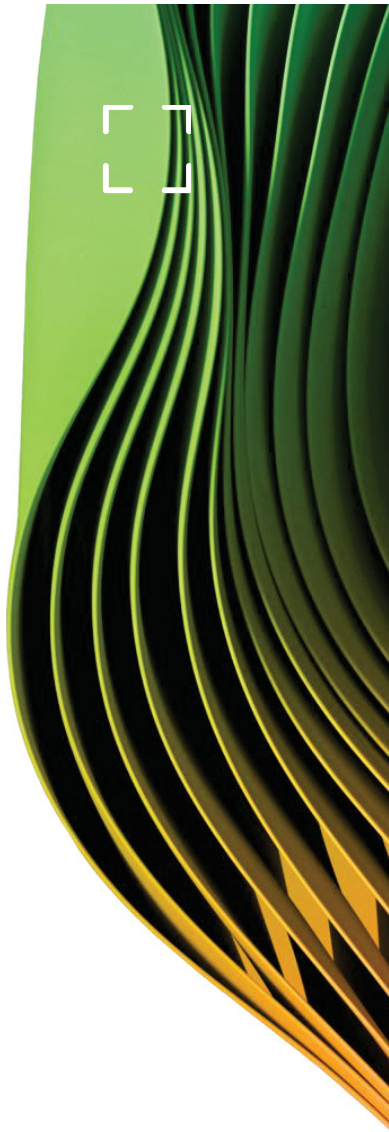
II. Begrippenlijst

(5/5)

Begrip	Definitie
SSUK (Stop Scams UK)	Een private, door de industrie geleide ledenorganisatie (non-profit) in het Verenigd Koninkrijk, opgericht in 2020, met als doel oplichting bij de bron te stoppen door samenwerking tussen banken, technologiebedrijven en telecomaanbieders te bevorderen
Stop. Check. Protect.	Een nationale gedragscampagne van het NASC in Australië, gericht op het creëren van een eenvoudige, reflexmatige en veilige reactie bij het publiek op verdachte situaties
TIZ (Taskforce Integriteit Zorgsector)	Een samenwerkingsverband dat op basis van een convenant met afspraken over rollen, informatie-uitwisseling en gezamenlijke werkwijzen ter versterking van de integriteit van de zorgsector
URL-blokkering (SSUK)	Een samenwerkingsverband gecoördineerd door SSUK om op grote schaal schadelijke domeinen te blokkeren, gericht op het verstoren van de criminele infrastructuur
Wbsrz (Wet bevorderen samenwerking en rechtmatige zorg)	Een Nederlandse wet die per 1 januari 2025 IKZ een juridische basis (RWT) geeft en de uitwisseling van signalen tussen negen zorgpartners mogelijk maakt om zorgfraude te bestrijden. Partners zijn onder de Wbsrz wettelijk verplicht om vermoedens van zorgfraude te melden aan IKZ

III. Bronnenlijst

(1/4)



Boeken, tijdschriften en rapporten

- Australian Competition & Consumer Commission. (2023, november). *National Anti-Scam Centre Advisory Board: Terms of Reference*. https://www.nasc.gov.au/system/files/national-anti-scam-centre-advisory-board-terms-of-reference-nov-23.pdf
- Australian Competiton & Consumer Commission. (2023). *National Anti Scam Centre in action: Quarterly update july-september 2023*. https://www.nasc.gov.au/
- Australian Competition & Consumer Commission. (2023). *Targeting scams: report of the ACCC on scams activity 2023*. https://www.nasc.gov.au/
- Australian Competition & Consumer Commission. (2024). *Investment Scam Fusion Cell report*. https://www.nasc.gov.au/
- Australian Competition & Consumer Commission. (2024). *Targeting scams report 2024*. https://www.nasc.gov.au
- Australian Competiton & Consumer Commission. (2025). *Job Scam Fusion Cell Report*. https://www.nasc.gov.au/
- Australian Competition & Consumer Commission. (2025). *Targeting scams report 2025*. https://www.nasc.gov.au
- Australian Competition & Consumer Commission. (2026). *Romance Scam Fusion Cell final report*. https://www.nasc.gov.au
- Bank Policy Institute. (2026). *What works, what doesn't in the global fight against scams*. https://bpi.com/what-works-what-doesnt-in-the-global-fight-against-scams/
- Centrum voor Cybersecurity België. (2025). *CCB Publicatie 10jaar*. https://ccb.belgium.be
- Centrum voor Cybersecurity België. (2025). *CCB Richtlijn voor de informatiesystemen van alle Belgische private en publieke organisaties gevestigd (of actief) in België*. CCB_Directive_1-2025_NL.pdf
- Centrum voor Cybersecurity België. (2025). *Cyber threat landscape and actions taken in Belgium 2025*. https://ccb.belgium.be
- Centrum voor Cybersecurity België. (2025). *Privacy Policy document 2025*. https://ccb.belgium.be
- Centrum voor Cybersecurity België. (2026). *Active Cyber Protection (ACP) policy document*. https://ccb.belgium.be
- De Kamer van Volksvertegenwoordigers van België. (zonder datum). *Begroting 2026*. lachambre.be
- Eerste Kamer der Staten-Generaal. (2020). *Wetsvoorstel bevorderen samenwerking en rechtmatige zorg*. https://www.eerstekamer.nl
- Informatieknooppunt Zorgfraude. (2022). *Rapport: Signalen fraude in de zorg 2022*. https://www.ikz.nl
- Informatieknooppunt Zorgfraude. (2023). *Rapport: Signalen fraude in de zorg 2023*. https://www.ikz.nl
- Informatieknooppunt Zorgfraude. (2025). *Jaarverslag 2025: Bestuursverslag en jaarrekening*. https://www.ikz.nl
- Informatieknooppunt Zorgfraude. (zonder datum). *Rapport misbruik van turboliquidaties in de zorg*. https://www.ikz.nl/onderzoek-en-analyse/
- Ministerie van Justitie en Veiligheid. (2026). *Actieplan Integrale Aanpak Online Fraude*.
- Stop Scams UK. (2022). *Annual report 2022*. https://stopscamsuk.org.uk
- Stop Scams UK. (2023). *The impact of artificial intelligence on fraud and scams*. https://stopscamsuk.org.uk

III. Bronnenlijst
(2/4)

Boeken, tijdschriften en rapporten (vervolg)

- Stop Scams UK. (2024). *The future of fraud*. https://stopscamsuk.org.uk
- Stop Scams UK. (zonder datum). *Written evidence submitted by Stop Scams UK*.
- Vereniging van Nederlandse Gemeenten. (zonder datum). *Verdiepend onderzoek Informatieknooppunt Zorgfraude (IKZ)*. https://vng.nl/kennisbank-impactanalyse/verdiepend-onderzoek-informatieknooppunt-zorgfraude-ikz

Wetten en juridische documenten

- Algemene Rekenkamer. (2019). *Statuten oprichting privaatrechtelijke rechtspersoon Stichting Informatieknooppunt zorgfraude*. https://www.rekenkamer.nl/
- *Australian Online Scams Code*. (zonder datum). (Verkrijgbaar via Digital Industry Group Inc.).
- *Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België van 10 oktober 2014*. (2014). Belgisch Staatsblad.
- *Scams Prevention Framework Act 2025*. (2025). (Australia).
- *Wet bevorderen samenwerking en rechtmatige zorg (Wbsrz)*. (2025). (Nederland). https://wetten.overheid.nl/BWBR0049565/2025-01-01

Media, persberichten en webartikelen

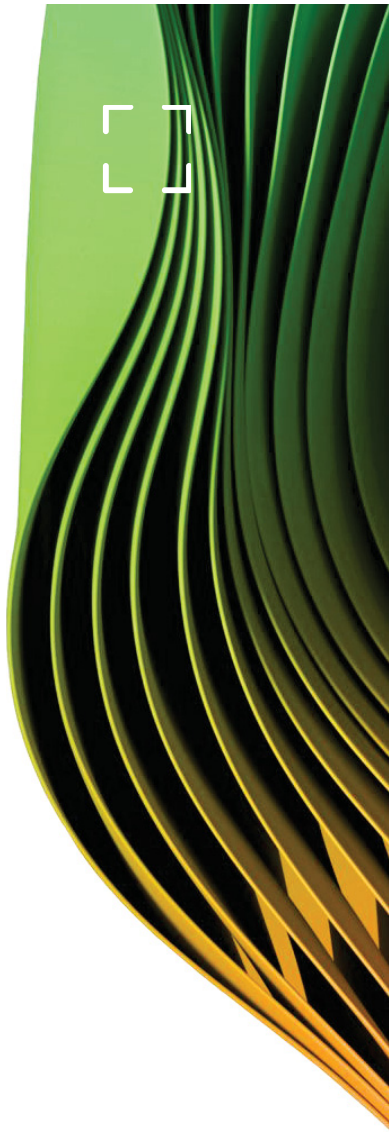
- Australian Competition & Consumer Commission. (zonder datum). *National Anti-Scam Centre calls for stronger business role to disrupt scams*. https://www.accc.gov.au/media-release/national-anti-scam-centre-calls-for-stronger-business-role-to-disrupt-scams
- Australian Competition & Consumer Commission. (zonder datum). *ACCC welcomes funding to establish National Anti-Scam Centre*. ACCC welcomes funding to establish National Anti-Scam Centre | ACCC
- Centrum voor Cybersecurity België. (zonder datum). *CCB en FOD Economie slaan handen ineen om beter online fraude aan te pakken*. https://ccb.belgium.be/nl/news/ccb-en-fod-economie-slaan-handen-ineen-om-beter-online-fraude-aan-te-pakken
- Centrum voor Cybersecurity België. (zonder datum). *De Safeonweb-campagne tegen beleggingsfraude: een groot succes*. https://ccb.belgium.be/nl/news/de-safeonweb-campagne-tegen-beleggingsfraude-een-groot-succes
- Centrum voor Cybersecurity België. (zonder datum). *Het CCB viert 10 jaar cybersecurity in België*. https://ccb.belgium.be/nl/news/het-ccb-viert-10-jaar-cybersecurity-belgie
- Centrum voor Cybersecurity België. (zonder datum). *Internationale betrekkingen*. https://ccb.belgium.be/nl/organisatie/samenwerking/internationale-betrekkingen
- Centrum voor Cybersecurity België. (zonder datum). *Meer aanvallen, meer meldingen: de cyberrealiteit in België 2025*. https://ccb.belgium.be/nl/news/meer-aanvallen-meer-meldingen-de-cyberrealiteit-belgie-2025
- Centrum voor Cybersecurity België. (zonder datum). *National Cybersecurity Certification Authority (NCCA)*. *https://ccb.belgium.be/nl/ncca*
- *Computer Weekly*. (zonder datum). *Stop Scams steps up to online fraud challenge*. https://www.computerweekly.com/news/366640819/Stop-Scams-steps-up-to-online-fraud-challenge

III. Bronnenlijst

(3/4)

Media, persberichten en webartikelen *(vervolg)*

- Cyberdaily.au. (zonder datum). *The National Anti-Scam Centre has warned more than 100 potential Australian crypto scam victims*. https://www.cyberdaily.au/security/11874-the-national-anti-scam-centre-has-warned-more-than-100-potential-australian-crypto-scam-victims
- Informatieknooppunt Zorgfraude. (zonder datum). *Samen tegen zorgfraude*. Samen tegen zorgfraude – Stichting Informatieknooppunt Zorgfraude
- Jacmac.com.au. (zonder datum). *Scams Prevention Framework*. https://www.jacmac.com.au/insights/scams-prevention-framework/
- NOS. (zonder datum). *Politie waarschuwt: criminelen zijn op grote schaal actief in de zorg*. https://nos.nl/artikel/2543324-politie-waarschuwt-criminelen-zijn-op-grote-schaal-actief-in-de-zorg
- Ofcom. (zonder datum). *Stop Scams UK's response to Ofcom's consultation on the approach to the implanting regulations to the Online Safety Bill*. https://www.ofcom.org.uk/
- Retail Banker International. (zonder datum). *UK companies fraud*. https://www.retailbankerinternational.com/news/uk-companies-fraud/?cf-view
- Secutec. (zonder datum). *Secutec wint exclusief contract met CCB voor levering van Cyber Threat Intelligence feeds*. https://secutec.com/nl/nieuws/secutec-wint-exclusief-contract-met-ccb-voor-levering-van-cyber-threat-intelligence-feeds
- Stop Scams UK. (zonder datum). *159 passes one million calls as Stop Scams UK and Virgin Money celebrate the service's success*. https://stopscamsuk.org.uk/159-one-million-calls-stop-scams-uk-virgin-money/
- Stop Scams UK. (zonder datum). *Stop Scams UK joins a global movement in the fight against fraud*. https://stopscamsuk.org.uk/stop-scams-uk-joins-a-global-movement-in-the-fight-against-fraud/
- Stop Scams UK. (zonder datum). *Stop Scams UK joint statement on data sharing and fraud*. https://stopscamsuk.org.uk/stop-scams-uk-joint-statement-data-sharing-fraud/
- Stop Scams UK. (zonder datum). *Stop Scams UK unites UK industries to intercept suspicious activity on a whole-sector basis*. https://stopscamsuk.org.uk/stop-scams-uk-unites-uk-industries/
- Stop Scams UK. (zonder datum). *Stop Scams UK wins at TECAs 2025*. https://stopscamsuk.org.uk/stop-scams-wins-at-tecas-2025/
- Stop Scams UK. (zonder datum). *Stop Scams UK wins PAY360 award for financial crime prevention*. https://stopscamsuk.org.uk/stop-scams-uk-wins-pay360-award-for-financial-crime-prevention/
- Stop Scams UK. (zonder datum). *UK dismantles organised crime infrastructure in fight against fraud*. https://stopscamsuk.org.uk/uk-dismantles-organised-crime-infrastructure-in-fight-against-fraud/
- Vereniging van Nederlandse Gemeenten. (zonder datum). *Verplicht aansluiten bij het Informatieknooppunt Zorgfraude*. https://vng.nl/nieuws/verplicht-aansluiten-bij-het-informatieknooppunt-zorgfraude
- VRT nieuws. (2026). *Phishing: Kan nieuw wapen tegen phishing aantal oplichtpogingen echt met 80 procent doen dalen?* https://www.vrt.be/vrtnws/nl/2026/03/18/phishing-nieuwe-tool-ccb-scanner/



III. Bronnenlijst

(4/4)

Overige webpagina's en documenten

- Centrum voor Cybersecurity België. (zonder datum). *Eerste hulp bij een cyberaanval*. https://ccb.belgium.be/nl/cert/eerste-hulp-bij-een-cyberaanval
- Companies House. (zonder datum). *Stop Scams UK Limited - Company information*. https://find-and-update.company-information.service.gov.uk/company/12505168
- Europol. (2024). *Internet Organised Crime Threat Assessment 2024*. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
- Europol. (2025). *Internet Organised Crime Threat Assessment 2025, 'Steal, deal and repeat. How cybercriminals trade and exploit your data'*. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf
- Informatieknooppunt Zorgfraude. (zonder datum). *Over Stichting Informatieknooppunt Zorgfraude (St. IKZ)*. *https://www.ikz.nl/portfolio/*
- Informatieknooppunt Zorgfraude. (zonder datum). *Privacy statement Stichting Informatieknooppunt Zorgfraude (IKZ)*. https://www.ikz.nl/privacy-statement-stichting-informatieknooppunt-zorgfraude-ikz/
- Ministerie van Justitie en Veiligheid. (zonder datum). *Samenwerkingspartners*. https://integraleaanpakonlinefraude.nl/page/view/2391c7c7-c9e2-47c7-b776-4bf6d8b615bb/samenwerkingspartners
- National Anti-Scam Centre. (zonder datum). *How we're run*. https://www.nasc.gov.au/what-we-do/how-were-run
- National Anti-Scam Centre. (zonder datum). *Short form privacy policy*. https://www.nasc.gov.au/what-we-do/using-our-website/short-form-privacy-policy
- Politie. (2024). *Online Fraude in Beeld. Fenomeenbeeld 2024*. https://www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2025/08c2a206-2a66-442d-bec7-90b3a3269189.pdf
- Rijksoverheid. (zonder datum). *Aanpak fraude in de zorg door uitwisselen informatie*. https://www.rijksoverheid.nl/onderwerpen/fouten-en-fraude-in-de-zorg/aanpak-fraude-in-de-zorg-door-uitwisselen-informatie
- Safeonweb @ work. (Zonder datum). https://atwork.safeonweb.be/nl
- Stop Scams UK. (zonder datum). *About*. https://stopscamsuk.org.uk/about/
- Stop Scams UK. (2021). *Introduction to Stop Scams and 159 presentation*. https://niccstandards.org.uk/wp-content/uploads/2021/11/14-NICC-StopScamsUK.pdf
- Stop Scams UK. (zonder datum). *Scam data sharing and scam intelligence privacy notice*. https://stopscamsuk.org.uk/privacy/scam-data-sharing-and-scam-intelligence-privacy-notice/
- United Nations. (2026). *Global Fraud Summit 2026, 'Call to Action on Combating Fraud'*. https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf

Deloitte.