EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BEOORDELINGSKADER VOOR NATIONALE CAPACITEITEN

DECEMBER 2020

OVER ENISA

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, streeft ernaar een hoog niveau van cyberbeveiliging in heel Europa te bereiken. Enisa is opgericht in 2004 en heeft een sterker fundament gekregen door de cyberbeveiligingsverordening van de EU. Het Agentschap draagt bij aan het cyberbeveiligingsbeleid van de EU, vergroot de betrouwbaarheid van ICT-producten, -diensten en -processen door middel van certificeringsprogramma's voor cyberbeveiliging, werkt samen met de lidstaten en instanties van de EU en helpt Europa zich voor te bereiden op de cyberuitdagingen van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de verbonden economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk de Europese samenleving en burgers digitaal veilig te stellen. Zie voor meer informatie www.enisa.europa.eu.

CONTACT

Om contact op te nemen met de auteurs kunt u gebruikmaken van team@enisa.europa.eu.
Voor persvragen over dit document kunt u gebruikmaken van press@enisa.europa.eu.

AUTEURS

Anna Sarri, Pinelopi Kyranoudi – Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

DANKBETUIGING

Enisa wil graag alle deskundigen bedanken die hebben deelgenomen aan en waardevolle input hebben geleverd voor dit verslag, en met name de volgende personen en instanties, op alfabetische volgorde:

Centraal Staatsbureau voor de ontwikkeling van de digitale samenleving (Kroatië), Marin Ante Pivcevic

Centrum voor Cybersecurity (België)

CFCS – Center for Cybersikkerhed (Denemarken), Thomas Wulff

Cyber Security Policy Division, Department of Environment, Climate and Communications (Ierland), James Caffrey

Europees Centrum voor de bestrijding van cybercriminaliteit – EC3, Alzofra Martinez Alvaro

Europees Centrum voor de bestrijding van cybercriminaliteit – EC3, Adrian-Ionut Bobeica

Federaal Ministerie van Binnenlandse Zaken (Duitsland), Sascha-Alexander Lettgen

Informatiebeveiligingsadministratie (Slovenië), Marjan Kavčič

Italiaanse regering (Italië)

Malta Information Technology Agency (Malta), Katia Bonello en Martin Camilleri

Ministerie van Digitaal Beleid (Griekenland), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali en Sotiris Vasilos

Ministerie van Economische Zaken en Communicatie (Estland), Anna-Liisa Pärnalaas

Ministerie van Justitie en Openbare Veiligheid (Noorwegen), Robin Bakke

Nationaal Agentschap voor cyber- en informatiebeveiliging (Tsjechië), Veronika Netolická

Nationaal Veiligheidsbureau (Spanje), Maria Mar Lopez Gil

Nationale Veiligheidsautoriteit (Slowakije)

NCTV, Ministerie van Justitie en Veiligheid (Nederland)

Portugees Nationaal centrum voor cyberbeveiliging (Portugal), Alexandre Leite en Pedro Matos

Universiteit van Oxford – Global Cyber Security Capacity Centre, Carolin Weisser Harris

Enisa wil ook graag alle deskundigen bedanken die waardevolle input hebben geleverd, maar liever anoniem blijven.

JURIDISCHE KENNISGEVING

AUTEURSRECHTVERMELDING

ISBN: 978-92-9204-490-9

DOI: 10.2824/962331

CATALOGUS: TP-02-21-253-NL-N

1. INHOUDSOPGAVE

VERKLARENDE WOORDENLIJST

ACRONIEM	DEFINITIE
AVG	algemene verordening gegevensbescherming
C2M2	maturiteitsmodel inzake cyberbeveiligingscapaciteit (Cybersecurity Capability Maturity Model)
CCRA	overeenkomst betreffende de erkenning van gemeenschappelijke criteria (Common Criteria Recognition Arrangement)
CCSMM	communautair maturiteitsmodel voor cyberbeveiliging (Community Cybersecurity Maturity Model)
CII	kritieke informatie-infrastructuur (Critical Information Infrastructure)
CMM	maturiteitsmodel inzake cyberbeveiliging voor naties (Cybersecurity Capacity Maturity Model for Nations)
CMMC	certificering van het maturiteitsmodel inzake cyberbeveiliging (Cybersecurity Maturity Model Certification)
CPI	index voor cybermacht (Cyber Power Index)
CSIRT	computercalamiteitenteams (Computer Security Incident Response Teams)
CVD	gecoördineerde openbaarmaking van kwetsbaarheden (Coordinated Vulnerability Disclosure)
DPA	gegevensbeschermingswet (Data Protection Act)
DSM	digitale eengemaakte markt (Digital Single Market)
ECCG	Europese Groep voor cyberbeveiligingscertificering (European Cybersecurity Certification Group)
ECSM	Europese maand van de cyberbeveiliging (European Cybersecurity Month)
ECSO	Europese organisatie voor cyberbeveiliging (European Cyber Security Organisation)
EQF	Europees kwalificatiekader (European Qualifications Framework)
EU	Europese Unie
EVA	Europese Vrijhandelsassociatie
GCI	wereldwijde index voor cyberbeveiliging (Global Cybersecurity Index)
GDS	digitale overheidsdienst (Government Digital Service)
IA-CM	model voor interne controlecapaciteit voor de publieke sector (Internal Audit Capability Model for the Public Sector)
ICT	informatie- en communicatietechnologie

ISMM	maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (Information Security Maturity Model for NIST Cybersecurity Framework)
ITU	Internationale Telecommunicatie-unie
KI	kunstmatige intelligentie
kmo's	kleine en middelgrote ondernemingen
LEA	rechtshandhavingsautoriteit (Law Enforcement Agency)
LS	lidstaat
NCSS	nationale cyberbeveiligingstrategie (National Cybersecurity Strategy)
NIB	netwerk- en informatiebeveiliging
NIST	National Institute of Standards and Technology (Amerikaans nationaal instituut voor normen en technologie)
NLO	nationale verbindingsfunctionarissen (National Liaison Officers)
O&O	onderzoek en ontwikkeling
OES	aanbieders van essentiële diensten (Operators of Essential Services)
OT	operationele technologieën (Operations Technology)
PET	privacybevorderende technologieën (Privacy Enhancing Technologies)
PIMS	informatiebeheerssysteem op het gebied van privacy (Privacy Information Management System)
PPP	publiek-private partnerschappen
Q-C2M2	Qatar-maturiteitsmodel inzake cyberbeveiliging (Qatar Cybersecurity Capability Maturity Model)
SOG-IS MRA	overeenkomst inzake wederzijdse erkenning van SOG-IS, de Groep van Hoge Ambtenaren voor de beveiliging van informatiesystemen (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement)

SAMENVATTING

Aangezien het huidige cyberdreigingslandschap zich blijft uitbreiden en de intensiteit en het aantal cyberaanvallen blijven toenemen, moeten de EU-lidstaten effectief reageren door hun nationale strategieën voor cyberbeveiliging (NCSS) verder te ontwikkelen en aan te passen. Sinds de publicatie van de eerste NCSS-studies door Enisa in 2012 hebben de EU-lidstaten en de EVA-landen grote vooruitgang geboekt bij de ontwikkeling en uitvoering van hun strategieën.

In dit verslag worden de werkzaamheden gepresenteerd die Enisa heeft verricht bij het opzetten van een beoordelingskader voor nationale capaciteiten (NCAF).

Het kader heeft ten doel lidstaten een zelfbeoordeling van hun maturiteitsniveau te bieden door het evalueren van hun NCSS-doelstellingen, en hen op die manier helpen zowel op strategisch als op operationeel niveau hun cyberbeveiligingscapaciteiten te verbeteren en op te bouwen.

Het schetst een eenvoudig representatief beeld van het maturiteitsniveau van de cyberbeveiliging van de lidstaat. Het NCAF is een instrument dat de lidstaten helpt:

- nuttige informatie te verstrekken voor de ontwikkeling van een langetermijnstrategie (bv. goede praktijken, richtsnoeren);
- ontbrekende elementen binnen de NCSS te identificeren;
- verder cyberbeveiligingscapaciteiten op te bouwen;
- de verantwoordingsplicht in verband met politiek handelen te ondersteunen;
- geloofwaardigheid te geven ten aanzien van het grote publiek en van internationale partners;
- voorlichtingsprogramma's te ondersteunen en het openbaar imago te verbeteren als transparante organisatie;
- te anticiperen op de uitdagingen die ons te wachten staan;
- de geleerde lessen en de beste praktijken in kaart te brengen;
- een referentiekader te bieden voor de cyberbeveiligingscapaciteit binnen de EU om de besprekingen te vergemakkelijken; en
- de nationale capaciteiten op het gebied van cybersecurity te beoordelen.

Dit kader werd ontworpen met de steun van deskundigen van Enisa en vertegenwoordigers van 19 lidstaten en EVA-landen[1]. De doelgroep van dit rapport zijn beleidsmakers, deskundigen en

[1] Vertegenwoordigers van de volgende lidstaten en EVA-landen zijn geïnterviewd: België, Denemarken, Duitsland, Estland, Griekenland, Hongarije, Ierland, Italië, Kroatië, Liechtenstein, Malta, Nederland, Noorwegen, Portugal, Slovenië, Slowakije, Spanje, Tsjechië, Zweden.

overheidsfunctionarissen die verantwoordelijk zijn voor of betrokken zijn bij het ontwerpen, uitvoeren en evalueren van een NCSS en, op een breder niveau, cyberbeveiligingscapaciteiten.

Het beoordelingskader voor nationale capaciteiten omvat 17 strategische doelstellingen en is opgebouwd rond vier hoofdclusters:

- Cluster 1: Cyberveiligheidsbeleid en -normen
  1. Ontwikkelen van een nationaal cybernoodplan
  2. Opstellen van basisbeveiligingsmaatregelen
  3. Beveiligen van de digitale identiteit en opbouwen van vertrouwen in digitale overheidsdiensten

- Cluster 2: Capaciteitsopbouw en bewustmaking
  4. Organiseren van cyberbeveiligingsoefeningen
  5. Opzetten van een incidentresponscapaciteit
  6. Vergroten van bewustzijn onder gebruikers
  7. Uitbreiden van onderwijs- en opleidingsprogramma's
  8. Bevorderen van O&O
  9. Bieden van stimulansen voor de private sector om te investeren in beveiligingsmaatregelen
  10. De cyberbeveiliging van de toeleveringsketen verbeteren

- Cluster 3: Wet- en regelgeving
  11. Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners
  12. Cybercriminaliteit aanpakken
  13. Ontwikkelen van mechanismen voor het melden van incidenten
  14. Versterken van privacy- en gegevensbescherming

- Cluster 4: Samenwerking
  15. Opzetten van een publiek-privaat partnerschap
  16. Institutionele samenwerking tussen openbare instanties
  17. Deelnemen aan internationale samenwerking

1. INLEIDING

In de richtlijn netwerk- en informatiebeveiliging (NIS-richtlijn), die in juli 2016 werd gepubliceerd, is vastgesteld dat EU-lidstaten een nationale strategie voor de beveiliging van netwerk- en informatiesystemen moeten aannemen, ook wel nationale cyberbeveiligingsstrategie (National Cyber Security Strategy, NCSS) genoemd, zoals vastgelegd in artikel 1 en 7. In deze context wordt een NCSS gedefinieerd als een kader waarbinnen strategische beginselen, richtsnoeren, strategische doelstellingen, prioriteiten, passend beleid en regelgevende maatregelen worden vastgesteld. Het beoogde doel van een NCSS is het bereiken en handhaven van een hoog niveau van netwerk- en systeembeveiliging, zodat de lidstaten potentiële bedreigingen kunnen beperken. Bovendien kan een NCSS ook een katalysator zijn voor industriële ontwikkeling en economische en sociale vooruitgang.

De cyberbeveiligingsverordening van de EU bepaalt dat Enisa de verspreiding van beste praktijken bij de definitie en implementatie van een NCSS moet bevorderen door lidstaten te ondersteunen bij de aanname van de NIS-richtlijn en door waardevolle feedback over hun ervaringen te verzamelen. Daartoe heeft Enisa verschillende instrumenten uitgewerkt om de lidstaten te helpen bij het ontwikkelen, uitvoeren en evalueren van hun nationale cyberbeveiligingsstrategieën.

Als onderdeel van zijn mandaat wil Enisa een kader voor zelfbeoordeling van nationale capaciteiten ontwikkelen om het maturiteitsniveau van de verschillende nationale cyberbeveiligingsstrategieën te meten. In dit rapport wordt de studie gepresenteerd die werd uitgevoerd bij het bepalen van het zelfbeoordelingskader.

1.1 TOEPASSINGSGEBIED EN DOELSTELLINGEN VAN DE STUDIE

Het hoofddoel van deze studie is het creëren van een kader voor zelfbeoordeling van nationale capaciteiten, hierna ook NCAF (National Capabilities Assessment Framework) genoemd, om het maturiteitsniveau van de cyberbeveiligingscapaciteiten van de lidstaten te meten. Meer in het bijzonder moet het kader de lidstaten in staat stellen:

- hun nationale cyberbeveiligingscapaciteiten te beoordelen;
- een beter besef van het maturiteitsniveau van het land te ontwikkelen;
- verbeterpunten in kaart te brengen; en
- cyberbeveiligingscapaciteiten op te bouwen.

Dit kader moet de lidstaten, en met name de nationale beleidsmakers, helpen een zelfbeoordeling uit te voeren om de nationale cyberbeveiligingscapaciteiten te verbeteren.

1.2 METHODOLOGISCHE AANPAK

De methodologische aanpak die is gebruikt voor de ontwikkeling van het beoordelingskader voor nationale capaciteiten berust op vier belangrijke stappen:

1. **Deskresearch**: in de eerst fase werd een uitgebreid literatuuronderzoek uitgevoerd om de beste praktijken te verzamelen met betrekking tot het ontwikkelen van een maturiteitsbeoordelingskader voor nationale cyberbeveiligingsstrategieën. De deskresearch richtte zich op een systematische analyse van relevante documenten over capaciteitsopbouw en strategiebepaling ten aanzien van cyberbeveiliging, op bestaande nationale cyberbeveiligingsstrategieën van lidstaten en op een vergelijking van bestaande maturiteitsmodellen op het gebied van cyberbeveiliging. Er werd een

benchmarkoefening op bestaande maturiteitsmodellen uitgevoerd met behulp van een analysekader dat ten behoeve van deze studie werd ontwikkeld. Het analysekader bouwt voort op de Becker-methode[2] voor de ontwikkeling van maturiteitsmodellen, die een generiek en geconsolideerd proceduremodel vastlegt voor het ontwerpen van maturiteitsmodellen en duidelijke eisen stelt voor de ontwikkeling van maturiteitsmodellen. Het analysekader werd verder aangepast om aan de behoeften van deze studie te voldoen.

2. **Verzameling van standpunten van deskundigen en belanghebbenden**: op basis van de gegevens die werden verzameld via deskresearch en de voorlopige bevindingen van de analyse, werd in deze fase gezocht naar deskundigen die ervaring hebben met de ontwikkeling en implementatie van nationale cyberbeveiligingsstrategieën of maturiteitsmodellen. Enisa nam contact op met zijn groep van deskundigen inzake nationale cyberbeveiligingstrategieën en nationale verbindingsfunctionarissen om de relevante deskundigen in elke lidstaat te vinden. Daarnaast werden enkele deskundigen geïnterviewd die betrokken zijn bij de ontwikkeling van maturiteitsmodellen. In totaal werden 22 interviews gehouden, waarvan 19 met vertegenwoordigers van cyberbeveiligingsagentschappen binnen verschillende lidstaten (en EVA-landen).
3. **Analyse van de inventarisatie-input:** de door middel van deskresearch en de interviews verzamelde gegevens werden vervolgens geanalyseerd om de beste praktijken in kaart te brengen bij het ontwerpen van een zelfbeoordelingskader om de maturiteit van nationale cyberbeveiligingstrategieën te meten, de behoeften van de lidstaten te begrijpen en te bepalen welke gegevens in de verschillende Europese landen daadwerkelijk kunnen worden verzameld[3]. Dankzij deze analyse kon het in de vorige stappen ontwikkelde voorlopige model worden verfijnd, alsook de in het model opgenomen indicatoren, de maturiteitsniveaus en de dimensies ervan.
4. **Afronding van het model:** een bijgewerkte versie van het kader voor zelfbeoordeling van nationale capaciteiten geëvalueerd door de desbetreffende deskundigen van Enisa en vervolgens, voorafgaand aan de publicatie, verder gevalideerd door deskundigen tijdens een workshop die in oktober 2020 is gehouden.

1.3 DOELGROEP

De doelgroep van dit rapport zijn beleidsmakers, deskundigen en overheidsfunctionarissen die verantwoordelijk zijn voor of betrokken zijn bij het ontwerpen, uitvoeren en evalueren van een NCSS en, op een breder niveau, cyberbeveiligingscapaciteiten. Bovendien kunnen de bevindingen die in dit document worden geformaliseerd waardevol zijn voor deskundigen en onderzoekers op het gebied van cyberbeveiligingsbeleid op nationaal of Europees niveau.

[2] J. Becker, R. Knackstedt en J. Pöppelbuß, “Developing Maturity Models for IT Management: A Procedure Model and its Application,” Business & Information Systems Engineering, vol. 1, nr. 3, blz. 213, juni 2009.
[3] In het kader van dit onderzoek omvatten de 'Europese landen' waarnaar in dit rapport wordt verwezen, de 27 EU-lidstaten.

2. ACHTERGROND

2.1 EERDERE WERKZAAMHEDEN OP HET GEBIED VAN DE LEVENSCYCLUS VAN EEN NCSS

Zoals vermeld in de cyberbeveiligingsverordening van de EU is een van de belangrijkste doelstellingen van Enisa het ondersteunen van de lidstaten bij het ontwikkelen van nationale strategieën voor de beveiliging van netwerk- en informatiesystemen, het bevorderen van de verspreiding van die strategieën en het monitoren van de uitvoering ervan. Als onderdeel van zijn mandaat heeft Enisa verschillende documenten over dit onderwerp opgesteld om de uitwisseling van goede praktijken te bevorderen en de uitvoering van nationale cyberbeveiligingsstrategieën binnen de EU te ondersteunen:

- de “Practical guide on the development and execution phase of NCSS”[4], gepubliceerd in 2012;
- de “Setting the course for national efforts to strengthen security in cyberspace”[5], gepubliceerd in 2012;
- het eerste Enisa-kader voor de beoordeling van de nationale cyberbeveiligingsstrategie van lidstaten, gepubliceerd in 2014[6];
- de “Online NCSS Interactive Map”[7], gepubliceerd in 2014;
- de “NCSS Good Practice Guide”[8], gepubliceerd in 2016;
- de “National Cybersecurity Strategies Evaluation Tool”[9], gepubliceerd in 2018;
- de “Good practices in innovation on Cybersecurity under the NCSS”[10], gepubliceerd in 2019.

BIJLAGE A geeft een korte samenvatting van de belangrijkste publicaties van Enisa over dit onderwerp.

De bovengenoemde gidsen en documenten werden bestudeerd als onderdeel van de deskresearch. Met name de “National Cybersecurity Strategies Evaluation Tool” (evaluatietool voor nationale cyberbeveiligingsstrategieën)[11] is een fundamenteel element van het NCAF. Het NCAF bouwt voort op de doelstellingen van de online tool voor de evaluatie van nationale cyberbeveiligingsstrategieën.

[4] NCSS: Practical Guide on Development and Execution (Enisa, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Enisa, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (Enisa, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (Enisa, 2014, bijgewerkt in 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Dit document is een update van de gids uit 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Enisa, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

2.2 GEMEENSCHAPPELIJKE DOELSTELLINGEN IN HET KADER VAN DE EUROPESE NATIONALE CYBERBEVEILIGINGSSTRATEGIEËN

De verschillen tussen de verschillende lidstaten maken het moeilijk om gemeenschappelijke activiteiten of actieplannen tussen verschillende nationale contexten, wettelijke kaders en politieke agenda's vast te stellen. De nationale cyberbeveiligingsstrategieën van de lidstaten hebben echter vaak strategische doelstellingen die rond dezelfde thema's zijn opgebouwd. Zo werden op basis van de eerdere werkzaamheden van Enisa en de analyse van de nationale cyberbeveiligingsstrategieën van de lidstaten 22 strategische doelstellingen aangewezen. Vijftien van deze strategische doelstellingen werden reeds aangewezen tijdens eerdere werkzaamheden van Enisa, twee werden nieuw toegevoegd in deze studie en vijf doelstellingen werden aangewezen voor verdere overwegingen.

2.2.1 Gemeenschappelijke strategische doelstellingen van de lidstaten

Steunend op eerdere werkzaamheden van Enisa, te weten de evaluatietool voor nationale cyberbeveiligingsstrategieën (National Cybersecurity Strategies Evaluation Tool[12]), toont de volgende tabel de bovengenoemde reeks van 15 strategische doelstellingen die doorgaans deel uitmaken van de nationale cyberbeveiligingsstrategieën van de lidstaten. De doelstellingen schetsen de kern van de algemene 'nationale filosofie' over dit onderwerp. Voor aanvullende informatie over de hieronder beschreven doelstellingen wordt verwezen naar het rapport van Enisa: "NCSS Good Practice Guide"[13].

Tabel 1: Gemeenschappelijke strategische doelstellingen die deel uitmaken van de nationale cyberbeveiligingsstrategie van een lidstaat

ID	Strategische doelstellingen binnen een nationale cyberbeveiligingsstrategie	Doelstellingen
1	**Ontwikkelen van nationale cybernoodplannen**	▶ de criteria presenteren en toelichten die gebruikt moeten worden om een situatie als crisis te definiëren; ▶ belangrijkste processen en acties vaststellen om de crisis aan te pakken; en ▶ duidelijk de rollen en verantwoordelijkheden van verschillende belanghebbenden tijdens een cybercrisis definiëren; ▶ de criteria presenteren en toelichten die bepalen dat een crisis voorbij is en/of wie de bevoegdheid heeft om dit uit te maken.
2	**Opstellen van basisbeveiligingsmaatregelen**	▶ de verschillende praktijken van de organisaties in zowel de publieke als de private sector harmoniseren; ▶ een gemeenschappelijke taal tussen de bevoegde overheidsinstanties en de organisaties en open veilige communicatiekanalen creëren; ▶ verschillende belanghebbenden in staat stellen om hun cyberbeveiligingscapaciteiten te controleren en te benchmarken; ▶ informatie delen over goede cyberbeveiligingspraktijken in elke bedrijfstak; en ▶ belanghebbenden helpen bij het prioriteren van hun investeringen in beveiliging.
3	**Organiseren van cyberbeveiligingsoefeningen**	▶ bepalen wat er getest moet worden (plannen en processen, mensen, infrastructuur, responscapaciteit, samenwerkingscapaciteit, communicatie, enz.);

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Dit document is een update van de gids uit 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Enisa, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Strategische doelstellingen binnen een nationale cyberbeveiligingsstrategie	Doelstellingen
		▶ een nationaal team voor het plannen van cyberoefeningen oprichten, met een duidelijke opdracht; en ▶ cyberoefeningen integreren in de levenscyclus van de nationale cyberbeveiligingsstrategie of het nationale cybernoodplan.
4	Ontwikkelen van een capaciteit voor incidentenrespons	▶ mandaat – dit heeft betrekking op de bevoegdheden, rollen en verantwoordelijkheden die door de respectieve overheid aan het team moeten worden toegekend; ▶ dienstenportfolio – dit omvat de diensten die een team aan zijn achterban verleent of gebruikt voor zijn eigen interne werking; ▶ operationele capaciteiten – deze betreffen de technische en operationele eisen waaraan een team moet voldoen; en ▶ samenwerkingscapaciteiten – deze omvatten de eisen met betrekking tot het delen van informatie met andere teams die niet onder de voorgaande drie categorieën vallen, bijvoorbeeld beleidsmakers, defensie, regelgevende instanties, exploitanten (van kritieke informatie-infrastructuur) en rechtshandhavingsautoriteiten.
5	Vergroten van bewustzijn onder gebruikers	▶ lacunes in de kennis over cyberbeveiliging of informatiebeveiliging in kaart brengen; en ▶ de lacunes opvullen door bewustzijn te vergroten of door kennisgrondslagen te ontwikkelen/versterken.
6	Uitbreiden van onderwijs- en opleidingsprogramma's	▶ de operationele capaciteiten van de bestaande informatiebeveiligingsmedewerkers verbeteren; ▶ studenten stimuleren deel te nemen en hen voorbereiden op het cyberbeveiligingswerkveld; ▶ de betrekkingen tussen de academische wereld van de informatiebeveiliging en de informatiebeveiligingssector bevorderen en stimuleren; en ▶ opleidingen op het gebied van cyberbeveiliging afstemmen op zakelijke behoeften.
7	Bevorderen van O&O	▶ de werkelijke oorzaken van de kwetsbaarheden in kaart brengen in plaats van de impact ervan te herstellen; ▶ wetenschappers uit verschillende disciplines samenbrengen om oplossingen te bieden voor multidimensionale en complexe problemen, zoals cyber-fysieke dreigingen; ▶ de behoeften van de sector en de onderzoeksresultaten samenbrengen, om zo de overgang van theorie naar praktijk te vergemakkelijken; en ▶ manieren vinden om niet alleen het cyberbeveiligingsniveau van bestaande cyberinfrastructuren ondersteunende producten en diensten te handhaven, maar ook om dit niveau te verhogen.
8	Bieden van stimulansen voor de private sector om te investeren in beveiligingsmaatregelen	▶ vaststellen van mogelijke stimulansen voor particuliere bedrijven om te investeren in beveiligingsmaatregelen; en ▶ bedrijven stimulansen bieden om investeringen in beveiliging aan te moedigen.
9	Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners	▶ kritieke informatie-infrastructuur in kaart brengen; en ▶ relevante risico's voor CII vaststellen en beperken.
10	Cybercriminaliteit aanpakken	▶ wetten opstellen op het gebied van cybercriminaliteit; en ▶ de effectiviteit van rechtshandhavingsautoriteiten verhogen.
11	Ontwikkelen van mechanismen voor het melden van incidenten	▶ kennis vergaren over de algehele bedreigingsomgeving; ▶ de impact van incidenten (bv. beveiligingsinbreuken, netwerkstoringen, dienstonderbrekingen) beoordelen; ▶ kennis vergaren over bestaande en nieuwe kwetsbaarheden en soorten aanvallen; ▶ de beveiligingsmaatregelen dienovereenkomstig actualiseren; en

ID	Strategische doelstellingen binnen een nationale cyberbeveiligingsstrategie	Doelstellingen
		▶ de bepalingen van de NIS-richtlijn met betrekking tot het melden van incidenten ten uitvoer leggen.
12	Versterken van privacy- en gegevensbescherming	▶ bijdragen aan de versterking van de grondrechten inzake privacy en gegevensbescherming.
13	Opzetten van een publiek-privaat partnerschap (PPP)	▶ afschrikken (om aanvallers af te schrikken); ▶ beschermen (maakt gebruik van onderzoek naar nieuwe beveiligingsdreigingen); ▶ detecteren (gebruikt informatie-uitwisseling om nieuwe bedreigingen aan te pakken); ▶ reageren (om de mogelijkheid te bieden om de eerste impact van een incident het hoofd te bieden); en ▶ herstellen (om de mogelijkheid te bieden om de uiteindelijke impact van een incident te herstellen).
14	Institutionele samenwerking tussen openbare instanties	▶ de samenwerking tussen openbare instanties met verantwoordelijkheden en bevoegdheden op het gebied van cyberbeveiliging verhogen; ▶ voorkomen dat de bevoegdheden en middelen van openbare instanties elkaar overlappen; en ▶ de samenwerking tussen openbare instanties op verschillende gebieden van cyberbeveiliging verbeteren.
15	Deelnemen aan internationale samenwerking (niet alleen met EU-lidstaten)	▶ profiteren van de totstandbrenging van een gemeenschappelijke kennisbasis tussen de EU-lidstaten; ▶ synergie-effecten creëren tussen nationale cyberbeveiligingsinstanties; en ▶ de strijd tegen transnationale misdaad mogelijk maken en opvoeren.

2.2.2 Aanvullende strategische doelstellingen

Op basis van het uitgevoerde deskresearch en de door Enisa gehouden interviews werden bijkomende strategische doelstellingen vastgesteld. De lidstaten pakken deze punten steeds vaker aan in hun nationale cyberbeveiligingsstrategieën of stellen hierover actieplannen op. Er worden ook voorbeelden gegeven van activiteiten die door de lidstaten worden uitgevoerd. Als een voorbeeld uit een publiek beschikbare bron afkomstig is, wordt een referentie gegeven. In gevallen waarin de voorbeelden gebaseerd zijn op vertrouwelijke gesprekken met ambtenaren van EU-lidstaten, worden geen referenties gegeven.

De volgende aanvullende strategische doelstellingen zijn vastgesteld:

- de cyberbeveiliging van de toeleveringsketen verbeteren; en
- de digitale identiteit beveiligen en vertrouwen in digitale overheidsdiensten ontwikkelen.

De cyberbeveiliging van de toeleveringsketen verbeteren

Kleine en middelgrote ondernemingen (kmo's) vormen de ruggengraat van de Europese economie. Zij vertegenwoordigen 99% van alle bedrijven in de EU[14]. Volgens schattingen uit

[14] https://ec.europa.eu/growth/smes/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2015 zijn kmo's goed voor ongeveer 85% van de nieuwe banen en zorgen ze voor twee derde van de totale werkgelegenheid in de particuliere sector in de EU. Bovendien verlenen kmo's diensten aan grote ondernemingen en werken ze steeds meer samen met de overheid[15], waardoor ze in de huidige onderling verbonden context de zwakke schakel vormen voor cyberaanvallen. Kmo's zijn inderdaad het meest blootgesteld aan cyberaanvallen, maar kunnen zich vaak geen adequate investering in cyberbeveiliging veroorloven[16]. Het verbeteren van de cyberbeveiliging van de toeleveringsketen moet dan ook plaatsvinden met een focus op kmo's.

Naast deze systematische aanpak kunnen de lidstaten ook extra inspanningen leveren wat betreft de cyberbeveiliging van specifieke ICT-diensten en -producten die als essentieel worden beschouwd: ICT-technologieën die worden gebruikt in kritieke informatie-infrastructuur, beveiligingsmechanismen die worden gehanteerd in de telecommunicatiesector (bv. controles op ISP-niveau), vertrouwensdiensten zoals gedefinieerd in de eIDAS-verordening, en cloudaanbieders. Zo heeft Polen zich er in zijn nationale cyberbeveiligingsstrategie voor 2019-2024[17] toe verbonden een nationaal systeem voor de beoordeling en certificering van cyberbeveiliging te ontwikkelen als een mechanisme voor kwaliteitsborging in de toeleveringsketen. Dit certificeringssysteem zal worden afgestemd op het EU-certificeringskader voor digitale ICT-producten, -diensten en -processen dat is vastgesteld bij de EU-cyberbeveiligingsverordening (2019/881).

Het verbeteren van de cyberbeveiliging van de toeleveringsketen is dus van het grootste belang. Dit kan onder andere worden bereikt door een krachtig beleid te voeren dat gericht is op het stimuleren van kmo's, door in openbare aanbestedingsprocedures richtsnoeren voor eisen inzake cyberbeveiliging op te nemen, door de samenwerking binnen de particuliere sector te bevorderen, door PPP's op te zetten, door mechanismen voor gecoördineerde openbaarmaking van kwetsbaarheden te bevorderen[18], door een productcertificeringsregeling uit te werken, met onder meer cyberbeveiligingscomponenten in digitale initiatieven voor kmo's, en door de ontwikkeling van vaardigheden te financieren.

Beveiligen van de digitale identiteit en opbouwen van vertrouwen in digitale overheidsdiensten

In februari 2020 heeft de Commissie haar visie op de digitale transformatie van de EU uiteengezet in de mededeling "De digitale toekomst van Europa vormgeven"[19], met als doel inclusieve technologieën tot stand te brengen die werken voor mensen en de fundamentele waarden van de EU respecteren. In de mededeling wordt met name gesteld dat het bevorderen van de digitale transformatie van overheidsdiensten binnen Europa van cruciaal belang is. In die zin is het opbouwen van vertrouwen in de overheid met betrekking tot digitale identiteit en vertrouwen in openbare diensten van het grootste belang. Dit is des te belangrijker wanneer men bedenkt dat transacties en gegevensuitwisselingen in de publieke sector vaak een gevoelig karakter hebben.

Veel landen hebben te kennen gegeven dat zij dit onderwerp in hun nationale cyberbeveiligingsstrategie willen behandelen. Het gaat onder meer om: Denemarken, Estland, Frankrijk, Luxemburg, Malta, Nederland, Spanje en het Verenigd Koninkrijk. Sommige van deze landen hebben ook aangegeven dat deze strategische doelstelling in het kader van een breder plan kan worden aangepakt:

[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] De digitale toekomst van Europa vormgeven, COM(2020) 67 final: https://ec.europa.eu/transparency/regdoc/rep/1/2020/NL/COM-2020-67-F1-NL-MAIN-PART-1.PDF

- Estland koppelt zijn bijbehorende actieplan over “de veiligheid van de elektronische identiteit en de mogelijkheid tot elektronische authenticatie” aan de bredere Digitale Agenda 2020 voor Estland.
- Volgens de Franse NCSS ziet de voor digitale technologie verantwoordelijke staatssecretaris toe op het opstellen van een stappenplan “ter bescherming van het digitale leven, de privacy en de persoonlijke gegevens van het Franse volk”.
- Volgens de Nederlandse NCSS wordt cyberbeveiliging bij overheidsdiensten en openbare dienstverlening aan burgers en bedrijven uitgebreider behandeld in de brede Agenda Digitale Overheid.
- Aangezien de Britse regering steeds meer van haar diensten naar een online omgeving verplaatst, heeft zij de digitale overheidsdienst (Government Digital Service, GDS) aangesteld om ervoor te zorgen dat alle nieuwe digitale diensten die door de overheid worden ontwikkeld of aangeschaft ook ‘standaard veilig' zijn, met ondersteuning van het Britse National Cybersecurity Centre (NCSC).

2.2.3 Andere overwogen strategische doelstellingen

Andere strategische doelstellingen werden bestudeerd tijdens de deskresearchfase en als onderdeel van de door Enisa gehouden interviews. Er werd echter besloten dat deze doelstellingen geen deel zouden uitmaken van het kader voor zelfbeoordeling. BIJLAGE C – Overige bestudeerde doelstellingen geeft voor elk van deze doelstellingen definities die kunnen worden gebruikt om toekomstige besprekingen over mogelijke NCSS-verbeteringen te voeden.

De volgende strategische doelstellingen werden onderzocht als toekomstige overwegingen:

- het ontwikkelen van sectorspecifieke cyberbeveiligingsstrategieën;
- strijden tegen desinformatiecampagnes;
- het beveiligen van geavanceerde technologieën (5G, KI, quantum computing enz.);
- het waarborgen van gegevenssoevereiniteit; en
- het bieden van stimulansen voor de ontwikkeling van de cyberverzekeringssector.

2.3 BELANGRIJKSTE BEVINDINGEN UIT DE BENCHMARKOEFENING

De deskresearch naar bestaande maturiteitsmodellen met betrekking tot cyberbeveiliging werd uitgevoerd om informatie en bewijzen te verzamelen met het oog op het ontwerp van het zelfbeoordelingskader voor nationale capaciteiten op het gebied van nationale cyberbeveiligingsstrategieën. In deze context werd een uitgebreid literatuuronderzoek naar bestaande modellen uitgevoerd als aanvulling op de bevindingen van het initiële verkennende onderzoek naar maturiteitsmodellen inzake cyberbeveiliging en bestaande nationale cyberbeveiligingsstrategieën, zoals uiteengezet in paragrafen 2.1 en 2.2. Deze systematische evaluatie ondersteunt de selectie en rechtvaardiging van de maturiteitsniveaus van het beoordelingskader en de bepaling van de verschillende dimensies en indicatoren.

In het kader van de systematische evaluatie van maturiteitsmodellen werden tien modellen in aanmerking genomen en geanalyseerd op basis van hun belangrijkste kenmerken. Het globale overzicht van de belangrijkste kenmerken voor elk model dat in het kader van deze studie werd geëvalueerd, is beschikbaar in Tabel 2: Overzicht van geanalyseerde maturiteitsmodellen en een meer gedetailleerde analyse is te vinden in BIJLAGE A.

Tabel 2: Overzicht van geanalyseerde maturiteitsmodellen

Naam model	Aantal maturiteit sniveaus	Aantal eigenschap pen	Beoordelingsmethode	Weergave van de resultaten
Maturiteitsmodel inzake cyberbeveiliging voor naties (CMM)	5	5 hoofddimens ies	Samenwerking met een lokale organisatie om het model te verfijnen alvorens het toe te passen op de nationale context	5-delige radar
Maturiteitsmodel inzake cyberbeveiligingscapaciteit (C2M2)	4	10 hoofddomei nen	Methode en toolkit voor zelfevaluatie	Scorekaart met cirkeldiagrammen
Kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur	n.v.t. (4 niveaus)	5 kernfuncties	Zelfbeoordeling	n.v.t.
Qatar-maturiteitsmodel inzake cyberbeveiliging (Q-C2M2)	5	5 hoofddomei nen	n.v.t.	n.v.t.
Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)	5	17 hoofddomei nen	Beoordeling door externe auditeurs	n.v.t.
Communautair maturiteitsmodel voor cyberbeveiliging (CCSMM)	5	6 hoofddimens ies	Beoordeling binnen gemeenschappen met input van staats- en federale rechtshandhavingsautoriteite n	n.v.t.
Maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (ISMM)	5	23 beoordeelde gebieden	n.v.t.	n.v.t.
Model voor interne controlecapaciteit (IA-CM) voor de publieke sector	5	6 elementen	Zelfbeoordeling	n.v.t.
Wereldwijde index voor cyberbeveiliging (GCI)	n.v.t.	5 pijlers	Zelfbeoordeling	Ranglijst
Index voor cybermacht (CPI)	n.v.t.	4 categorieën	Benchmarking door de Economist Intelligence Unit	Ranglijst

Deze systematische evaluatie heeft het mogelijk gemaakt conclusies te trekken over de beste praktijken die in de bestaande modellen zijn aangenomen om de ontwikkeling van het conceptuele model voor het huidige maturiteitsmodel te ondersteunen. In het bijzonder ondersteunde de benchmarkoefening de definitie van de maturiteitsniveaus, de ontwikkeling van dimensieclusters en de selectie van indicatoren, alsmede een passende visualisatiemethode voor de resultaten van het model. De meest relevante bevindingen voor elk van deze elementen worden weergegeven in Tabel 3.

Tabel 3: Belangrijkste bevindingen uit de benchmarkoefening

Kenmerk	Belangrijkste bevinding
Maturiteitsniveaus	▶ Een maturiteitsschaal met vijf niveaus voor beoordelingskaders voor cyberbeveiligingscapaciteiten wordt algemeen aanvaard en kan granulaire beoordelingsresultaten opleveren (zie Tabel 6 Vergelijking van maturiteitsniveaus voor een uitputtend overzicht van de definitie van de maturiteitsniveaus voor elk model); ▶ Alle modellen bieden een definitie op hoog niveau van elk maturiteitsniveau dat vervolgens wordt aangepast aan de verschillende dimensies of clusters van dimensies; ▶ Bij het meten van de maturiteit van cyberbeveiligingscapaciteiten worden doorgaans twee belangrijke aspecten beoordeeld: de maturiteit van strategieën en de maturiteit van processen die worden ontwikkeld om strategieën uit te voeren.
Eigenschappen	▶ De vergelijkende analyse van de eigenschappen van de bestaande maturiteitsmodellen laat heterogene resultaten zien, met per model gemiddeld vier tot vijf eigenschappen; ▶ Een model dat op zo'n vier of vijf eigenschappen berust, biedt landen de juiste mate van gegevensgranulariteit door relevante dimensies te groeperen en de leesbaarheid van de resultaten te waarborgen (zie Tabel 7: Vergelijking van eigenschappen/dimensies voor een beschrijving van de eigenschappen voor elk model); ▶ Het basisprincipe dat door alle modellen wordt gehanteerd bij het definiëren van de clusters is gebaseerd op de consistentie van elementen die binnen elke cluster worden gegroepeerd.
Beoordelingsmethode	▶ De beoordelingsmethoden die in de verschillende geanalyseerde modellen worden gebruikt, verschillen van model tot model; ▶ De meest gebruikelijke beoordelingsmethode is gebaseerd op zelfevaluatie.
Weergave van de resultaten	▶ Het is belangrijk dat de resultaten op verschillende granulariteitsniveaus worden gepresenteerd; ▶ De wijze van visualisatie moet zelfverklarend en gemakkelijk leesbaar zijn.

Het conceptuele model werd gebaseerd op de benchmarkingoefening van de verschillende maturiteitsmodellen en op eerdere werkzaamheden van Enisa. Ook werd besloten voort te bouwen op het *interactieve online-instrument* van Enisa om voor elke eigenschap maturiteitsindicatoren te ontwikkelen.

2.4 UITDAGINGEN VAN DE NCSS-EVALUATIE

Lidstaten worden geconfronteerd met tal van uitdagingen wanneer zij cyberbeveiligingscapaciteiten ontwikkelen, en meer bepaald wanneer zij ervoor willen zorgen dat hun capaciteiten zijn aangepast aan de laatste ontwikkelingen. Hieronder volgt een samenvatting van de uitdagingen die in het kader van deze studie door de lidstaten werden vastgesteld en met hen werden besproken:

- **Moeilijkheden bij de coördinatie en de samenwerking:** het coördineren van cyberbeveiligingsinspanningen op nationaal niveau met het oog op een efficiënte reactie op cyberbeveiligingskwesties kan, gezien het grote aantal belanghebbenden, een uitdaging zijn.
- **Gebrek aan middelen om de beoordeling uit te voeren:** afhankelijk van de lokale context en de nationale bestuursstructuur ten aanzien van cyberbeveiliging, kan de evaluatie van een nationale cyberbeveiligingsstrategie en de doelstellingen ervan meer dan 15 mandagen in beslag nemen.
- **Gebrek aan ondersteuning voor de ontwikkeling van cyberbeveiligingscapaciteiten:** sommige lidstaten deelden mee dat zij, om een

begroting te verdedigen en ondersteuning te krijgen voor de ontwikkeling van cyberbeveiligingscapaciteiten, eerst een evaluatiefase moeten uitvoeren om lacunes en beperkingen vast te stellen.

- **Moeilijkheden bij het toeschrijven van successen of veranderingen aan de strategie:** aangezien bedreigingen elke dag evolueren en de technologie verbetert, moeten actieplannen voortdurend worden aangepast om hierop te reageren. Het evalueren van een NCSS en het toeschrijven van veranderingen aan de strategie zelf blijven echter een lastige opgave. Dit bemoeilijkt op zijn beurt de vaststelling van de beperkingen en tekortkomingen van de NCSS.
- **Moeilijkheden om de doeltreffendheid van de NCSS te meten:** er kunnen meetwaarden worden verzameld om verschillende aspecten te meten, zoals vooruitgang, uitvoering, maturiteit en doeltreffendheid. Hoewel het meten van vooruitgang en uitvoering relatief eenvoudig is in vergelijking met het meten van doeltreffendheid, blijft dit laatste zinvoller voor het evalueren van de uitkomsten en effecten van een NCSS. Op basis van de door Enisa gehouden interviews verklaarde een groot aantal lidstaten dat het kwantitatief meten van de doeltreffendheid van een NCSS belangrijk is, maar ook een zeer veeleisende taak is die in sommige gevallen zo goed als onmogelijk is.
- **Moeilijkheid om een gemeenschappelijk kader aan te nemen:** de EU-lidstaten opereren in verschillende contexten wat betreft politiek, organisaties, cultuur, maatschappelijke structuur en NCSS-maturiteit. Bepaalde lidstaten die in het kader van deze studie werden geïnterviewd, gaven aan dat het moeilijk zou kunnen zijn een 'one-size-fits-all'-zelfbeoordelingskader te verdedigen en te gebruiken.

2.5 VOORDELEN VAN EEN BEOORDELING VAN NATIONALE CAPACITEITEN

Sinds 2017 hebben alle EU-lidstaten een NCSS[20]. Hoewel dit een positieve ontwikkeling is, is het ook van belang dat de lidstaten deze nationale cyberbeveiligingsstrategieën naar behoren kunnen beoordelen en zodoende een meerwaarde kunnen geven aan hun strategische planning en uitvoering.

Een van de doelstellingen van het beoordelingskader voor nationale capaciteiten is de cyberbeveiligingscapaciteiten te beoordelen op basis van de prioriteiten die in de verschillende nationale cyberbeveiligingsstrategieën zijn vastgesteld. In de kern beoordeelt het kader het maturiteitsniveau van de cyberbeveiligingscapaciteiten van de lidstaten op de gebieden die door de NCSS-doelstellingen worden bepaald. De resultaten van het kader ondersteunen op die manier de beleidsmakers van de lidstaten bij het bepalen van de nationale cyberbeveiligingsstrategie door hen per land informatie te verstrekken over de stand van zaken[21]. Het NCAF is uiteindelijk bedoeld om lidstaten te helpen bij het vaststellen van gebieden waar verbetering mogelijk is en bij het opbouwen van capaciteiten.

Het kader heeft ten doel lidstaten een zelfbeoordeling van hun maturiteitsniveau te bieden door het evalueren van hun NCSS-doelstellingen, en hen op die manier helpen zowel op strategisch als op operationeel niveau hun cyberbeveiligingscapaciteiten te verbeteren en op te bouwen.

Wat de meer praktische aanpak betreft, werden op basis van de gesprekken die Enisa heeft gevoerd met verschillende agentschappen die in verschillende lidstaten verantwoordelijk zijn

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

voor cyberbeveiliging, de volgende voordelen van het beoordelingskader voor nationale capaciteiten aan het licht gebracht en onderstreept:

- verstrekken van nuttige informatie voor de ontwikkeling van een langetermijnstrategie (bv. goede praktijken, richtsnoeren);
- identificeren van ontbrekende elementen binnen de NCSS;
- verder opbouwen van cyberbeveiligingscapaciteiten;
- ondersteunen van de verantwoordingsplicht van politieke maatregelen;
- geloofwaardigheid geven ten aanzien van het grote publiek en van internationale partners;
- voorlichtingsprogramma's ondersteunen en het openbaar imago van transparante organisatie verbeteren;
- anticiperen op toekomstige uitdagingen;
- de geleerde lessen en de beste praktijken in kaart brengen;
- een referentiekader bieden voor de cyberbeveiligingscapaciteit binnen de EU om de besprekingen te vergemakkelijken; en
- de nationale capaciteiten op het gebied van cybersecurity beoordelen.

3. METHODE VAN HET BEOORDELINGSKADER VOOR NATIONALE CAPACITEITEN

3.1 ALGEMEEN DOEL

Het **hoofddoel** van het NCAF is het meten van het maturiteitsniveau van de cyberbeveiligingscapaciteiten van de **lidstaten** om hen te ondersteunen bij het evalueren van hun nationale cyberbeveiligingscapaciteiten, het vergroten van het bewustzijn van het nationale maturiteitsniveau, het vaststellen van gebieden die voor verbetering vatbaar zijn en het opbouwen van cyberbeveiligingscapaciteiten.

3.2 MATURITEITSNIVEAUS

Het kader is gebaseerd op **vijf maturiteitsniveaus** die de fasen bepalen die de lidstaten doorlopen bij het opbouwen van cyberbeveiligingscapaciteiten op het gebied dat onder elke NCSS-doelstelling valt. De niveaus vertegenwoordigen oplopende niveaus van maturiteit, te beginnen met **Niveau 1**, waarbij de lidstaten geen duidelijk omschreven aanpak hebben voor de opbouw van cyberbeveiligingscapaciteit op de gebieden die onder de doelstellingen van de NCSS vallen, en eindigend met **Niveau 5**, waarbij de strategie voor de opbouw van cyberbeveiligingscapaciteit dynamisch is en zich aanpast aan ontwikkelingen van de omgeving. Tabel 4 toont de schaal van maturiteitsniveaus met een beschrijving van elk maturiteitsniveau.

Tabel 4: De vijf niveaus van de maturiteitsschaal van het beoordelingskader voor nationale capaciteiten van Enisa

NIVEAU 1 – INITIEEL/AD HOC	NIVEAU 2 – VROEGE OMSCHRIJVING	NIVEAU 3 – VASTSTELLING	NIVEAU 4 – OPTIMALISATIE	NIVEAU 5 – ADAPTIVITEIT
De lidstaat heeft geen duidelijk omschreven aanpak voor de opbouw van cyberbeveiligingscapaciteit op de gebieden die onder de doelstellingen van de NCSS vallen. Niettemin kan het land een aantal algemene doelstellingen hebben en een aantal studies hebben uitgevoerd (technisch, politiek, beleidsmatig) om de nationale capaciteiten te verbeteren.	De nationale aanpak voor capaciteitsopbouw op het gebied dat onder de NCSS-doelstellingen valt, werd omschreven. De actieplannen of activiteiten om de resultaten te bereiken zijn er, maar bevinden zich in een vroeg stadium. Daarnaast zijn actieve belanghebbenden mogelijk geïdentificeerd en/of ingeschakeld.	Het actieplan voor capaciteitsopbouw op het gebied dat onder de doelstellingen van de NCSS valt, is duidelijk omschreven en wordt ondersteund door de betrokken belanghebbenden. De praktijken en activiteiten worden op nationaal niveau op uniforme wijze gehandhaafd en uitgevoerd. De activiteiten worden omschreven en gedocumenteerd, met een duidelijke toewijzing van middelen, een duidelijk beheer en een aantal deadlines.	Het actieplan wordt op gezette tijden geëvalueerd: het is geprioriteerd, geoptimaliseerd en duurzaam. De prestaties van de activiteiten voor capaciteitsopbouw op het gebied van cyberbeveiliging worden regelmatig gemeten. Succesfactoren, uitdagingen en lacunes bij de uitvoering van de activiteiten worden in kaart gebracht.	De strategie voor capaciteitsopbouw op het gebied van cyberbeveiliging is dynamisch en adaptief. Voortdurende aandacht voor milieuontwikkelingen (technologische vooruitgang, wereldwijde conflicten, nieuwe bedreigingen) bevordert een snelle besluitvorming en een vermogen om snel verbeteringen aan te brengen.

3.3 CLUSTERS EN OVERKOEPELENDE STRUCTUUR VAN HET ZELFBEOORDELINGSKADER

Het zelfbeoordelingskader wordt gekenmerkt door **vier clusters**: (I) Cyberveiligheidsbeleid en -normen, (II) Capaciteitsopbouw en bewustmaking, (III) Wet- en regelgeving en (IV) Samenwerking. Elk van deze clusters bestrijkt een belangrijk thematisch gebied voor de opbouw van cyberbeveiligingscapaciteit in een land en bevat een pool van verschillende doelstellingen die de lidstaten in hun nationale cyberbeveiligingsstrategieën kunnen opnemen. In het bijzonder:

- **(I) Cyberveiligheidsbeleid en -normen**: deze cluster meet de capaciteit van de lidstaten om goed beleid en goede normen en praktijken op het gebied van cyberbeveiliging tot stand te brengen. Hierbij wordt rekening gehouden met verschillende aspecten van cyberdefensie en veerkracht, terwijl de ontwikkeling van de nationale cyberbeveiligingssector wordt ondersteund en het vertrouwen in overheden wordt opgebouwd;
- **(II) Capaciteitsopbouw en bewustmaking**: deze cluster beoordeelt de capaciteit van de lidstaten om bewustzijn te creëren voor cyberbeveiligingsrisico's en -dreigingen en voor het aanpakken van deze risico's. Bovendien wordt hierbij het vermogen gemeten van het land om voortdurend cyberbeveiligingscapaciteiten op te bouwen en de globale kennis en vaardigheden in dit verband te verhogen. De cluster richt zich op de ontwikkeling van de cyberbeveiligingsmarkt en de vooruitgang in O&O op het gebied van cyberbeveiliging. Deze cluster groepeert alle doelstellingen die de basis leggen voor het bevorderen van capaciteitsopbouw;
- **(III) Wet- en regelgeving**: deze cluster meet het vermogen van de lidstaten om de nodige wet- en regelgevingsinstrumenten in te voeren om de toename van

cybercriminaliteit en gerelateerde cyberincidenten aan te pakken en tegen te gaan, en om kritieke informatie-infrastructuur te beschermen. Daarnaast wordt ook het vermogen beoordeeld van de lidstaten om een rechtskader tot stand te brengen dat burgers en bedrijven beschermt, bijvoorbeeld bij het vinden van het juiste evenwicht tussen veiligheid en privacy; en

- **(IV) Samenwerking:** deze cluster evalueert de samenwerking en informatie-uitwisseling tussen verschillende groepen belanghebbenden op nationaal en internationaal niveau als een belangrijk instrument om een beter inzicht te krijgen in en te reageren op een voortdurend veranderende dreigingsomgeving.

De doelstellingen die in het model zijn opgenomen, zijn de doelstellingen die gewoonlijk door de lidstaten worden aangenomen, en zij werden gekozen uit de doelstellingen in paragraaf 2.2. Het model beoordeelt met name de volgende doelstellingen:

- 1. Ontwikkelen van nationale cybernoodplannen (I)
- 2. Opstellen van basisbeveiligingsmaatregelen (I)
- 3. Beveiligen van de digitale identiteit en opbouwen van vertrouwen in digitale overheidsdiensten (I)
- 4. Opzetten van een incidentresponscapaciteit (II)
- 5. Vergroten van bewustzijn onder gebruikers (II)
- 6. Organiseren van cyberbeveiligingsoefeningen (II)
- 7. Uitbreiden van onderwijs- en opleidingsprogramma's (II)
- 8. Bevorderen van O&O (II)
- 9. Bieden van stimulansen voor de private sector om te investeren in beveiligingsmaatregelen (II)
- 10. Verbeteren van de cyberbeveiliging van de toeleveringsketen (II)
- 11. Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners (III)
- 12. Aanpakken van cybercriminaliteit (III)
- 13. Ontwikkelen van mechanismen voor het melden van incidenten (III)
- 14. Versterken van privacy- en gegevensbescherming (III)
- 15. Institutionele samenwerking tussen openbare instanties (IV)
- 16. Deelnemen aan internationale samenwerking (IV)
- 17. Opzetten van een publiek-privaat partnerschap (IV)

De vier clusters en onderliggende doelstellingen worden in het model gecombineerd om een holistisch beeld te krijgen van de maturiteit van de cyberbeveiligingscapaciteiten van de lidstaten. Figuur 1 presenteert de overkoepelende structuur van het zelfbeoordelingskader en laat zien hoe deze elementen, namelijk de doelstellingen, de clusters en het zelfbeoordelingskader, gekoppeld zijn aan het evalueren van de prestaties van een land.

Figuur 1: Structuur van het zelfbeoordelingskader

Voor elke doelstelling binnen het zelfbeoordelingskader is er een reeks indicatoren, verdeeld over de vijf maturiteitsniveaus. Elke indicator is gebaseerd op een dichotome (ja/nee-) vraag. De indicator kan een vereiste of een niet-vereiste zijn.

3.4 SCORINGSSYSTEEM

Het **scoringssysteem** van het zelfbeoordelingskader houdt rekening met de bovengenoemde elementen en met de in paragraaf 3.5 genoemde principes. Het model geeft een score op basis van de waarde van twee parameters, het **maturiteitsniveau** en de **dekkingsgraad**. Elk van deze parameters kan worden berekend op verschillende niveaus: (i) per doelstelling, (ii) per cluster van doelstellingen of (iii) globaal.

Scores op doelstellingsniveau

De **score voor het maturiteitsniveau** geeft een beeld van het maturiteitsniveau en laat zien welke capaciteiten en praktijken zijn uitgevoerd. De score voor het maturiteitsniveau wordt berekend als het hoogste niveau waarvoor de respondent aan alle vereisten heeft voldaan (d.w.z. antwoord JA op alle vereiste vragen), en hij bovendien aan alle vereisten van de vorige maturiteitsniveaus heeft voldaan.

De **dekkingsgraad** geeft de mate van dekking aan van alle indicatoren waarvoor het antwoord positief is, ongeacht hun niveau. Het is een aanvullende waarde die rekening houdt met alle indicatoren die een doelstelling meten. De dekkingsgraad wordt berekend als de verhouding tussen het totale aantal vragen binnen de doelstelling en het aantal vragen waarop het antwoord positief is.

Er zij op gewezen dat in de rest van het document het woord ***score*** wordt gebruikt om te verwijzen naar zowel de waarden van het maturiteitsniveau als die van de dekkingsgraad.

Figuur 2 – Scoringssysteem per doelstelling biedt een visualisatie van het in paragraaf 3.1 beschreven evaluatiesysteem, dat hieronder verder zal worden uitgewerkt.

Figuur 2: Scoringssysteem per doelstelling

Figuur 2 geeft een voorbeeld van hoe het maturiteitsniveaus per doelstelling wordt berekend. Er zij op gewezen dat de respondent aan alle vereisten van de eerste drie maturiteitsniveaus heeft voldaan, en slechts gedeeltelijk aan die van niveau 4. Vandaar dat de score aangeeft dat het ***maturiteitsniveau van de respondent Niveau 3 is voor de doelstelling "Organiseren van cyberbeveiligingsoefeningen"****.*

In het voorbeeld in Figuur 2 is het maturiteitsniveau van de doelstelling echter niet in staat de informatie vast te leggen die wordt verstrekt door de indicatoren die een positieve score hebben en boven Maturiteitsniveau 3 liggen. In dat geval kan de dekkingsgraad een overzicht geven van alle elementen die de respondent heeft uitgevoerd om die doelstelling te bereiken, ondanks zijn werkelijke maturiteitsniveau. In dit geval is de verhouding tussen het totale aantal vragen binnen de doelstelling en het aantal vragen waarop het antwoord positief is, gelijk aan 19/27, wat betekent dat ***de dekkingsgraad 70% is.***

Om de score aan te passen aan de specifieke kenmerken van de lidstaten en tegelijk een consistent overzicht mogelijk te maken, wordt de score bovendien berekend op basis van twee verschillende steekproeven op clusterniveau en globaal niveau:

- **Algemene scores:** één volledige steekproef die betrekking heeft op alle doelstellingen die deel uitmaken van de cluster of het globale kader (van 1 tot 17);
- **Specifieke scores:** één specifieke steekproef die alleen betrekking heeft op de door de lidstaat geselecteerde doelstellingen (deze stemmen doorgaans overeen met de doelstellingen van de NCSS van het specifieke land) binnen de cluster of binnen het globale kader.

Scores op clusterniveau

Het **algemene maturiteitsniveau van elke cluster** wordt berekend als het rekenkundig gemiddelde van het maturiteitsniveau van alle doelstellingen binnen die cluster.

Het **specifieke maturiteitsniveau van elke cluster** wordt berekend als het rekenkundig gemiddelde van het maturiteitsniveau van de doelstellingen binnen die cluster die de lidstaat

gekozen heeft te beoordelen (deze stemmen doorgaans overeen met de doelstellingen van de NCSS van het specifieke land).

Figuur 1 laat bijvoorbeeld zien dat de cluster (I) Cyberveiligheidsbeleid en -normen uit drie doelstellingen bestaat. Ervan uitgaande dat de respondent ervoor heeft gekozen alleen de eerste twee doelstellingen te beoordelen, maar niet de derde, en ervan uitgaande dat de eerste twee doelstellingen een maturiteitsniveau van respectievelijk 2 en 4 hebben, dan is het maturiteitsniveau van de cluster die alle doelstellingen in aanmerking neemt Niveau 2 (Cluster (I) algemeen maturiteitsniveau = (2+4)/3), terwijl het maturiteitsniveau van de cluster die alleen de door de beoordelaar geselecteerde specifieke doelstellingen in aanmerking neemt Niveau 3 is (Cluster (I) specifiek maturiteitsniveau = (2+4)/2).

De **algemene dekkingsgraad van elke cluster** wordt berekend als de verhouding tussen het totale aantal vragen binnen de cluster en het aantal vragen waarop het antwoord positief is.

De **specifieke dekkingsgraad van elke cluster** wordt berekend als de verhouding tussen het totale aantal vragen binnen de cluster met betrekking tot de doelstellingen die de lidstaat gekozen heeft te beoordelen (deze stemmen doorgaans overeen met de doelstellingen van de NCSS van het specifieke land) en het aantal vragen waarop het antwoord positief is.

Scores op globaal niveau

Het **globale algemene maturiteitsniveau van een land** wordt berekend als het rekenkundig gemiddelde van het maturiteitsniveau van alle doelstellingen binnen het kader, van 1 tot 17.

Het **globale specifieke maturiteitsniveau van een land** wordt berekend als het rekenkundig gemiddelde van het maturiteitsniveau van de doelstellingen binnen het kader die de lidstaat gekozen heeft te beoordelen (deze stemmen meestal overeen met de doelstellingen van de NCSS van het specifieke land).

De **globale algemene dekkingsgraad van een land** wordt berekend als de verhouding tussen het totale aantal vragen binnen alle doelstellingen die in het kader zijn opgenomen (van 1 tot 17) en het aantal vragen waarop het antwoord positief is.

De **globale specifieke dekkingsgraad van een land** wordt berekend als de verhouding tussen het totale aantal vragen binnen de doelstellingen binnen het kader die de lidstaat gekozen heeft te beoordelen (deze stemmen doorgaans overeen met de doelstellingen van de NCSS van het specifieke land) en het aantal vragen waarop het antwoord positief is.

Voor elke indicator kunnen de respondenten een derde optie “weet niet/niet van toepassing” als antwoord kiezen. In dat geval wordt de indicator buiten beschouwing gelaten bij de totale berekening van de resultaten.

De maturiteitsniveaus op clusterniveau en globaal niveau worden berekend met een rekenkundig gemiddelde om de vooruitgang tussen twee beoordelingen te tonen. Het alternatief, waarbij de maturiteitsniveaus op cluster- en globaal niveau worden gemeten als het maturiteitsniveau van de minst volwassen doelstelling – dat weliswaar relevant is vanuit maturiteitsoogpunt – kan immers geen verklaring bieden voor de vooruitgang die wordt geboekt op gebieden die onder andere doelstellingen vallen.

Aangezien het clusterniveau en het globale niveau voor rapportagedoeleinden worden geconsolideerd, is ervoor gekozen het rekenkundig gemiddelde te gebruiken. Gebruik voor een grotere nauwkeurigheid de scores op doelstellingsniveau voor rapportagedoeleinden.

Figuur 3 hieronder geeft een overzicht van de scoringssystemen op de verschillende niveaus van het model (doelstelling, cluster, globaal).

Figuur 3: Globaal scoringssysteem

3.5 VEREISTEN VOOR HET ZELFBEOORDELINGSKADER

Het in dit deel gepresenteerde beoordelingskader voor nationale capaciteiten is gebaseerd op de door de lidstaten aangegeven behoeften en is opgebouwd rond een reeks vereisten die hierna worden opgesomd:

- Het NCAF wordt door de lidstaat op vrijwillige basis gebruikt als zelfbeoordelingskader;
- Het NCAF beoogt de cyberbeveiligingscapaciteiten van de lidstaten te meten met betrekking tot de 17 doelstellingen. De lidstaat kan echter de doelstellingen kiezen die hij wil beoordelen en slechts een deel van de 17 doelstellingen beoordelen;
- Het zelfbeoordelingskader beoogt het maturiteitsniveau van de cyberbeveiligingscapaciteiten van de lidstaat te meten;
- De resultaten van de beoordeling worden niet bekendgemaakt, tenzij de lidstaat daartoe op eigen initiatief besluit;
- De lidstaat kan bij het weergeven van de beoordelingsresultaten het maturiteitsniveau van de cyberbeveiligingscapaciteiten van het land, van een cluster van doelstellingen of zelfs van één doelstelling presenteren;
- Alle beoordeelde doelstellingen zijn even relevant binnen het beoordelingskader en hebben daarom hetzelfde belang. Hetzelfde geldt voor de binnen het beoordelingskader gehanteerde indicatoren; en
- De lidstaat kan zijn vorderingen in de tijd volgen.

Het zelfbeoordelingskader beoogt de lidstaten te ondersteunen bij het opbouwen van cyberbeveiligingscapaciteiten, en omvat derhalve ook een reeks aanbevelingen of richtsnoeren die de Europese landen een leidraad moeten bieden bij het verbeteren van hun maturiteitsniveau.

Opmerking: deze aanbevelingen of richtsnoeren zijn algemeen en gebaseerd op ENISA-publicaties en lessen die uit andere landen zijn getrokken, en zullen afhangen van het resultaat van de zelfevaluatie.

4. NCAF-INDICATOREN

4.1 INDICATOREN VAN HET KADER

In deze paragraaf worden de indicatoren van het beoordelingskader voor nationale capaciteiten van Enisa gepresenteerd. De volgende paragrafen zijn georganiseerd per cluster.

Voor elke cluster wordt in een tabel de uitgebreide reeks indicatoren gepresenteerd in de vorm van vragen die representatief zijn voor een bepaald maturiteitsniveau. De vragenlijst is het belangrijkste instrument voor de zelfbeoordeling. Voor elke doelstelling moet nota worden genomen van twee reeksen indicatoren:

- een reeks generieke vragen over de maturiteit van de strategie (9 generieke vragen) - aangeduid met een letter van 'a' tot 'c' voor elk maturiteitsniveau - die herhaald worden voor elke doelstelling; en
- een reeks vragen over de cyberbeveiligingscapaciteit (319 vragen over de cyberbeveiligingscapaciteit) - genummerd van 1 tot 10 voor elk maturiteitsniveau - die specifiek zijn voor het gebied waarop de doelstelling betrekking heeft.

Elke vraag wordt voorzien van een label (0-1) dat aangeeft of de vraag een vereiste-indicator (1) of een niet-vereiste-indicator (0) is voor het maturiteitsniveau.

Elke vraag kan worden geïdentificeerd aan de hand van een identificatienummer dat bestaat uit:

- het doelstellingsnummer;
- het maturiteitsniveau; en
- het vraagnummer.

Vraag ID 1.2.4 is bijvoorbeeld de vierde vraag binnen maturiteitsniveau 2 van de strategische doelstelling (I) “Ontwikkelen van nationale cybernoodplannen”.

Er zij op gewezen dat de vragen in de vragenlijst betrekking hebben op het nationale niveau, tenzij anders vermeld. In alle vragen verwijst het voornaamwoord “U” naar de lidstaat in algemene zin en niet naar de persoon of de overheidsinstantie die de beoordeling uitvoert.

De definitie van elke doelstelling is te vinden in hoofdstuk 2.2 – Gemeenschappelijke doelstellingen in het kader van de Europese nationale cyberbeveiligingsstrategieën.

4.1.1 Cluster 1: Cyberveiligheidsbeleid en -normen

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
1 – Ontwikkelen van nationale cybernoodplannen	a	Behandelt u de doelstelling in uw huidige NCSS of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en een duidelijk beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Bent u begonnen met het opstellen van nationale cybernoodplannen? Bijvoorbeeld het vaststellen van de algemene doelstellingen, het toepassingsgebied en/of de beginselen van de noodplannen.	1	Beschikt u over een doctrine/nationale strategie waarin cyberbeveiliging als crisisfactor is opgenomen (d.w.z. een blauwdruk, een beleid, enz.)?	1	Beschikt u over een nationaal plan voor cybercrisisbeheer?	1	Bent u tevreden over het aantal of het percentage kritieke sectoren dat in het nationale cybernoodplan is opgenomen?	1	Beschikt u over een proces om lering te trekken uit cyberoefeningen of feitelijke crises op nationaal niveau?	1
	2	Wordt algemeen begrepen dat cyberincidenten een crisisfactor vormen die de nationale veiligheid kan bedreigen?	0	Beschikt u over een hub om informatie in te winnen en besluitvormers te informeren? Dat wil zeggen methoden, platforms of locaties om ervoor te zorgen dat alle crisisresponsactoren toegang hebben tot dezelfde, real-time informatie over de cybercrisis.	1	Beschikt u op nationaal niveau over specifieke procedures voor cybercrisisbeheer?	1	Organiseert u regelmatig activiteiten (d.w.z. oefeningen) met betrekking tot nationale cybernoodplanning?	1	Beschikt u over een proces om het nationale plan regelmatig te testen?	1
	3	Zijn er studies (technische, operationele, politieke) uitgevoerd op het gebied van cybernoodplanning?	0	Worden de relevante middelen ingezet om toe te zien op de ontwikkeling en uitvoering van nationale cybernoodplannen?	1	Beschikt u over een communicatieteam dat speciaal is opgeleid om te reageren op cybercrises en om het publiek te informeren?	1	Beschikt u over voldoende mensen die zich bezighouden met crisisplanning, het bestuderen van de getrokken lessen en het doorvoeren van veranderingen?	1	Beschikt u over adequate instrumenten en platforms om situationeel bewustzijn op te bouwen?	1
	4	-		Beschikt u op nationaal niveau over een methode voor de beoordeling van cyberdreigingen, met inbegrip van procedures voor effectbeoordeling?	0	Betrekt u alle relevante nationale belanghebbenden (nationale veiligheid, defensie, civiele bescherming, wetshandhaving, ministeries, autoriteiten enz.) bij het proces?	1	Beschikt u over voldoende opgeleide personen om te reageren op cybercrises op nationaal niveau?	1	Volgt u een specifiek maturiteitsmodel om het cybernoodplan te controleren en te verbeteren?	0

	5	-		-		Beschikt u over adequate faciliteiten voor crisisbeheer en crisiskamers?	1	-		Beschikt u over middelen die specifiek anticiperen op bedreigingen of die werken aan prospectieve cyberbeveiliging om toekomstige crises of toekomstige uitdagingen aan te pakken?	0
	6	-		-		Werkt u, indien nodig, samen met internationale belanghebbenden in de EU?	0	-		-	
	7	-		-		Werkt u, indien nodig, samen met internationale belanghebbenden in niet-EU-landen?	0	-		-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
2 – Opstellen van basisbeveiligingsmaatregelen	a	Behandelt u de doelstelling in uw huidige NCSS of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u een studie uitgevoerd om de vereisten en lacunes voor **publieke** organisaties te identificeren op basis van internationaal erkende normen, bv . ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS enz.?	1	Zijn de getroffen veiligheidsmaatregelen in overeenstemming met internationale/nationale normen?	1	Zijn basisbeveiligingsmaatregelen verplicht?	1	Is er een proces om de basisbeveiligingsmaatregelen regelmatig bij te werken?	1	Beschikt u over een proces om ICT te versterken wanneer incidenten niet door de maatregelen worden verholpen?	1

	2	Hebt u een studie uitgevoerd om de vereisten en lacunes voor **particuliere** organisaties te identificeren op basis van internationaal erkende normen, bv . ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS enz.?	1	Worden de particuliere sector en andere belanghebbenden geraadpleegd bij het vaststellen van de basisveiligheidsmaatregelen?	1	Implementeert u horizontale beveiligingsmaatregelen in kritieke sectoren?	1	Bestaat er een controlemechanisme om na te gaan in hoeverre basisbeveiligingsmaatregelen worden toegepast?	1	Evalueert u de relevantie van nieuwe normen die worden ontwikkeld in reactie op de laatste ontwikkelingen in het bedreigingslandschap?	1
	3	-		-		Implementeert u sectorspecifieke beveiligingsmaatregelen in kritieke sectoren?	1	Is er een nationale autoriteit die controleert of de basisbeveiligingsmaatregelen al dan niet worden nageleefd?	1	Hebt of bevordert u een nationaal gecoördineerd proces voor de bekendmaking van kwetsbaarheden (coordinated vulnerability disclosure – CVD)?	1
	4	-				Zijn de basisbeveiligingsmaatregelen in overeenstemming met de relevante certificeringsregelingen?	1	Beschikt u over een proces om binnen een specifiek tijdsbestek niet-conforme organisaties te identificeren?	1	-	
	5	-		-		Bestaat er een proces voor zelfbeoordeling van risico's in verband met basisbeveiligingsmaatregelen?	1	Bestaat er een auditproces om ervoor te zorgen dat de beveiligingsmaatregelen correct worden toegepast?	1	-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
2 – Opstellen van basisbeveiligingsmaatregelen	6	-		-		Evalueert u verplichte basisbeveiligingsmaatregelen in het aanbestedingsproces van overheidsinstanties?	0	Stelt u veilige normen vast voor de ontwikkeling van kritieke IT/OT-producten (medische apparatuur, geconnecteerde en autonome voertuigen, professionele radioapparatuur, apparatuur voor de zware industrie) of moedigt u de toepassing ervan actief aan?	0	-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
3 – Beveiligen van de digitale identiteit en opbouwen van vertrouwen in digitale overheidsdiensten	a	Behandelt u de doelstelling in uw huidige NCSS, of bent u van plan dat in de volgende editie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1

	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u studies of 'gapanalyses' uitgevoerd voor het vaststellen van de behoeften om digitale overheidsdiensten voor burgers en bedrijven te beveiligen?	1	Voert u risicoanalyses uit om het risicoprofiel van de activa of diensten te bepalen alvorens ze naar de cloud te verplaatsen of om digitale-transformatieprojecten uit te voeren?	1	Bevordert u privacy-door-ontwerpmethoden in alle e-overheidsprojecten?	1	Verzamelt u indicatoren over cyberbeveiligingsincidenten met inbreuken op digitale overheidsdiensten?	1	Neemt u deel aan Europese werkgroepen om normen te handhaven en/of nieuwe eisen te ontwerpen voor elektronische vertrouwensdiensten (elektronische handtekeningen, elektronische zegels, aangetekende elektronische bezorgdiensten, tijdstempels, website-authenticatie)? Bv. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU enz.	1
	2	-		Hebt u een strategie om veilige nationale elektronische identificatiesystemen (eID's) voor burgers en bedrijven te ontwikkelen of te bevorderen?	1	Betrekt u particuliere belanghebbenden bij het ontwerpen en leveren van veilige digitale overheidsdiensten?	1	Hebt u met andere lidstaten een wederzijdse erkenning van e-identificatiemiddelen uitgevoerd?	1	Neemt u actief deel aan peer reviews in het kader van de aanmelding van eID-regelingen bij de Europese Commissie?	1
	3	-		Hebt u een strategie om veilige nationale elektronische vertrouwensdiensten (elektronische handtekeningen, elektronische zegels, aangetekende elektronische bezorgdiensten, tijdstempels, website-authenticatie) voor burgers en bedrijven op te zetten of te bevorderen?	1	Implementeert u een minimumbeveiligingsbasis voor alle digitale overheidsdiensten?	1	-		-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
3 – Beveiligen van de digitale identiteit en opbouwen van vertrouwen in digitale overheidsdiensten	4	-		Beschikt u over een strategie voor nationale cloud computing (een cloud computing-strategie die gericht is op de overheid en overheidsinstanties zoals ministeries, overheidsinstanties en overheidsadministraties enz.) waarin rekening wordt gehouden met de beveiligingsimplicaties?	0	Zijn er elektronische-identificatiesystemen beschikbaar voor burgers en bedrijven met een aanzienlijk of hoog betrouwbaarheidsniveau, zoals gedefinieerd in de bijlage bij eIDAS (Verordening (EU) nr. 910/2014)?	1	-		-	

	5	-		-		Beschikt u over digitale overheidsdiensten die elektronische identificatiesystemen vereisen met een substantieel of hoog betrouwbaarheidsniveau, zoals gedefinieerd in de bijlage bij eIDAS (Verordening (EU) nr. 910/2014)?	1	-		-	
	6	-		-		Beschikt u over aanbieders van vertrouwensdiensten voor burgers en bedrijven (elektronische handtekeningen, elektronische zegels, aangetekende elektronisch bezorgdiensten, tijdstempels, authenticatie van websites)?	1	-		-	
	7	-		-		Bevordert u de invoering van basisbeveiligingsmaatregelen voor alle cloud-implementatiemodellen (bv. privaat, publiek, hybride, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Cluster 2: Capaciteitsopbouw en bewustmaking

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
4 – Opzetten van een incidentresponscapaciteit	a	Behandelt u de doelstelling in uw huidige NCSS, of bent u van plan dat in de volgende editie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Beschikt u over een informele incidentresponscapaciteit die binnen of tussen publieke en private sectoren wordt beheerd?	1	Beschikt u over ten minste één officieel nationaal CSIRT?	1	Beschikt u over incidentresponscapaciteiten voor de in bijlage II bij de NIS-richtlijn genoemde sectoren?	1	Hebt u gestandaardiseerde praktijken voor incidentresponsprocedures en incidentclassificatieschema's vastgesteld en bevorderd?	1	Beschikt u over mechanismen voor vroegtijdige opsporing, identificatie, preventie, reactie en beperking van zerodaykwetsbaarheden?	1
	2	-		Heeft (hebben) uw nationale CSIRT('s) een duidelijk omschreven actieterrein? Bv. afhankelijk van de beoogde sector, de soorten incidenten, de gevolgen.	1	Bestaat er in uw land een CSIRT-samenwerkingsmechanisme om te reageren op incidenten?	1	Evalueert u uw incidentresponscapaciteit om te garanderen dat u over de nodige middelen en vaardigheden beschikt om de taken van bijlage I, punt 2, bij de NIS-richtlijn uit te voeren?	1	-	
	3	-		Heeft (hebben) uw nationale CSIRT('s) duidelijk omschreven relaties met andere nationale belanghebbenden wat betreft het nationale cyberbeveiligingslandschap en praktijken in verband met incident response (bv. LEA, defensie, ISP's, NCSC)?	0	Beschikt (beschikken) uw nationale CSIRT('s) over een incidentresponscapaciteit overeenkomstig bijlage I bij de NIS-richtlijn? *D.w.z.* beschikbaarheid, fysieke beveiliging, bedrijfscontinuïteit, internationale samenwerking, monitoring van incidenten, capaciteit voor vroegtijdige waarschuwing en alarmmeldingen, reageren op incidenten, risicoanalyse en situationeel bewustzijn, samenwerking met de particuliere sector, standaardpraktijken ...	1	-		-	

	4	-				Bestaat er een mechanisme voor samenwerking met andere buurlanden in verband met incidenten?	1	-		-	
	5	-		-		Beschikt u over formeel vastgestelde duidelijke beleidsregels en procedures voor incidentenbehandeling?	1	-		-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
4 – Een incidentresponscapaciteit opzetten	6	-		-		Neemt (nemen) uw nationale CSIRT('s) deel aan cyberbeveiligingsoefeningen op zowel nationaal als internationaal niveau?	1	-		-	
	7	-		-		Is (zijn) uw nationale CSIRT('s) aangesloten bij FIRST (Forum of Incident Response and Security Teams)?	0	-		-	

NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
5 – Vergroten van bewustzijn onder gebruikers	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende editie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Is er een minimale erkenning door de overheid, de particuliere sector of de algemene gebruikers dat er nood is aan het creëren van bewustzijn voor cyberbeveiliging en privacykwesties?	1	Hebt u een specifieke doelgroep vastgesteld voor het bewust maken van gebruikers? Bv. algemene gebruikers, jongeren, zakelijke gebruikers (die verder kunnen worden uitgesplitst: kmo's, aanbieders van essentiële diensten, digitaledienstverleners enz.).	1	Hebt u communicatieplannen/strategieën voor de campagnes ontwikkeld?	1	Ontwikkelt u in de planningsfase meetwaarden voor de evaluatie van uw campagne?	1	Beschikt u over mechanismen om ervoor te zorgen dat bewustmakingscampagnes voortdurend relevant zijn voor de technologische vooruitgang, veranderingen in het bedreigingslandschap, wettelijke voorschriften en nationale beveiligingsrichtlijnen?	1

	2	Voeren overheidsinstanties binnen hun organisatie op ad-hocbasis bewustmakingscampagnes op het gebied van cyberbeveiliging, bijvoorbeeld naar aanleiding van een cyberbeveiligingsincident?	0	Stelt u een projectplan op om bewustzijn te creëren voor informatiebeveiliging en privacykwesties?	1	Hebt u een proces voor het creëren van inhoud op overheidsniveau?	1	Evalueert u uw campagnes na de uitvoering?	1	Voert u periodieke evaluaties of studies uit om de attitudeverandering of gedragsverandering met betrekking tot cyberbeveiliging en privacykwesties in particuliere en publieke sectoren te meten?	1
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
5 – Vergroten van bewustzijn onder gebruikers	3	Voeren overheidsinstanties op ad-hocbasis bewustmakingscampagnes over cyberbeveiliging voor het grote publiek? Bv. in de nasleep van een cyberbeveiligingsincident.	0	Beschikt u over middelen die gemakkelijk herkenbaar zijn (bv. één onlineportaal, bewustmakingskits) voor gebruikers die meer willen weten over kwesties op het gebied van cyberbeveiliging en privacy?	1	Beschikt u over mechanismen om doelgebieden voor het creëren van bewustzijn vast te stellen (d.w.z. Enisa-bedreigingslandschap, nationale landschappen, internationale landschappen, feedback van nationale cybercriminaliteitscentra, enz.)?	1	Beschikt u over mechanismen om, afhankelijk van het doelpubliek, de meest relevante media- of communicatiekanalen te identificeren om het toepassingsgebied en de betrokkenheid te maximaliseren? Bv. verschillende soorten digitale media, brochures, e-mails, pedagogisch materiaal, posters in drukke gebieden, TV, radio enz.	1	Overlegt u met gedragsdeskundigen om uw campagne af te stemmen op het doelpubliek?	1
	4	-		-		Brengt u belanghebbenden met deskundigen en communicatieteams samen om inhoud te creëren?	1			-	
	5	-		-		Betrekt u de particuliere sector bij uw bewustmakingsinspanningen om de boodschappen te promoten en onder een breder publiek te verspreiden?	1	-		-	
	6	-		-		Ontwikkelt u specifieke bewustmakingsinitiatieven ten behoeve van leidinggevenden in de openbare, de particuliere, de academische of de civiele sector?	1	-		-	
	7	-		-		Neemt u deel aan de European Cybersecurity Month-campagnes van Enisa (ECSM)?	0	-		-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
6 – Cyberbeveiligingsoefeningen organiseren	a	Behandelt u de doelstelling in uw huidige NCSS of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Houdt u crisisoefeningen in andere sectoren (andere dan cyberbeveiliging) op nationaal of pan-Europees niveau?	1	Hebt u een oefenprogramma voor cyberbeveiliging op nationaal niveau?	1	Betrekt u alle betrokken overheidsinstanties bij de zaak? (zelfs als het scenario sectorspecifiek is)	1	Schrijft u na het voltooien van de oefening evaluatierapporten?	1	Beschikt u over een capaciteit voor het analyseren van lessen die werden geleerd op cybergebied (rapportageprocessen, analyse, mitigatie)?	1
	2	Wijst u middelen toe aan het ontwerpen en plannen van crisisbeheersingsoefeningen?	1	Voert u cybercrisisbeheersingsoefeningen uit met betrekking tot vitale maatschappelijke functies en kritieke infrastructuur, of prioriteert u zulke oefeningen?	1	Betrekt u de particuliere sector bij de planning en uitvoering van de oefeningen?	1	Test u plannen en procedures op nationaal niveau?	1	Beschikt u over een proces om lering te trekken uit de opgedane ervaring?	1
6 – Cyberbeveiligingsoefeningen organiseren	3	-		Hebt u een coördinerende instantie aangewezen om toezicht te houden op het ontwerpen en plannen van cyberbeveiligingsoefeningen (overheidsinstantie, consultancy)?	0	Organiseert u sectorspecifieke oefeningen op nationaal en/of internationaal niveau?	1	Neemt u deel aan cyberbeveiligingsoefeningen op pan-Europees niveau?	1	Past u de oefenscenario's aan naar gelang van de laatste ontwikkelingen (technologische vooruitgang, wereldwijde conflicten, bedreigingslandschap)?	1
	4	-		-		Organiseert u oefeningen in alle in bijlage II bij de NIS-richtlijn vermelde kritieke sectoren?	1	-		Stemt u uw crisisbeheersingsprocedures af op die van andere lidstaten om een doeltreffend pan-Europees crisisbeheer te waarborgen?	1
	5	-		-		Organiseert u intersectorale en/of sectoroverschrijdende cyberbeveiligingsoefeningen?	1	-		Beschikt u over een mechanisme om de strategie, plannen en procedures snel aan te passen aan de hand van de lessen die tijdens de oefeningen zijn geleerd?	0

	6	-		-		Organiseert u cyberbeveiligingsoefeningen die specifiek zijn voor verschillende niveaus? (technisch en operationeel niveau, procedureniveau, besluitvormingsniveau, politiek niveau)	0	-		-

NCSS-doelstelling	#	Level 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
7 – Uitbreiden van onderwijs- en opleidingsprogramma's	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Overweegt u opleidings- en onderwijsprogramma's op het gebied van cyberbeveiliging te ontwikkelen?	1	Stelt u cursussen over cyberbeveiliging samen?	1	Integreert uw land reeds in een vroeg stadium van het onderwijstraject een cultuur van cyberbeveiliging? Bevordert u bijvoorbeeld cyberbeveiliging op de middelbare school?	1	Dringt u erop aan dat het personeel in de private en publieke sector geaccrediteerd of gecertificeerd is?	1	Beschikt u over mechanismen om ervoor te zorgen dat opleidings- en onderwijscampagnes voortdurend relevant zijn voor de huidige en opkomende technologische vooruitgang, veranderingen in het bedreigingslandschap, wettelijke voorschriften en nationale beveiligingsrichtlijnen?	1
	2	-		Bieden universiteiten in uw land doctoraten in cyberbeveiliging aan als een zelfstandige discipline en niet als een vak in de informatica?	1	Beschikt u over nationale onderzoekslaboratoria en onderwijsinstellingen die gespecialiseerd zijn in cyberbeveiliging?	1	Heeft uw land opleidings- of mentorschapsprogramma's op het gebied van cyberbeveiliging ontwikkeld om nationale start-ups en kmo's te ondersteunen?	1	Richt u academische expertisecentra op het gebied van cyberbeveiliging op die als centra voor onderzoek en onderwijs fungeren?	1
	3	-		Bent u van plan docenten, los van hun vakgebied, op te leiden in informatiebeveiliging en privacykwesties, bijvoorbeeld onlinebeveiliging, bescherming van persoonsgegevens, cyberpesten?	1	Stimuleert/financiert u speciale cursussen of opleidingen in cyberbeveiliging voor werknemers van arbeidsbureaus in de lidstaten?	1	Bevordert u actief de toevoeging van cursussen informatiebeveiliging in het hoger onderwijs, niet alleen voor studenten computerwetenschappen, maar ook voor andere beroepsspecialismen? Bv . cursussen die zijn toegesneden op de behoeften van dat beroep.	1	Nemen academische instellingen deel aan toonaangevende discussies op het gebied van onderwijs en onderzoek inzake cyberbeveiliging op internationaal niveau?	0
	4	-		-		Beschikt u over cursussen en/of een gespecialiseerd curriculum cyberbeveiliging voor niveau 5 tot 8 van het EKK (Europees kwalificatiekader)?	1	Evalueert u regelmatig de vaardigheidskloof (tekort aan cyberbeveiligers) op het gebied van informatiebeveiliging?	1	-	

	5	-		-		Stimuleert en/of steunt u initiatieven om cursussen over veilig internetgebruik op te nemen in het lager en middelbaar onderwijs?	1	Bevordert u de vorming van netwerken en de uitwisseling van informatie tussen academische instellingen, zowel op nationaal als op internationaal niveau?	1		
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
7 - Uitbreiden van onderwijs- en opleidingsprogramma's	6	-		-		Financiert u basiscursussen cyberbeveiliging voor burgers of biedt u deze gratis aan?	0	Betrekt u de private sector op enigerlei wijze bij onderwijsinitiatieven op het gebied van cyberbeveiliging, bijvoorbeeld bij het ontwerpen en geven van cursussen, stages enz.	1	-	
	7	-		-		Organiseert u jaarlijkse evenementen rond informatiebeveiliging (bv. hackwedstrijden of hackathons)?	0	Implementeert u financieringsmechanismen om de invoering van cyberbeveiligingsdiploma's aan te moedigen? Bv. studiebeurzen, gegarandeerde stageplaatsen, gegarandeerde banen in specifieke sectoren of functies in de publieke sector.	0	-	

NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
8 – Bevorderen van O&O	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						

	1	Hebt u studies of analyses uitgevoerd om de O&O-prioriteiten op het gebied van cyberbeveiliging te bepalen?	1	Beschikt u over een proces om O&O-prioriteiten te bepalen (bv. opkomende onderwerpen voor het afschrikken van, beschermen tegen, opsporen van en aanpassen aan nieuwe soorten cyberaanvallen)?	1	Is er een plan om O&O-initiatieven te koppelen aan de reële economie?	1	Zijn de O&O-initiatieven op het gebied van cyberbeveiliging in overeenstemming met de relevante strategische doelstellingen, zoals DSM, H2020, Digitaal Europa, de EU-strategie inzake cyberbeveiliging?	1	Streeft u op nationaal niveau naar samenwerking met internationale O&O-initiatieven op het gebied van cyberbeveiliging?	1
	2	-		Is de particuliere sector betrokken bij de vaststelling van O&O-prioriteiten?	1	Bestaan er nationale projecten op het gebied van cyberbeveiliging?	1	Bestaat er een evaluatieregeling voor O&O-initiatieven?	1	Zijn de O&O-prioriteiten afgestemd op de huidige of toekomstige regelgeving (op nationaal niveau)?	1
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
8 – Bevorderen van O&O	3	-		Is de academische wereld betrokken bij de vaststelling van O&O-prioriteiten?	1	Beschikt u over lokale/regionale startup-ecosystemen en andere netwerkkanalen (bv. technologieparken, innovatieclusters, netwerkevenementen/platforms) om innovatie te bevorderen (ook voor start-ups op het gebied van cyberbeveiliging)?	1	Bestaan er samenwerkingsovereenkomsten met universiteiten en andere onderzoeksfaciliteiten?	1	Neemt u deel aan toonaangevende discussies over een of meer innovatieve O&O-thema's op internationaal niveau?	0
	4	-		Bestaan er nationale O&O-initiatieven op het gebied van cyberbeveiliging?	0	Wordt er in de academische wereld en de particuliere sector geïnvesteerd in O&O-programma's op het gebied van cyberbeveiliging?	1	Is er een erkend institutioneel orgaan dat toezicht houdt op de O&O-activiteiten op het gebied van cyberbeveiliging?	0	-	
	5	-		-		Zijn er leerstoelen voor industrieel onderzoek aan universiteiten om een brug te slaan tussen onderzoeksonderwerpen en marktbehoeften?	1	-		-	
	6	-		-		Hebt u speciale financieringsprogramma's voor O&O op het gebied van cyberbeveiliging?	0	-		-	

NCSS-doelstelling	#	Level 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
9 – Bieden van stimulansen voor de private sector om te investeren in beveiligingsmaatregelen	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Is er een industrieel beleid of politieke wil om de ontwikkeling van de cyberbeveiligingssector aan te moedigen?	1	Is de particuliere sector betrokken bij het ontwerpen van stimulansen?	1	Bestaan er economische/regelgevende of andersoortige stimulansen om investeringen in cyberbeveiliging te bevorderen?	1	Zijn er particuliere actoren die op stimulansen reageren door in beveiligingsmaatregelen te investeren? Bv. in cyberbeveiliging gespecialiseerde investeerders en niet-gespecialiseerde investeerders.	1	Stelt u uw stimulansen voor cyberbeveiliging afhankelijk van de nieuwste ontwikkelingen op het gebied van bedreigingen?	1
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
9 – Bieden van stimulansen voor de private sector om te investeren in beveiligingsmaatregelen	2	-		Hebt u specifieke onderwerpen in verband met cyberbeveiliging geïdentificeerd die verder ontwikkeld moeten worden? Bv. cryptografie, privacy, nieuwe vorm van authenticatie, AI voor cyberbeveiliging enz.	0	Biedt u ondersteuning (bv. fiscale stimulansen) voor start-ups en kmo's?	1	Biedt u de particuliere sector stimulansen om zich te richten op de beveiliging van geavanceerde technologieën, bv. 5G, kunstmatige intelligentie, IoT, quantumcomputing?	1	-	
	3	-		-		Biedt u fiscale stimulansen of andere financiële prikkels voor particuliere investeerders in startende cyberbeveiligingsbedrijven?	1	-		-	
	4	-		-		Vergemakkelijkt u de toegang voor startende cyberbeveiligingsbedrijven en kmo's bij openbareaanbestedingsprocedures?	0	-		-	
	5	-		-		Is er budget beschikbaar om stimulansen te bieden aan de particuliere sector?	0	-		-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
10 – De cyberbeveiliging van de toeleveringsketen verbeteren	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen tot het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u een studie verricht naar goede praktijken op het gebied van beveiliging voor het beheer van de toeleveringsketen die bij aanbestedingen in diverse sectorsegmenten en/of in de publieke sector worden toegepast?	1	Voert u cyberbeveiligingsbeoordelingen uit in de hele toeleveringsketen van ICT-diensten en -producten in kritieke sectoren (zoals geïdentificeerd in bijlage II bij de NIS-richtlijn (2016/1148))?	1	Maakt u gebruik van een beveiligingscertificeringsregeling voor op ICT gebaseerde producten en diensten? Bv. SOG-IS MRA in Europa (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement), Common Criteria Recognition Arrangement (CCRA), nationale initiatieven, sectorale initiatieven.	1	Beschikt u over een proces om de cyberbeveiligingsbeoordelingen van de toeleveringsketen van ICT-diensten en -producten in kritieke sectoren (zoals geïdentificeerd in bijlage II bij de NIS-richtlijn (2016/1148)) te actualiseren?	1	Beschikt u over opsporingsinstrumenten in belangrijke onderdelen van de toeleveringsketen om vroegtijdige kenmerken van compromissen op te sporen? Bv. beveiligingscontroles op ISP-niveau, beveiligingsinstrumenten in belangrijke infrastructuurcomponenten.	1

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
10 – De cyberbeveiliging van de toeleveringsketen verbeteren	2	-		Past u normen toe in het inkoopbeleid van overheidsadministraties om ervoor te zorgen dat leveranciers van ICT-producten of -diensten voldoen aan basisvereisten op het gebied van informatiebeveiliging, bv. ISO/IEC 27001 en 27002, ISO/IEC 27036?	1	Bevordert u actief de toepassing van beste praktijken op het gebied van beveiliging en Privacy by Design in de ontwikkeling van ICT-producten en -diensten, bv. veilige softwareontwikkelingscyclus, IoT-levenscyclus?	1	Beschikt u over een proces om zwakke schakels op het gebied van cyberbeveiliging in de toeleveringsketen van kritieke sectoren (zoals geïdentificeerd in bijlage II bij de NIS-richtlijn (2016/1148) op te sporen?	1	-	
	3	-		-		Ontwikkelt en verstrekt u een gecentraliseerde catalogus met uitgebreide informatie van bestaande informatiebeveiligings- en privacynormen die schaalbaar zijn voor en toepasbaar zijn door kmo's?	1	Beschikt u over mechanismen om ervoor te zorgen dat ICT-producten en -diensten die van kritiek belang zijn voor aanbieders van essentiële diensten, cyberbestendig zijn(d.w.z. dat zij beschikbaar en veilig kunnen blijven in geval van een cyberincident), bv. door middel van tests, regelmatige evaluaties, detectie van gecompromitteerde elementen.	1	-	
	4	-				Neemt u actief deel aan het ontwerp van een EU-certificeringskader voor digitale ICT-producten, -diensten en -processen, zoals vastgesteld in de EU-cyberbeveiligingsverordening (Verordening (EU) 2019/881)? Bv. deelname aan de European Cybersecurity Certification Group (ECCG), bevordering van technische normen en procedures voor de beveiliging van ICT-producten/diensten.	0	Bevordert u de ontwikkeling van certificeringsregelingen voor kmo's om de invoering van informatiebeveiligings- en privacynormen te stimuleren?	0	-	
	5	-		-		Biedt u bepaalde stimulansen voor kmo's om beveiligings- en privacynormen in te voeren?	0	Hebt u gezorgd voor voorzieningen om grote ondernemingen aan te moedigen de cyberbeveiliging van kleine ondernemingen in hun toeleveringsketens te verbeteren? Bv. een cyberbeveiligingshub, opleidings- en bewustmakingscampagnes.	0	-	

	6	-		-		Moedigt u softwareleveranciers aan kmo's te ondersteunen door te zorgen voor veilige standaardconfiguraties in producten die bestemd zijn voor kleine organisaties?	0	-		-	

4.1.3 Cluster 3: Wet- en regelgeving

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
11 – Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Bestaat er algemeen overeenstemming dat CII-operatoren bijdragen aan de nationale veiligheid?	1	Beschikt u over een methode om essentiële diensten te identificeren?	1	Hebt u de NIS-richtlijn (2016/1148) uitgevoerd?	1	Beschikt u over een procedure om het risicoregister te actualiseren?	1	Maakt en actualiseert u bedreigingslandschapsrapporten?	1

	2	-		Beschikt u over een methode voor de identificatie van CII's?	1	Hebt u uitvoering gegeven aan de ECI-richtlijn (2008/114) inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren?	1	Beschikt u over andere mechanismen om te meten of de technische en organisatorische maatregelen die door aanbieders van essentiële diensten worden uitgevoerd geschikt zijn om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheren? Bv. regelmatige cyberbeveiligingsaudits, een nationaal kader voor de implementatie van standaardmaatregelen, technische instrumenten die door de overheid ter beschikking worden gesteld, zoals detectiesondes of systeemspecifieke configuratiebeoordelingen.	1	Bent u, afhankelijk van de laatste ontwikkelingen in het bedreigingslandschap, in staat een nieuwe sector in uw actieplan voor de bescherming van kritieke informatie-infrastructuur op te nemen?	1
	3	-		Beschikt u over een methode om aanbieders van essentiële diensten te identificeren?	1	Beschikt u over een nationaal register voor geïdentificeerde aanbieders van essentiële diensten per kritieke sector?	1	Evalueert en actualiseert u ten minste om de twee jaar de lijst van geïdentificeerde aanbieders van essentiële diensten?	1	Bent u, afhankelijk van de laatste ontwikkelingen in het bedreigingslandschap, in staat nieuwe vereisten in uw actieplan voor de bescherming van kritieke informatie-infrastructuur aan te passen?	1

NCSS-doelstelling	#										
11 – Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners	4	-		Beschikt u over een methode om digitaledienstverleners te identificeren?	1	Beschikt u over een nationaal register voor geïdentificeerde digitaledienstverleners?	1	Beschikt u over andere mechanismen om te meten of de technische en organisatorische maatregelen die door digitaledienstverleners worden uitgevoerd geschikt zijn om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheren? Bv. regelmatige cyberbeveiligingsaudits, een nationaal kader voor de implementatie van standaardmaatregelen, technische instrumenten die door de overheid ter beschikking worden gesteld, zoals detectiesondes of systeemspecifieke configuratiebeoordelingen.	1	-	
	5	-		Beschikt u over een of meer nationale autoriteiten die toezicht houden op de bescherming van kritieke informatie-infrastructuur en de beveiliging van netwerk- en informatiesystemen? Bv. zoals vereist krachtens de NIS-richtlijn (2016/1148).	1	Beschikt u over een nationaal register voor geïdentificeerde of bekende risico's?	1	Evalueert en actualiseert u ten minste om de twee jaar de lijst van geïdentificeerde digitaledienstverleners?	1	-	
	6	-		Ontwikkelt u sectorspecifieke beschermingsplannen? Bv. met basismaatregelen voor cyberbeveiliging (verplicht of richtsnoeren).	0	Beschikt u over een methode om CII's in kaart te brengen?	1	Maakt u gebruik van een (nationale of internationale) beveiligingscertificeringsregeling om aanbieders van essentiële diensten en digitaledienstverleners te helpen veilige ICT-producten te identificeren? Bv. SOG-IS MRA in Europa, nationale initiatieven.	1	-	

	7	-		-		Maakt u gebruik van risicobeheerpraktijken om risico's in verband met CII's op nationaal niveau vast te stellen, te kwantificeren en te beheren?	1	Maakt u gebruik van een beveiligingscertificeringsregeling of kwalificatieprocedure om dienstverleners die met aanbieders van essentiële diensten werken, te beoordelen? Bv. dienstverleners op het gebied van opsporing van incidenten, incidentenrespons, cyberbeveiligingsaudit, clouddiensten, smartcards enz.	1	-	
	8	-		-		Voert u een raadplegingsproces uit om grensoverschrijdende afhankelijkheden vast te stellen?	1	Beschikt u over mechanismen om het nalevingsniveau van aanbieders van essentiële diensten en digitaledienstverleners te meten met betrekking tot basismaatregelen op het gebied van cyberbeveiliging?	0	-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
11 – Beschermen van kritieke informatie-infrastructuur, aanbieders van essentiële diensten en digitaledienstverleners	9					Hebt u één aanspreekpunt dat verantwoordelijk is voor de coördinatie van kwesties die verband houden met de beveiliging van netwerk- en informatiesystemen op nationaal niveau en grensoverschrijdende samenwerking op EU-niveau?	1	Beschikt u over voorzieningen om de continuïteit te waarborgen van de diensten die door kritieke informatie-infrastructuren worden geleverd? Bv. anticipatie op crises, procedures om kritieke informatiesystemen opnieuw op te bouwen, bedrijfscontinuïteit zonder IT, air gap-backupprocedures.	0		
	10					Definieert u basismaatregelen met betrekking tot cyberbeveiliging (verplicht of richtsnoeren) voor digitale dienstverleners en alle sectoren die in bijlage II bij de NIS-richtlijn (2016/1148) worden genoemd?	1				
	11	-		-		Biedt u instrumenten of methoden om cyberincidenten op te sporen?	1	-		-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
12 – Cybercriminaliteit aanpakken	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u een studie verricht om na te gaan welke rechtshandhavingsvereisten (rechtsgrondslag, middelen, vaardigheden) nodig zijn om cybercriminaliteit doeltreffend aan te pakken?	1	Is uw nationale rechtskader volledig in overeenstemming met het relevante EU-rechtskader, met name met Richtlijn 2013/40/EU over aanvallen op informatiesystemen? Bv. illegale toegang tot informatiesystemen, illegale systeemverstoring, illegale gegevensverstoring, illegale interceptie, instrumenten die worden gebruikt voor het plegen van strafbare feiten.	1	Beschikt u over speciale eenheden om cybercriminaliteit aan te pakken op parketten?	1	Verzamelt u statistieken overeenkomstig de bepalingen van artikel 14, lid 1, van Richtlijn 2013/40/EU (richtlijn over aanvallen op informatiesystemen)?	1	Hebt u interinstitutionele opleidingen of opleidingsworkshops voor LEA's, rechters, openbare aanklagers en nationale/gouvernementele CSIRT's op nationaal niveau en/of op multilateraal niveau?	1
	2	Hebt u een studie verricht om na te gaan welke vereisten in verband met openbare aanklagers en rechters (rechtsgrondslag, middelen, vaardigheden) nodig zijn om cybercriminaliteit doeltreffend aan te pakken?	1	Beschikt u over wettelijke bepalingen om online identiteitsdiefstal en diefstal van persoonsgegevens aan te pakken?	1	Hebt u een speciaal budget ten behoeve van diensten voor cybercriminaliteit?	1	Verzamelt u afzonderlijke statistieken over cybercriminaliteit? Bv. operationele statistieken, statistieken over trends in cybercriminaliteit, statistieken over de opbrengsten van cybercriminaliteit en de schade die eruit voortvloeit.	1	Neemt u deel aan gecoördineerde acties op internationaal niveau om criminele activiteiten te verstoren? Bv. infiltratie in criminele hackersfora, georganiseerde cybercrimegroepen en dark-webmarkten, verwijdering van botnets.	1
	3	Heeft uw land het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa ondertekend?	1	Beschikt u over een wettelijke bepaling inzake online inbreuken op intellectuele eigendom en auteursrechten?	1	Hebt u een centraal orgaan/entiteit opgericht om de activiteiten op het gebied van de bestrijding van cybercriminaliteit te coördineren?	1	Evalueert u of de toereikendheid van de opleiding die aan het personeel van LEA's, het gerecht en nationale CSIRT('s) wordt gegeven om cybercriminaliteit aan te pakken?	1	Zijn de taken van CSIRT's, LEA's en het gerecht (aanklagers en rechters) duidelijk gescheiden wanneer zij samenwerken om cybercriminaliteit aan te pakken?	1

	4			Beschikt u over wettelijke bepalingen tegen online pesterijen of cyberpesten?	1	Hebt u samenwerkingsmechanismen tot stand gebracht tussen relevante nationale instellingen die betrokken zijn bij de bestrijding van cybercriminaliteit, waaronder nationale CSIRT's voor rechtshandhaving?	1	Evalueert u regelmatig of u over voldoende middelen (personeel, budget en instrumenten) beschikt ten behoeve van de diensten voor de bestrijding van cybercriminaliteit binnen LEA's?	1	Vergemakkelijkt uw regelgevingskader de samenwerking tussen CSIRT's/LE en het gerechtelijk apparaat (aanklagers en rechters)?	1
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
12 – Cybercriminaliteit aanpakken	5			Beschikt u over wettelijke bepalingen ter bestrijding van computerfraude, bijvoorbeeld naleving van de bepalingen van het Verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van de Raad van Europa?	1	Werkt u samen en deelt u informatie met andere lidstaten op het gebied van de bestrijding van cybercriminaliteit?	1	Evalueert u regelmatig of u over voldoende middelen (personeel, budget en instrumenten) beschikt ten behoeve van de diensten voor de bestrijding van cybercriminaliteit binnen de vervolgingsautoriteiten?	1	Werkt u mee aan het ontwikkelen en onderhouden van gestandaardiseerde instrumenten en methoden, formulieren en procedures die gedeeld moeten worden met belanghebbenden in de EU (LEA's, CSIRT's, Enisa, EC3 van Europol)?	1
	6	-		Beschikt u over wettelijke bepalingen inzake onlinebescherming van kinderen? Bv. naleving van de bepalingen van Richtlijn 2011/93/EU en het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa.	1	Werkt u samen en deelt u informatie met EU-agentschappen (bv. EC3 van Europol, Eurojust, Enisa) op het gebied van de bestrijding van cybercriminaliteit?	1	Beschikt u over speciale rechtbanken of gespecialiseerde rechters om zaken in verband met cybercriminaliteit te behandelen?	1	Beschikt u over geavanceerde mechanismen om personen ervan te weerhouden zich aangetrokken te voelen tot of betrokken te raken bij cybercriminaliteit?	0
	7	-		Hebt u een operationeel nationaal aanspraakpunt aangewezen voor het uitwisselen van informatie en het beantwoorden van dringende informatieverzoeken van andere lidstaten met betrekking tot strafbare feiten die zijn opgenomen in Richtlijn 2013/40/EU (richtlijn inzake aanvallen op informatiesystemen)?	1	Beschikt u over de juiste instrumenten om cybercriminaliteit aan te pakken? Bv. taxonomie en classificatie van cybercriminaliteit, instrumenten om elektronisch bewijs te verzamelen, instrumenten voor computer forensics, betrouwbare deelplatforms.	1	Beschikt u over voorzieningen om steun en bijstand te verlenen aan slachtoffers van cybercriminaliteit (algemene gebruikers, kmo's, grote ondernemingen)?	1	Maakt uw land gebruik van de Blauwdruk van de EU en/of het Law Enforcement Emergency Response Protocol (EU LE ERP) om doeltreffend te reageren op grootschalige cyberincidenten?	0

	8			Heeft uw rechtshandhavingsinstantie een speciale eenheid voor cybercriminaliteit?	1	Beschikt u over standaardprocedures voor het behandelen van elektronisch bewijsmateriaal?	1	Hebt u een interinstitutioneel kader en samenwerkingsmechanismen tot stand gebracht tussen alle relevante belanghebbenden (bv. LEA, nationale CSIRT, rechtsgemeenschappen), waaronder de particuliere sector (bv. aanbieders van essentiële diensten, dienstverleners) indien van toepassing, om te reageren op cyberaanvallen?	1	-	
	9			Hebt u, overeenkomstig artikel 35. van het Verdrag van Boedapest, een 24/7 aanspreekpunt aangewezen?	1	Neemt uw land deel aan opleidingsmogelijkheden die worden aangeboden en/of ondersteund door EU-agentschappen (bv. Europol, Eurojust, OLAF, Cepol, Enisa)?	0	Vergemakkelijkt uw regelgevingskader de samenwerking tussen CSIRT's en LE?	1	-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
12 – Cybercriminaliteit aanpakken	10	-		Hebt u een 24/7 operationeel nationaal aanspreekpunt aangewezen voor het EU Law Enforcement Emergency Response Protocol (EU LE ERP) om te reageren op grote cyberaanvallen?	1	Overweegt uw land het tweede aanvullende protocol bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa aan te nemen?	0	Beschikt u over mechanismen (bv. instrumenten, procedures) om de informatie-uitwisseling en de samenwerking tussen het CSIRT/LE en eventueel het gerechtelijk apparaat (aanklagers en rechters) op het gebied van de bestrijding van cybercriminaliteit te vergemakkelijken?	1	-	
	11			Biedt u regelmatig gespecialiseerde opleidingen aan voor belanghebbenden die betrokken zijn bij de aanpak van cybercriminaliteit (LEA's, gerecht, CSIRT's)? Bv. opleidingssessies over het instellen van procedures wegens/vervolgen van cybercriminaliteit, opleidingen over het verzamelen van elektronisch bewijsmateriaal en het waarborgen van de integriteit van de digitale bewakingsketen en forensisch computeronderzoek enz.	1						

	12			Is uw land overgegaan tot de ratificatie van/toetreding tot het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa?	1			-	-	-		
	13	-		Heeft uw land het Aanvullend Protocol (strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen) bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa ondertekend en geratificeerd?	0	-	-	-		-		

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
13 – Ontwikkelen van mechanismen voor het melden van incidenten	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Beschikt u over informele mechanismen voor het delen van informatie over cyberbeveiligingsincidenten tussen particuliere organisaties en nationale autoriteiten?	1	Beschikt u over een regeling voor het melden van incidenten voor alle sectoren die onder bijlage II bij de NIS-richtlijn vallen?	1	Beschikt u over een regeling voor verplichte melding van incidenten die in de praktijk werkt?	1	Beschikt u over een geharmoniseerde procedure voor het melden van sectorale incidenten?	1	Stelt u een jaarlijks incidentenrapport op?	1
	2	-		Hebt u de meldingsplichten voor aanbieders van telecommunicatiediensten overeenkomstig artikel 40 van de Richtlijn (EU) 2018/1972 ten uitvoer gelegd? De richtlijn schrijft voor dat de lidstaten ervoor moeten zorgen dat aanbieders van openbare elektronische-communicatienetwerken of van algemeen beschikbare elektronische-communicatiediensten de bevoegde instantie onverwijld in kennis stellen van een beveiligingsincident dat een belangrijke impact heeft gehad op de exploitatie van netwerken of diensten.	1	Bestaat er een coördinatie-/samenwerkingsmechanisme voor de meldingsplicht bij incidenten met betrekking tot de AVG, de NIS-richtlijn, artikel 40 (vroegere artikel 13a) en eIDAS?	1	Beschikt u over een regeling voor het melden van incidenten voor andere sectoren dan die welke onder de NIS-richtlijn vallen?	1	Bestaan er rapporten over het cyberbeveiligingslandschap of andere soorten analyses die worden opgesteld door de entiteit die de incidentenrapporten ontvangt?	1

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
13 – Ontwikkelen van mechanismen voor het melden van incidenten	3	-		Hebt u de meldingsplichten voor verleners van vertrouwensdiensten overeenkomstig artikel 19 van eIDAS (Verordening (EU) nr. 910/2014) ten uitvoer gelegd? Artikel 19 schrijft onder meer voor dat aanbieders van vertrouwensdiensten de toezichthoudende instantie in kennis moeten stellen van significante incidenten/overtredingen.	1	Beschikt u over de juiste instrumenten om de vertrouwelijkheid en integriteit te waarborgen van de informatie die via de verschillende meldingskanalen wordt gedeeld?	1	Meet u de doeltreffendheid van de procedures voor incidentenmelding? Bv. indicatoren over incidenten die via de geëigende kanalen zijn gemeld, timing van de incidentenmelding.	1	-	
	4	-		Hebt u de meldingsplichten voor digitaledienstverleners overeenkomstig artikel 16 van de NIS-richtlijn ten uitvoer gelegd? Artikel 16 schrijft voor dat digitaledienstverleners ieder incident dat substantiële gevolgen heeft voor de verlening van een door hen in de Unie aangeboden dienst als bedoeld in bijlage III, onverwijld aan de bevoegde autoriteit of het CSIRT moeten melden.	1	Beschikt u over een platform/tool om de meldingsprocedure te vergemakkelijken?	0	Beschikt u op nationaal niveau over een gemeenschappelijke taxonomie voor de indeling van incidenten en categorieën van onderliggende oorzaken?	0	-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
14 – Versterken van privacy- en gegevensbescherming	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u studies of analyses verricht om na te gaan op welke gebieden verbeteringen mogelijk zijn om de privacyrechten van de burgers beter te beschermen?	1	Is de nationale gegevensbeschermingsautoriteit betrokken bij aan cyberbeveiliging gerelateerde kwesties (bv. opstellen van nieuwe wet- en regelgeving op het gebied van cyberbeveiliging, vaststellen van minimale beveiligingsmaatregelen)?	1	Bevordert u beste praktijken inzake beveiligingsmaatregelen en gegevensbescherming door ontwerp voor de openbare en/of de particuliere sector?	1	Evalueert u regelmatig of u over voldoende middelen (personeel, budget en instrumenten) beschikt ten behoeve van de gegevensbeschermingsautoriteit?	1	Beschikt u over mechanismen om de laatste technologische ontwikkelingen te volgen met het oog op de aanpassing van relevante richtsnoeren en wettelijke bepalingen/verplichtingen?	1
	2	Hebt u op nationaal niveau een rechtsgrondslag ontwikkeld voor de handhaving van de algemene verordening gegevensbescherming (Verordening (EU) nr. .2016/679)? Bv. meer specifieke bepalingen of beperkingen op de regels van de verordening handhaven of invoeren	0	-		Lanceert u bewustmakings- en opleidingsprogramma's rond dit thema?	1	Moedigt u organisaties en bedrijven aan zich te certificeren volgens ISO/IEC 27701:2019 inzake het Privacy Information Management System (Privacy Information Management System – PIMS)?	1	Neemt u actief deel aan/bevordert u O&O-initiatieven met betrekking tot technologieën ter bevordering van de persoonlijke levenssfeer (privacy enhancing technologies – PET)?	0
	3	-		-		Coördineert u de procedures voor incidentenmelding met de gegevensbeschermingsautoriteit?	1	-		-	
	4	-		-		Bevordert en ondersteunt u de ontwikkeling van technische normen inzake informatiebeveiliging en privacy? Zijn ze specifiek toegesneden op kleine en middelgrote ondernemingen (kmo's)?	0	-		-	

	5	-		-		Biedt u praktische en schaalbare richtsnoeren om verschillende soorten verwerkingsverantwoordelijken te ondersteunen bij het voldoen aan de wettelijke vereisten en verplichtingen inzake privacy en gegevensbescherming?	0	-		-

4.1.4 Cluster 4: Samenwerking

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
15 – Opzetten van een publiek-privaat partnerschap (PPP)	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Wordt algemeen begrepen dat PPP's op verschillende manieren bijdragen aan het verhogen van het niveau van cyberbeveiliging in het land? Bv. het delen van belangen in de groei van de cyberbeveiligingssector, samenwerking bij het ontwikkelen van een relevant regelgevingskader voor cyberbeveiliging, het bevorderen van O&O.	1	Beschikt u over een nationaal actieplan voor het opzetten van PPP's?	1	Hebt u nationale publiek-private partnerschappen opgezet?	1	Hebt u sectoroverschrijdende PPP's opgezet?	1	Bent u in staat om, afhankelijk van de laatste technologische en regelgevende ontwikkelingen, PPP's aan te passen of op te zetten?	1
	2	-		Schept u een wettelijke of contractuele grondslag (specifieke wetten, NDA's, intellectuele eigendom) om het toepassingsgebied van PPP's te bepalen?	1	Hebt u sectorspecifieke PPP's opgezet?	1	Richt u zich bij de opgezette PPP's ook op publiek-publieke en privaat-private samenwerking?	1		
	3	-		-		Voorziet u in financiering voor het opzetten van PPP's?	1	Bevordert u PPP's bij kleine en middelgrote ondernemingen (kmo's)?	1	-	

	4	-		-		Leiden openbare instellingen de PPP's in het algemeen? D.w.z. één enkel aanspreekpunt van de publieke sector dat de PPP's bestuurt en coördineert, overheidsinstellingen die van tevoren afspreken wat zij willen bereiken, duidelijke richtsnoeren van de overheidsdiensten over hun behoeften en beperkingen ten aanzien van de particuliere sector.	1	Meet u de resultaten van PPP's?	1	-	
	5	-		-		Bent u lid van het contractuele publiek-private partnerschap (cPPP) van de Europese Cyber Security Organisatie (ECSO)?	0	-		-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
15 – Opzetten van een publiek-privaat partnerschap (PPP)	6	-		-		Hebt u een of meer PPP's die zich bezighouden met CSIRT-activiteiten?	0	-		-	
	7					Hebt u een of meer PPP's die zich bezighouden met de bescherming van kritieke informatie-infrastructuur?	0				
	8	-		-		Hebt u een of meer PPP's die zich bezighouden met het creëren van bewustzijn voor cyberbeveiliging en het ontwikkelen van vaardigheden?	0	-		-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
16 – De samenwerking tussen openbare instanties institutionaliseren	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen tot het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1

	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Beschikt u over informele samenwerkingskanalen tussen openbare instanties?	1	Hebt u een nationaal samenwerkingsverband dat zich richt op cyberbeveiliging? Bv. adviesraden, stuurgroepen, forums, raden, cybercentra of vergadergroepen van deskundigen.	1	Nemen overheidsinstanties deel aan de samenwerkingsregeling?	1	Zorgt u ervoor dat er voor cyberbeveiliging bestemde samenwerkingskanalen bestaan tussen ten minste de volgende overheidsinstanties: inlichtingendiensten, binnenlandse rechtshandhaving, vervolgingsautoriteiten, overheidsactoren, nationale CSIRT en defensie?	1	Krijgen openbare instanties uniforme minimale informatie over de meest recente ontwikkelingen in het bedreigingslandschap en cyberbeveiligingsbewustzijn?	1
	2	-		-		Hebt u samenwerkingsplatforms opgezet om informatie uit te wisselen?	1	Meet u de successen en beperkingen van de verschillende samenwerkingsregelingen bij het bevorderen van doeltreffende samenwerking?	1	-	
NCSS-doelstelling	**#**	**Niveau 1**	**R**	**Niveau 2**	**R**	**Niveau 3**	**R**	**Niveau 4**	**R**	**Niveau 5**	**R**
16 – De samenwerking tussen openbare instanties institutionaliseren	3	-		-		Hebt u het toepassingsgebied van de samenwerkingsplatforms gedefinieerd (bv. taken en verantwoordelijkheden, aantal probleemgebieden)?	1	-		-	
	4	-		-		Organiseert u jaarlijkse bijeenkomsten?	1	-		-	
	5	-		-		Beschikt u over samenwerkingsmechanismen tussen bevoegde autoriteiten in verschillende geografische regio's? Bv. een netwerk van beveiligingscorrespondenten per regio, cyberbeveiligingsfunctionaris in regionale kamers van koophandel.	1	-		-	

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
17 – Deelnemen aan internationale samenwerking (niet alleen met EU-lidstaten)	a	Behandelt u de doelstelling in uw huidige NCSS , of bent u van plan dat in de volgende versie te doen?	1	Bestaan er informele praktijken of activiteiten die bijdragen aan het bereiken van de doelstelling op een niet-gecoördineerde manier?	1	Beschikt u over een actieplan dat formeel is vastgesteld en gedocumenteerd?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om de prestaties ervan te testen?	1	Beschikt u over mechanismen om ervoor te zorgen dat het actieplan dynamisch wordt aangepast aan ontwikkelingen in de omgeving?	1
	b			Hebt u de beoogde resultaten, de leidende beginselen of de kernactiviteiten van uw actieplan gedefinieerd?	1	Beschikt u over een actieplan met een duidelijke toewijzing van middelen en beleid?	1	Evalueert u uw actieplan met betrekking tot de doelstelling om ervoor te zorgen dat het correct geprioriteerd en geoptimaliseerd wordt?	1		
	c			Is uw actieplan, indien relevant, uitgevoerd en al van kracht op een beperkt toepassingsgebied?	0						
	1	Hebt u een strategie inzake internationale betrekkingen?	1	Hebt u samenwerkingsovereenkomsten met andere landen (bilateraal, multilateraal) of partners in andere landen? Bv. uitwisseling van informatie, capaciteitsopbouw, bijstand.	1	Wisselt u informatie uit op strategisch niveau? Bv. beleid op hoog niveau, risicoperceptie.	1	Zijn de nationale openbare instanties op het gebied van cyberbeveiliging in uw land betrokken bij internationale samenwerkingsregelingen?	1	Leidt u besprekingen over één of meer onderwerpen binnen multilaterale overeenkomsten?	1
	2	Hebt u informele samenwerkingskanalen met andere landen?	1	Beschikt u over één aanspreekpunt dat een verbindingsfunctie kan vervullen met het oog op grensoverschrijdende samenwerking met de autoriteiten van de lidstaten (samenwerkingsgroep, CSIRT-netwerk)?	1	Wisselt u informatie uit op tactisch niveau? Bv. bulletin van bedreigingsactoren, ISAC's, TTP's.	1	Evalueert u op regelmatige basis de resultaten van internationale samenwerkingsinitiatieven?	1	Leidt u besprekingen over één of meer onderwerpen binnen internationale verdragen of conventies?	1

NCSS-doelstelling	#	Niveau 1	R	Niveau 2	R	Niveau 3	R	Niveau 4	R	Niveau 5	R
17 – Deelnemen aan internationale samenwerking (niet alleen met EU-lidstaten)	3	Heeft het publieke leiderschap verklaard internationaal samen te willen werken op het gebied van cyberbeveiliging?	1	Beschikt u over toegewijde personen die betrokken zijn bij internationale samenwerking?	1	Wisselt u informatie uit op operationeel niveau? Bv. informatie over operationele coördinatie, lopende incidenten, IOC's.	1	-		Leidt u besprekingen of onderhandelingen over een of meer onderwerpen binnen internationale groepen van deskundigen? Bv. de wereldcommissie voor stabiliteit in cyberspace (Global Commission on the Stability of Cyberspace – GCSC), de NIS-samenwerkingsgroep van Enisa, de VN-groep van regeringsdeskundigen op het gebied van informatieveiligheid.	1
	4	-		-		Neemt u deel aan internationale cyberbeveiligingsoefeningen?	1	-		-	
	5	-		-		Neemt u deel aan internationale initiatieven voor capaciteitsopbouw? Bv. opleidingen, ontwikkeling van vaardigheden, opstellen van standaardprocedures.	0	-		-	
	6	-		-		Hebt u overeenkomsten inzake wederzijdse bijstand gesloten met andere landen? Bv. activiteiten van LEA's, juridische procedures, delen van incidentresponscapaciteiten, delen van cyberbeveiligingsvoorzieningen enz.	0	-		-	
	7	-		-		Hebt u internationale verdragen of conventies op het gebied van cyberbeveiliging ondertekend of geratificeerd? Bv. Internationale Gedragscode voor informatiebeveiliging, Verdrag inzake cybercriminaliteit.	0	-		-	

4.2 RICHTLIJNEN VOOR HET GEBRUIK VAN HET KADER

In dit deel wordt getracht de lidstaten een aantal richtsnoeren en aanbevelingen te geven voor de invoering van het kader en het invullen van de vragenlijst. De onderstaande aanbevelingen vloeien hoofdzakelijk voort uit de feedback die tijdens de interviews met de vertegenwoordigers van de lidstaten is verzameld:

- **Anticipeer op coördinatieactiviteiten om gegevens te verzamelen en te consolideren.** De meeste lidstaten erkennen dat het uitvoeren van een dergelijke zelfevaluatie ongeveer 15 mandagen in beslag zal nemen. Om de zelfevaluatie uit te voeren, zal een groot aantal verschillende belanghebbenden moeten worden benaderd. Daarom wordt aanbevolen tijd uit te trekken voor de voorbereidingsfase om alle relevante belanghebbenden binnen overheidsorganen, openbare instanties en de particuliere sector aan te wijzen.
- **Wijs een centraal orgaan aan dat belast is met de uitvoering van de zelfbeoordeling op nationaal niveau.** Aangezien het verzamelen van materiaal voor alle indicatoren van het NCAF heel wat belanghebbenden kan omvatten, wordt aanbevolen om een centraal orgaan of agentschap te belasten met het uitvoeren van de zelfbeoordeling en het verzorgen van het contact en de coördinatie met alle relevante belanghebbenden.
- **Gebruik de beoordelingsoefening als een manier om ervaringen uit te wisselen en te communiceren over thema's op het gebied van cyberbeveiliging.** Uit de door de lidstaten gedeelde ervaringen blijkt dat besprekingen (in de vorm van individuele gesprekken of collectieve workshops) een goede gelegenheid zijn om de dialoog rond cyberbeveiliging te bevorderen en gemeenschappelijke standpunten en verbeterpunten uit te wisselen. Het delen van resultaten kan niet alleen een licht werpen op belangrijke verwezenlijkingen, maar ook helpen om onderwerpen op het gebied van cyberbeveiliging onder de aandacht te brengen.
- **Gebruik de NCSS als toepassingsgebied om de doelstellingen van de beoordeling te selecteren.** De 17 doelstellingen waaruit het NCAF is opgebouwd, zijn gebaseerd op de doelstellingen die de lidstaten gewoonlijk in hun NCSS opnemen. De doelstellingen die als onderdeel van de NCSS worden behandeld, moeten worden gebruikt als een middel om het toepassingsgebied van de beoordeling te bepalen. De NCSS mag de beoordeling echter niet beperken. Aangezien de NCSS zich gewoonlijk op prioriteiten concentreert, worden bepaalde gebieden doelbewust weggelaten uit de NCSS. Dit betekent echter niet dat een bepaalde capaciteit niet aanwezig is. Indien bijvoorbeeld een specifieke doelstelling niet is opgenomen in de NCSS, maar het land beschikt over cyberbeveiligingscapaciteiten die verband houden met die doelstelling, kan de beoordeling van die doelstelling plaatsvinden.
- **Zorg ervoor de interpretatie van de score consistent blijft met de ontwikkeling van de NCSS wanneer het toepassingsgebied van de NCSS zich ontwikkelt.** De levenscyclus van de NCSS is een proces van meerdere jaren. De nationale cyberbeveiligingsstrategieën van sommige lidstaten worden gewoonlijk toegepast met een routekaart van drie tot vijf jaar met wijzigingen in het toepassingsgebied tussen twee opeenvolgende edities van een NCSS. Daarom moet bijzonder voorzichtig te werk worden gegaan bij de presentatie van de resultaten van de zelfbeoordeling tussen twee edities van een NCSS: wijzigingen in het toepassingsgebied kunnen immers gevolgen hebben voor de uiteindelijke maturiteitsscore. Er wordt aanbevolen om de scores over het volledige toepassingsgebied van strategische doelstellingen van jaar tot jaar te vergelijken(d.w.z. globale algemene score).

Herhaling van het scoringssysteem – voorbeeld van de dekkingsgraad
Het scoringssysteem omvat twee scoreniveaus:
(i) een **globale algemene dekkingsgraad** die gebaseerd is op de volledige lijst van strategische doelstellingen van het zelfbeoordelingskader; en

(ii) een **globale specifieke dekkingsgraad** die gebaseerd is op door de lidstaat geselecteerde strategische doelstellingen (die gewoonlijk overeenstemmen met de doelstellingen van de NCSS van het specifieke land).

Door ontwerp (zie paragraaf 3.1 over het scoringssysteem) zal de globale specifieke dekkingsgraad gelijk zijn aan of hoger zijn dan de globale algemene dekkingsgraad, aangezien de laatste doelstellingen kan omvatten die niet door de lidstaat worden behandeld, waardoor de globale algemene dekkingsgraad daalt. Wanneer een lidstaat een nieuwe doelstelling toevoegt, zal de dekkingsgraad toenemen (d.w.z. er worden meer maturiteitsindicatoren bestreken), terwijl de globale specifieke maturiteit kan afnemen (ingeval de nieuw toegevoegde doelstelling zich in een beginstadium bevindt en dus een laag maturiteitsniveaus heeft).

- **Bij het invullen van de vragenlijst voor zelfbeoordeling mag niet uit het oog worden verloren dat het hoofddoel is de lidstaten te ondersteunen bij de capaciteitsopbouw op het gebied van cyberbeveiliging.** Daarom wordt aanbevolen om bij het invullen van de zelfbeoordeling, het antwoord te kiezen dat het meest algemeen aanvaard is, ook al kan het in sommige situaties moeilijk zijn om de vraag op een definitieve manier te beantwoorden. Indien het antwoord op een vraag bijvoorbeeld JA is voor een bepaalde toepassingsgebied, maar NEE voor een ander toepassingsgebied, moeten de lidstaten voor ogen houden dat een NEE-antwoord een actie vereist: ofwel een herstelplan, ofwel een plan om actie te ondernemen op een verbeteringsgebied dat bij toekomstige ontwikkelingen in aanmerking moet worden genomen.

5. VOLGENDE STAPPEN

5.1 TOEKOMSTIGE VERBETERINGEN

Tijdens interviews met vertegenwoordigers van de lidstaten en tijdens de deskresearchfase werden tevens de volgende aanbevelingen ter verbetering van het huidige beoordelingskader voor nationale capaciteiten aangemerkt als mogelijke toekomstige ontwikkelingen:

- **Ontwikkel het scoresysteem met het oog op een grotere nauwkeurigheid.** Zo zou in plaats van het binaire antwoord JA/NEE een dekkingspercentage kunnen worden ingevoerd om beter rekenschap te kunnen geven van de complexiteit van de consolidatie van de capaciteiten op nationaal niveau. Als eerste stap werd gekozen voor een eenvoudige aanpak met JA/NEE-antwoorden.
- **Voer kwantitatieve meetwaarden in om de doeltreffendheid van de NCSS van de lidstaten te meten.** Het beoordelingskader voor nationale capaciteiten evalueert immers het maturiteitsniveau van de cyberbeveiligingscapaciteiten van de lidstaten. Dit zou kunnen worden aangevuld met meetwaarden om de doeltreffendheid te meten van de activiteiten en actieplannen die door de lidstaten worden uitgevoerd om deze capaciteiten op te bouwen. Het leek niet realistisch om in de huidige fase dergelijke doeltreffendheidsmeetwaarden op te stellen, aangezien er: weinig feedback uit het veld is, het moeilijk is zinvolle indicatoren te vinden die de output koppelen aan de uitvoering van de NCSS, en het moeilijk is realistische indicatoren te ontwikkelen die naderhand kunnen worden verzameld. Dit blijft echter een punt voor toekomstig werk.
- **Schakel over van een zelfbeoordelingsoefening naar een beoordelingsbenadering.** Een mogelijke toekomstige ontwikkeling van het kader zou kunnen bestaan uit een omschakeling naar een beoordelingsbenadering om de maturiteit van de cyberbeveiligingscapaciteiten van de lidstaten op een meer consistente manier te beoordelen. Door de beoordeling door een derde partij te laten uitvoeren, kan een mogelijk vooroordeel inderdaad tot een minimum worden beperkt.

BIJLAGE A – OVERZICHT VAN RESULTATEN DESKRESEARCH

Bijlage A bevat een samenvatting van eerdere werkzaamheden van Enisa op het gebied van nationale cyberbeveiligingsstrategieën en een overzicht van relevante openbaar beschikbare maturiteitsmodellen inzake cyberbeveiligingscapaciteit. Bij de selectie en beoordeling van de modellen is uitgegaan van de volgende veronderstellingen:

- niet alle modellen zijn gebaseerd op een rigoureuze onderzoeksmethode;
- de structuur en de resultaten van de modellen worden niet altijd grondig toegelicht met duidelijke verbanden tussen de verschillende elementen die elk model kenmerken;
- sommige modellen bieden geen details over het ontwikkelingsproces, de structuur en de beoordelingsmethode;
- andere modellen en instrumenten die we zijn tegengekomen, bieden geen details over de structuur en de inhoud en worden daarom niet vermeld; en
- De selectie van de te beoordelen modellen is gebaseerd op geografische dekking. De nadruk zal in de eerste plaats liggen op maturiteitsmodellen voor cyberbeveiligingscapaciteit die zijn ontwikkeld om de prestaties van Europese landen te beoordelen. Het is echter belangrijk om de geografische dekking uit te breiden om goede praktijken inzake het ontwikkelen van maturiteitsmodellen over de hele wereld te analyseren.

Deze systematische beoordeling van relevante openbaar beschikbare maturiteitsmodellen inzake cyberbeveiligingscapaciteit werd uitgevoerd met gebruikmaking van een aangepast analysekader dat gebaseerd is op de door Becker gedefinieerde methode voor de ontwikkeling van maturiteitsmodellen[22]. Voor elk bestaand maturiteitsmodel werden de volgende elementen geanalyseerd:

- **Naam van het maturiteitsmodel:** de naam van het maturiteitsmodel en de belangrijkste referenties;
- **Bron:** de openbare of particuliere instelling die belast is met het ontwerpen van het model;
- **Algemeen doel:** het algemene toepassingsgebied van het model en het beoogde doel (de beoogde doelen);
- **Aantal niveaus en omschrijving ervan:** het aantal maturiteitsniveaus van het model, alsmede hun algemene omschrijving;
- **Aantal eigenschappen en hun naam:** het aantal eigenschappen die het maturiteitsmodel gebruikt en hun naam. De analyse van de eigenschappen heeft een drieledig doel:
  - het maturiteitsmodel opsplitsen in gemakkelijk te begrijpen onderdelen;
  - verschillende eigenschappen samenvoegen tot clusters van eigenschappen die hetzelfde doel hebben; en
  - verschillende standpunten over het onderwerp ‘maturiteitsniveau’ verstrekken.
- **Beoordelingsmethode:** de methode voor de beoordeling van het maturiteitsmodel;

[22] J. Becker, R. Knackstedt en J. Pöppelbuß, “Developing Maturity Models for IT Management: A Procedure Model and its Application,” Business & Information Systems Engineering, vol. 1, nr. 3, blz. 213, juni 2009.

- **Weergave van de resultaten**: de visualisatiemethode voor de resultaten van het maturiteitsmodel bepalen. De gedachte achter deze stap is dat maturiteitsmodellen vaak aan hun doel voorbijgaan als zij te complex zijn en dat de weergave derhalve aan praktische behoeften moet voldoen.

Eerdere werkzaamheden in verband met nationale cyberbeveiligingsstrategieën

Enisa heeft in 2012 twee documenten over nationale cyberbeveiligingsstrategieën gepubliceerd in het kader van reeds geleverde prestaties. 1) In de "Practical guide on the development and execution phase of NCSS"[23] wordt een reeks concrete acties voorgesteld voor de efficiënte uitvoering van een NCSS en wordt de levenscyclus van een NCSS in vier fasen gepresenteerd: strategieontwikkeling, strategie-uitvoering, strategie-evaluatie en strategie-onderhoud. 2) In "Setting the course for national efforts to strengthen security in cyberspace"[24] wordt de status van de strategieën inzake cyberbeveiliging binnen de EU en daarbuiten in 2012 geschetst en wordt voorgesteld dat de lidstaten gemeenschappelijke thema's en verschillen tussen hun nationale cyberbeveiligingsstrategieën vaststellen.

In 2014 werd het eerste Enisa-kader voor de evaluatie van de nationale cyberbeveiligingsstrategieën van een lidstaat gepubliceerd[25]. Dit kader bevat aanbevelingen en goede praktijken, alsmede een reeks instrumenten voor capaciteitsopbouw voor de evaluatie van een NCSS (bv. vastgestelde doelstellingen, inputs, outputs, kernprestatie-indicatoren). Deze instrumenten zijn aangepast aan de uiteenlopende behoeften van landen met verschillende maturiteitsniveaus in hun strategische planning. Datzelfde jaar publiceerde Enisa de "Online NCSS Interactive Map"[26], waarmee gebruikers snel de nationale cyberbeveiligingsstrategieën van alle lidstaten en EVA-landen kunnen raadplegen, inclusief hun strategische doelstellingen en goede voorbeelden van uitvoering. De map werd eerst ontwikkeld als een NCSS-register (2014) en werd in 2018 bijgewerkt met voorbeelden van uitvoering. Sinds 2019 fungeert de map als *information hub* om gegevens te centraliseren die door de lidstaten worden verstrekt over hun inspanningen om de nationale cyberbeveiliging te verbeteren.

In de in 2016 gepubliceerde "NCSS Good Practice Guide"[27] worden vijftien strategische doelstellingen vastgesteld. In deze gids wordt ook de stand van uitvoering van de NCSS van elke lidstaat geanalyseerd en worden verschillende lacunes en uitdagingen met betrekking tot deze uitvoering vastgesteld.

In 2018 publiceerde Enisa de "National Cybersecurity Strategies Evaluation Tool"[28]: een interactief zelfbeoordelingsinstrument om lidstaten te helpen hun strategische prioriteiten en

[23] NCSS: Practical Guide on Development and Execution (Enisa, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Enisa, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (Enisa, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies – Interactive Map (Enisa, 2014, bijgewerkt in 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Dit document is een update van de gids uit 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Enisa, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

doelstellingen met betrekking tot hun nationale cyberbeveiligingsstrategieën te evalueren. Aan de hand van een reeks eenvoudige vragen biedt dit instrument de lidstaten specifieke aanbevelingen voor de uitvoering van elke doelstelling. Tot slot komt in de in 2019 gepubliceerde “Good practices in innovation on Cybersecurity under the NCSS”[29] het thema innovatie in cyberbeveiliging in het kader van de nationale cyberbeveiligingsstrategieën aan bod. Het document beschrijft de uitdagingen en goede praktijken voor de verschillende aspecten van innovatie, zoals die door deskundigen ter zake worden waargenomen, teneinde toekomstige strategische innovatiedoelstellingen te helpen formuleren.

A.1 Maturiteitsmodel inzake cyberbeveiliging voor naties (CMM)

Het maturiteitsmodel inzake cyberbeveiliging voor naties (Cybersecurity Capacity Maturity Model for Nations – CMM) werd ontwikkeld door het Global Cyber Security Capacity Centre (Capacity Centre), onderdeel van de Oxford Martin School binnen de Universiteit van Oxford. Het doel van het Capacity Centre is de schaal en de doeltreffendheid van de capaciteitsopbouw op het gebied van cyberbeveiliging te vergroten, zowel binnen het Verenigd Koninkrijk als internationaal, door de toepassing van het maturiteitsmodel inzake cyberbeveiliging (CMM). Het CMM is rechtstreeks gericht op landen die hun nationale capaciteit op het gebied van cyberbeveiliging wensen te versterken. Het CMM, dat oorspronkelijk in 2014 werd uitgevoerd, werd in 2016 herzien nadat het was gebruikt bij de beoordeling van elf nationale cyberbeveiligingscapaciteiten.

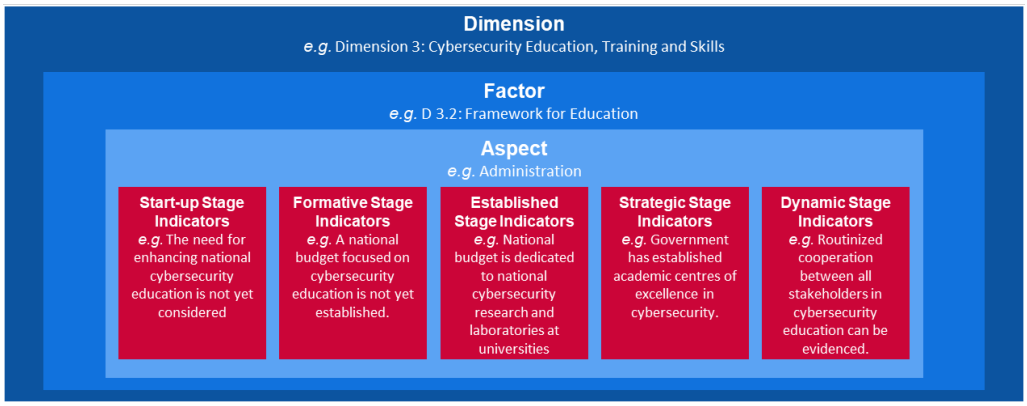
Eigenschappen/dimensies

Volgens het CMM bestaat cyberbeveiligingscapaciteit uit **vijf dimensies** die de clusters van cyberbeveiligingscapaciteit weergeven. Elke cluster vertegenwoordigt een andere ‘lens’ voor onderzoek aan de hand waarvan cyberbeveiligingscapaciteit kan worden bestudeerd en begrepen. Binnen de vijf dimensies beschrijven **factoren** de details van het bezit van cyberbeveiligingscapaciteit. Deze details zijn elementen die bijdragen tot de verbetering van de maturiteit van de cyberbeveiligingscapaciteit binnen elke dimensie. Voor elke factor vertegenwoordigen verschillende **aspecten** verschillende componenten van de factor. Aspecten vertegenwoordigen een organisatorische methode om indicatoren op te delen in kleinere clusters die gemakkelijker te begrijpen zijn. Elk aspect wordt vervolgens geëvalueerd aan de hand van **indicatoren** die de stappen, acties of bouwstenen beschrijven die indicatief zijn voor een specifieke fase van maturiteit (omschreven in de volgende paragraaf) binnen een afzonderlijk aspect, factor en dimensie.

De hierboven vermelde termen kunnen gelaagd worden weergegeven zoals in onderstaande figuur wordt getoond.

[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

Figuur 4: Voorbeeld van CMM-indicatoren



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimensie bv. Dimensie 3: Onderwijs, opleiding en vaardigheden op het gebied van cyberbeveiliging
Factor e.g. D 3.2: Framework for Education	Factor bv. D 3.2: Kader voor onderwijs
Aspect e.g. Administration	Aspect bv. Administratie
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indicatoren m.b.t. initiële fase bv. er wordt nog niet nagedacht over een verbetering van het nationale onderwijs op het vlak van cyberbeveiliging
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indicatoren m.b.t. formatieve fase bv. een nationaal budget voor onderwijs op het gebied van cyberbeveiliging wordt nog niet in overweging genomen
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indicatoren m.b.t. vastgestelde fase bv. er wordt een nationaal budget uitgetrokken voor nationaal cyberbeveiligingsonderzoek en laboratoria aan universiteiten
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indicatoren m.b.t. strategische fase bv. de overheid heeft academische expertisecentra voor onderwijs in cyberbeveiliging opgericht
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicatoren m.b.t. dynamische fase bv. een routinematige samenwerking tussen alle belanghebbenden bij het cyberbeveiligingsonderwijs kan worden aangetoond

De vijf dimensies worden hieronder beschreven:

i ontwikkelen van beleid en strategie inzake cyberbeveiliging (zes factoren);
ii aanmoedigen van een verantwoordelijke cyberbeveiligingscultuur binnen de samenleving (vijf factoren);
iii ontwikkelen van kennis op het gebied van cyberbeveiliging (drie factoren);
iv creëren van doeltreffende wet- en regelgevingskaders (drie factoren); en
v beheersen van risico's via normen, organisaties en technologieën (zeven factoren).

Maturiteitsniveaus

Het CMM hanteert **vijf maturiteitsniveaus** om te bepalen in welke mate een land vooruitgang heeft geboekt met betrekking tot een bepaald(e) factor/aspect van cyberbeveiligingscapaciteit. Deze niveaus dienen als momentopname van de bestaande cyberbeveiligingscapaciteit:

- **Initieel**: in deze fase is de cyberbeveiligingsmaturiteit ofwel nihil ofwel nog zeer embryonaal van aard. Er kunnen eerste besprekingen over capaciteitsopbouw op het gebied van cyberbeveiliging plaatsvinden, maar er zijn nog geen concrete acties ondernomen. In deze fase is er geen waarneembaar bewijs;

- **Formatief**: sommige kenmerken van de aspecten beginnen te groeien en worden onder woorden gebracht, maar kunnen ad hoc, ongeorganiseerd, slecht gedefinieerd – of gewoon 'nieuw' zijn. Deze activiteit kan echter duidelijk aangetoond worden;
- **Vastgesteld**: de elementen van het aspect zijn operationeel en werken. Er is echter niet goed nagedacht over de relatieve toewijzing van middelen. Er zijn weinig afwegingen gemaakt met betrekking tot de 'relatieve' investering in de verschillende elementen van het aspect. Het aspect is echter functioneel en gedefinieerd;
- **Strategisch**: er zijn keuzes gemaakt over welke delen van het aspect belangrijk zijn, en welke minder belangrijk zijn voor de specifieke organisatie of natie. De strategische fase weerspiegelt het feit dat deze keuzes zijn gemaakt, afhankelijk van de bijzondere omstandigheden van de natie of organisatie; en
- **Dynamisch**: in deze fase zijn er duidelijke mechanismen voorhanden om de strategie te wijzigen afhankelijk van de heersende omstandigheden, zoals de technologie van de bedreigingsomgeving, een wereldwijd conflict of een significante verandering op een bepaald gebied (bv. cybercriminaliteit of privacy). Dynamische organisaties hebben methoden ontwikkeld om strategieën soepel te wijzigen. Snelle besluitvorming, herverdeling van middelen en voortdurende aandacht voor de veranderende omgeving zijn kenmerken van deze fase.

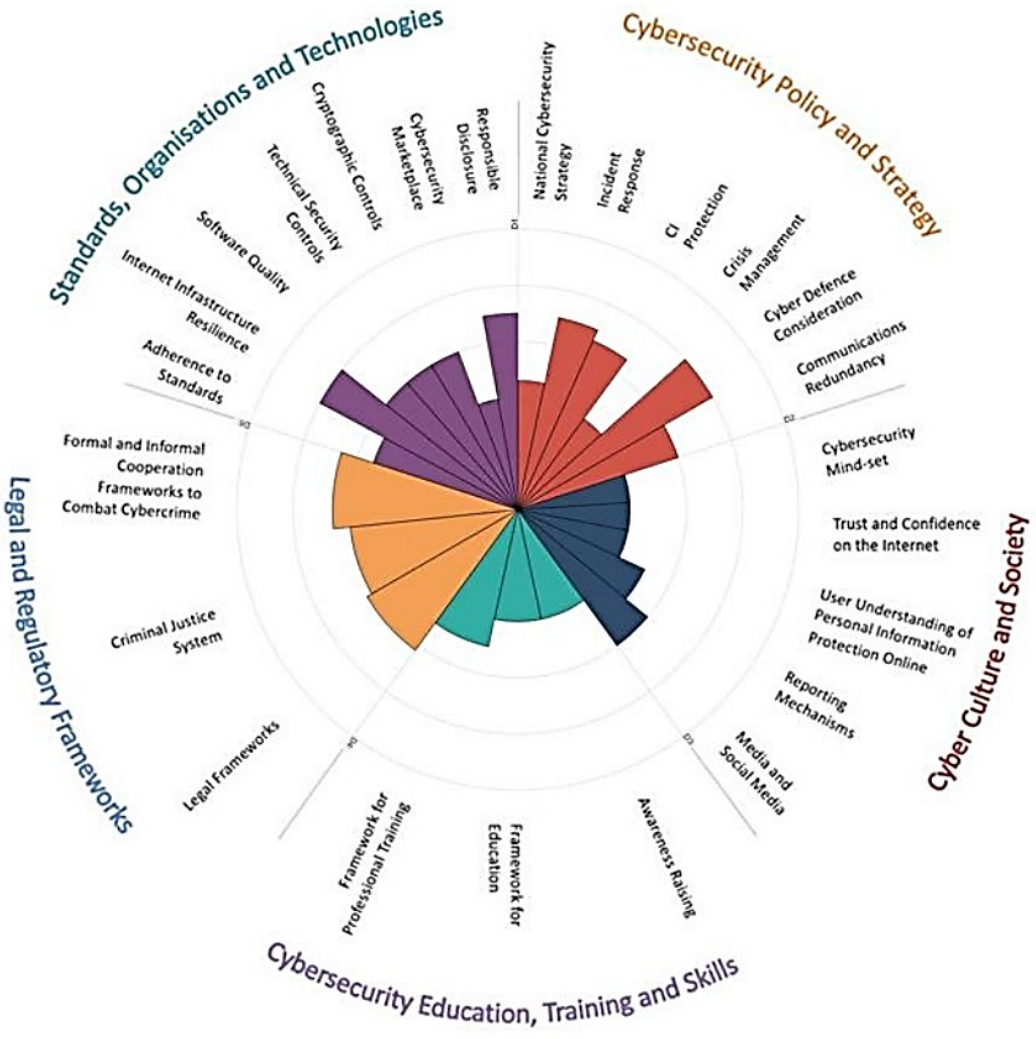
Beoordelingsmethode

Aangezien het Capacity Centre geen grondig en diepgaand inzicht heeft in elke nationale context waarin het model wordt toegepast, werkt het samen met internationale organisaties, gastministeries of organisaties in het betrokken land om de maturiteit van de cyberbeveiligingscapaciteit te beoordelen. Om het maturiteitsniveau van de vijf dimensies van het CMM te beoordelen, komen het Capacity Centre en de gastorganisatie gedurende twee of drie dagen bijeen met relevante nationale belanghebbenden van de openbare en de particuliere sector om focusgroepen te houden over de dimensies van het CMM. Elke dimensie wordt ten minste tweemaal besproken door verschillende clusters van belanghebbenden. Dit vormt het voorlopige pool van gegevens voor de latere beoordeling.

Weergave van de resultaten

Het CCM geeft een overzicht van het maturiteitsniveau van elk land aan de hand van een radar die bestaat uit vijf delen, één voor elke dimensie. Elke dimensie vertegenwoordigt een vijfde van de grafiek, waarbij de vijf maturiteitsfasen voor elke factor vanaf het midden van de grafiek zich uitstrekken naar buiten; zoals hieronder getoond, bevindt de fase 'Initieel' zich het dichtst bij het midden van de grafiek en bevindt de fase 'Dynamisch' zich aan de rand.

Figuur 5 CMM: Overzicht van resultaten



Standards, Organisations and Technologies	Normen, organisaties en technologieën
Legal Regulatory Frameworks	Wettelijke en regelgevende kaders
Cybersecurity Education, Training and Skills	Onderwijs, opleiding en vaardigheden op het gebied van cyberbeveiliging
Cybersecurity Policy and Strategy	Beleid en strategie op het gebied van cyberbeveiliging
Cyber Culture and Society	Cybercultuur en -samenleving
Responsible Disclosure	Verantwoorde bekendmaking
Cybersecurity market place	Cyberbeveiligingsmarkt
Cryptographic Controls	Cryptografische controles
Technical Security Controls	Controles inzake technische veiligheid
Software Quality	Softwarekwaliteit
Internet Infrastructure Resilience	Veerkracht van de internetinfrastructuur
Adherence to Standards	Naleving van normen
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formele en informele samenwerkingskaders voor de bestrijding van cybercriminaliteit
Criminal Justice System	Strafrechtelijk systeem
Legal Frameworks	Wettelijke kaders
Framework for Professional Training	Kader voor professionele opleiding
Framework for Education	Kader voor onderwijs

Awareness Raising	Bewustzijn creëren
Media and Social Medai	Media en sociale media
Reporting Mechanisms	Meldingsmechanismen
User Understanding of Personal Information Protection Online	Begrip van de gebruiker wat betreft de bescherming van persoonlijke informatie online
Trust and Confidence on the Internet	Vertrouwen op het internet
Cybersecurity Mind-set	Mindset inzake cyberbeveiliging
Communications Redundancy	Communicatieredundantie
Cyber Defence Consideration	Overweging m.b.t. cyberdefensie
Crisis Management	Crisisbeheer
CI Protection	Bescherming CI
Incident Response	Incidentenrespons
National Cybersecurity Strategy	Nationale strategie voor cyberbeveiliging

Global Cyber Security Capacity Centre Oxford Martin School, Universiteit van Oxford, 2017.

A.2 Maturiteitsmodel inzake cyberbeveiligingscapaciteit (C2M2)

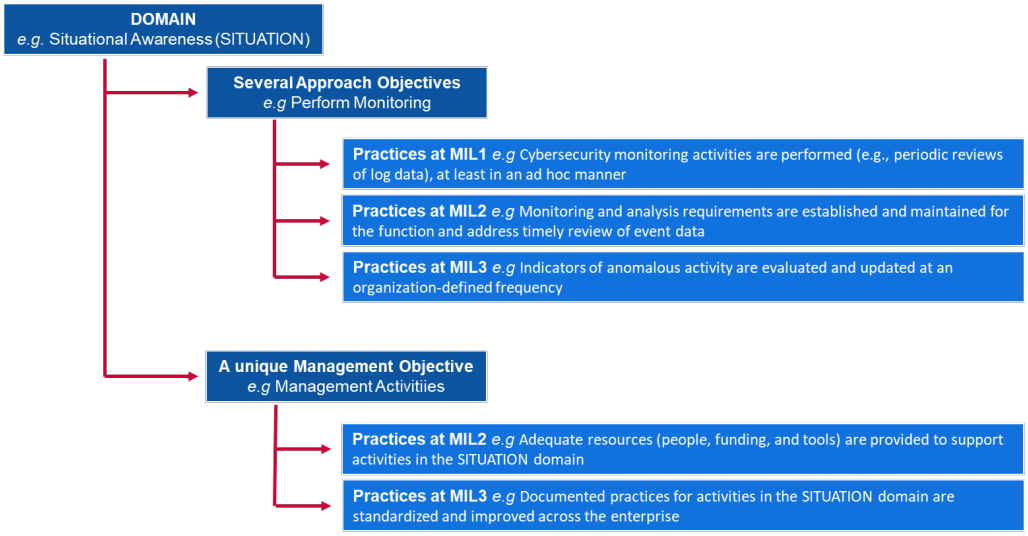
Het maturiteitsmodel inzake cyberbeveiligingscapaciteit (Cybersecurity Capacity Maturity Model – C2M2) werd ontwikkeld door het Amerikaanse ministerie van Energie, in samenwerking met deskundigen uit de particuliere en de publieke sector. Het doel van het Capacity Centre is organisaties in alle sectoren, en van alle soorten en maten te helpen hun cyberbeveiligingsprogramma's te evalueren en te verbeteren, en hun operationele veerkracht te versterken. Het C2M2 richt zich op de uitvoering en het beheer van cyberbeveiligingspraktijken in verband met activa voor informatie, informatietechnologie (IT) en operationele technologie (OT) en de omgevingen waarin deze werken. Het C2M2 definieert maturiteitsmodellen als: "een geheel van kenmerken, eigenschappen, indicatoren of patronen die de capaciteit en de vooruitgang in een bepaalde discipline weergeven". Het C2M2, dat oorspronkelijk in 2014 werd uitgevoerd, werd in 2019 herzien.

Eigenschappen/dimensies

Het C2M2 gaat uit van **tien domeinen** als een logische groepering van praktijken op het gebied van cyberbeveiliging. Elke reeks praktijken geeft de activiteiten weer die een organisatie kan uitvoeren om capaciteit in het domein tot stand te brengen en te ontwikkelen. Elk domein wordt vervolgens gekoppeld aan een **unieke beheerdoelstelling** en **verschillende benaderingsdoelstellingen**. Binnen zowel de aanpak als de beheerdoelstellingen worden **verschillende praktijken** gespecificeerd om geïnstitutionaliseerde activiteiten te beschrijven.

Het verband tussen deze begrippen wordt hieronder samengevat:

Figuur 6: Voorbeeld van C2M2-indicator



Domain eg Situational Awareness (SITUATION)	**Domein** b.v. situationeel bewustzijn (SITUATIE)
Several Approaches Objectives e.g. Perform Monitoring	**Verschillende benaderingen doelstellingen** b.v. een monitoring verrichten
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Praktijken op MIL1** bv. er worden ad hoc cyberbeveiligingsmonitoringactiviteiten uitgevoerd (bv. periodieke controles van loggegevens)
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Praktijken op MIL2** bv. er worden monitoring- en analysevereisten voor de functie opgesteld en bijgehouden die voorzien in een tijdige beoordeling van gebeurtenisgegevens
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Praktijken op MIL3** bv. er worden indicatoren van afwijkende activiteit geëvalueerd en bijgewerkt met een door de organisatie vastgestelde frequentie
A unique Management Objectve e.g. Management Activities	Een uniek beheerdoelstelling, bv. beheeractiviteiten
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Praktijken op MIL2** bv. er wordt gezorgd voor adequate middelen (mensen, financiering en instrumenten) ter ondersteuning van activiteiten in het domein SITUATIE
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Praktijken op MIL3** bv. gedocumenteerde praktijken voor activiteiten in het domein SITUATIE worden gestandaardiseerd en verbeterd binnen de onderneming

De tien domeinen worden hieronder gespecificeerd:

i risicobeheer (RISICO);
ii activa-, wijzigings- en configuratiebeheer (ACTIVA);
iii identiteits- en toegangsbeheer (TOEGANG);
iv beheer van dreigingen en kwetsbaarheden (DREIGING);
v situationeel bewustzijn (SITUATIE);
vi reactie op gebeurtenissen en incidenten (REACTIE);
vii beheer van toeleveringsketens en externe afhankelijkheden (AFHANKELIJKHEDEN);
viii personeelsbeheer (PERSONEEL);
ix cyberbeveiligingsarchitectuur (ARCHITECTUUR); en
x beheer van het cyberbeveiligingsprogramma (PROGRAMMA).

Maturiteitsniveaus

Het C2M2 hanteert **vier maturiteitsniveaus** (de zogenaamde Maturity Indicator Levels – MIL) om een tweeledige vooruitgang in maturiteit te bepalen: een vooruitgang in aanpak en een vooruitgang in beheer. De MIL's lopen van MIL0 tot MIL3 en zijn bedoeld om onafhankelijk op elk domein te worden toegepast.

- **MIL0**: er worden geen praktijken uitgevoerd.
- **MIL1**: er worden initiële praktijken uitgevoerd, maar dit kan op ad-hocbasis zijn.
- **MIL2**: kenmerken van het beheer:
  - praktijken worden gedocumenteerd;
  - er worden passende middelen ter beschikking gesteld om het proces te ondersteunen;
  - het personeel dat de praktijken uitvoert, beschikt over voldoende vaardigheden en kennis; en

- er worden verantwoordelijkheden en bevoegdheden voor de uitvoering van de praktijken toegewezen.

Kenmerken van de aanpak:

- de praktijken zijn volledieger of geavanceerder dan op MIL1.

- **MIL3**: kenmerken van het beheer:
  - activiteiten worden gestuurd door beleid (of andere richtlijnen van de organisatie);
  - er worden prestatiedoelstellingen voor domeinactiviteiten vastgesteld en gemonitord om de prestaties te volgen; en
  - gedocumenteerde praktijken voor domeinactiviteiten worden gestandaardiseerd en verbeterd binnen de onderneming.

  Kenmerken van de aanpak:
  - de praktijken zijn volledieger of geavanceerder dan op MIL2.

Beoordelingsmethode

Het C2M2 is ontworpen voor gebruik met een **methode en toolkit voor zelfevaluatie** (verkrijgbaar op verzoek) waarmee een organisatie haar cyberbeveiligingsprogramma kan meten en verbeteren. Een zelfevaluatie met behulp van de toolkit kan in één dag worden voltooid, maar de toolkit kan worden aangepast voor een nauwgezettere evaluatie. Bovendien kan het C2M2 worden gebruikt om de ontwikkeling van een nieuw cyberbeveiligingsprogramma te sturen.

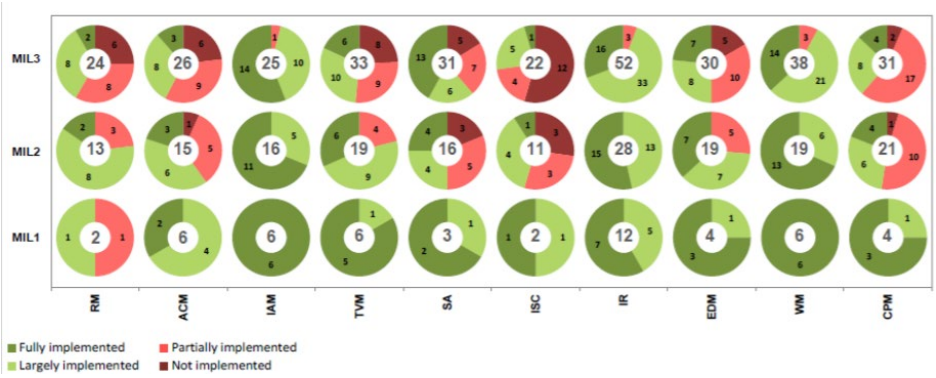
De inhoud van het model wordt op een hoog abstractieniveau gepresenteerd, zodat het kan worden geïnterpreteerd door organisaties van verschillende typen, structuren, groottes en sectoren. Een breed gebruik van het model door een sector kan de benchmarking van de cyberbeveiligingscapaciteiten van de sector ondersteunen.

Weergave van de resultaten

Het C2M2 levert een evaluatierapport op basis van de enquêteresultaten. Het rapport presenteert resultaten in twee weergaven: de doelstellingenweergave (Objective) met de antwoorden op Practice-vragen van elk domein en de desbetreffende doelstellingen en de domeinweergave (Domain) met de antwoorden van alle domeinen en MIL's. Beide weergaven zijn gebaseerd op een weergavesysteem met cirkeldiagrammen (of "donuts"), één per antwoord, en een scoringssysteem met verkeerslichten. Zoals getoond in Figuur 7, geven de rode sectoren in een donutdiagram een telling weer van het aantal vragen waarop in de enquête is geantwoord met "niet uitgevoerd" (donkerrood) of "gedeeltelijk uitgevoerd" (lichtrood). De groene sectoren geven het aantal vragen aan waarop is geantwoord met "Grotendeels uitgevoerd" (lichtgroen) of "Volledig uitgevoerd" (donkergroen).

Figuur 7 is een voorbeeld van een scorekaart aan het einde van een maturiteitsbeoordeling. Op de X-as staan de tien domeinen van het C2M2, en op de Y-as de maturiteitsniveaus (MIL's). Wanneer we naar de grafiek kijken en het domein risicobeheer (RM) in ogenschouw nemen, zien we drie cirkeldiagrammen, één voor elk maturiteitsniveau MIL1, MIL2 en MIL3. Voor het domein RM laat de grafiek zien dat er twee items zijn die moeten worden geëvalueerd om het eerste maturiteitsniveau, MIL1, te bereiken. In dit geval één met de score "grotendeels uitgevoerd" en één met de score "gedeeltelijk uitgevoerd". Voor het tweede maturiteitsniveau, MIL2, voorziet het model in 13 te evalueren items. Twee van die 13 items behoren tot het eerste niveau, MIL1, en elf tot het tweede niveau, MIL2. Hetzelfde geldt voor het derde niveau MIL3.

Figuur 7: C2M2 – Voorbeeld domeinweergave



Fully implemented	Volledig uitgevoerd
Largely implemented	Grotendeels uitgevoerd
Partially implemented	Gedeeltelijk uitgevoerd
Not implemented	Niet uitgevoerd
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	Risicobeheer
ACM	Activa-, wijzigings- en configuratiebeheer
IAM	Identiteits- en toegangsbeheer
TVM	Beheer van dreigingen en kwetsbaarheden
SA	Situationeel bewustzijn
ISC	Uitwisseling van informatie en communicatie
IR	Reactie op gebeurtenissen en incidenten
EDM	Beheer van toeleveringsketens en externe afhankelijkheden
WM	Personeelsbeheer
CPM	Beheer van het cyberbeveiligingsprogramma

Bron: U.S. Department of Energy, Office of electricity delivery and energy reliability, 2015.

A.3 Kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur

Het kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur werd ontwikkeld binnen het National Institute of Standards and Technology (NIST, het Amerikaans nationaal instituut voor normen en technologie). Het kader is gericht zich op het begeleiden van cyberbeveiligingsactiviteiten en het beheren van risico's binnen een organisatie. Ook is het gericht op alle soorten organisaties, ongeacht hun omvang, de mate van cyberbeveiligingsrisico's of de complexiteit van cyberbeveiliging. Aangezien het hier om een framework (kader) en niet om een model gaat, is het anders opgebouwd dan de eerder geanalyseerde modellen.

Het kader bestaat uit drie delen: de kaderkern, de uitvoeringsniveaus en de kaderprofielen:

- De **kaderkern** bestaat uit een reeks cyberbeveiligingsactiviteiten, gewenste resultaten en toepasselijke referenties die gelden voor alle sectoren met kritieke infrastructuur. Deze zijn vergelijkbaar met de eigenschappen of dimensies die in de maturiteitsmodellen voor cyberbeveiligingscapaciteit worden aangetroffen.
- **Uitvoeringsniveaus van het kader** ("niveaus") bieden context over hoe een organisatie aankijkt tegen cyberbeveiligingsrisico's en tegen de processen die zijn uitgevoerd om die risico's te beheersen. Variërend van gedeeltelijk (niveau 1) tot adaptief (niveau 4) beschrijven de niveaus een toenemende mate van striktheid en verfijning in risicobeheerpraktijken op het gebied van cyberbeveiliging. Niveaus vertegenwoordigen geen maturiteitsniveaus, maar zijn bedoeld ter ondersteuning van de besluitvorming binnen de organisatie over de manier waarop

cyberbeveiligingsrisico's moeten worden beheerd en over welke dimensies van de organisatie een hogere prioriteit hebben en extra middelen kunnen krijgen.

- Een **kaderprofiel** ("profiel") vertegenwoordigt de op zakelijke behoeften gebaseerde resultaten die een organisatie heeft geselecteerd uit de kadercategorieën en subcategorieën. Het profiel kan worden gekenmerkt aan de hand van de afstemming van normen, richtsnoeren en praktijken in de kaderkern in een bepaald uitvoeringsscenario. Profielen kunnen worden gebruikt om mogelijkheden voor verbetering van de cyberbeveiligingsmaturiteit vast te stellen door een "huidig profiel" (de huidige status) te vergelijken met een "doelprofiel" (de doelstatus).

Kaderkern

De kaderkern bestaat uit vijf **functies**. Samen bieden deze functies een strategische visie op hoog niveau op de levenscyclus van het beheer van cyberbeveiligingsrisico's door een organisatie. De kaderkern identificeert vervolgens onderliggende **categorieën** en **subcategorieën** voor elke functie en koppelt deze aan voorbeeldinformatie zoals bestaande normen, richtlijnen en praktijken voor elke subcategorie.

De functies en categorieën worden hieronder nader toegelicht:

i **Identificeren**: een organisatorisch inzicht ontwikkelen in de wijze waarop cyberbeveiligingsrisico's voor systemen, mensen, activa, gegevens en capaciteiten moeten worden beheerd.
   - Subcategorieën: activabeheer; bedrijfsomgeving; beleid; risicobeoordeling; en strategie voor risicobeheer

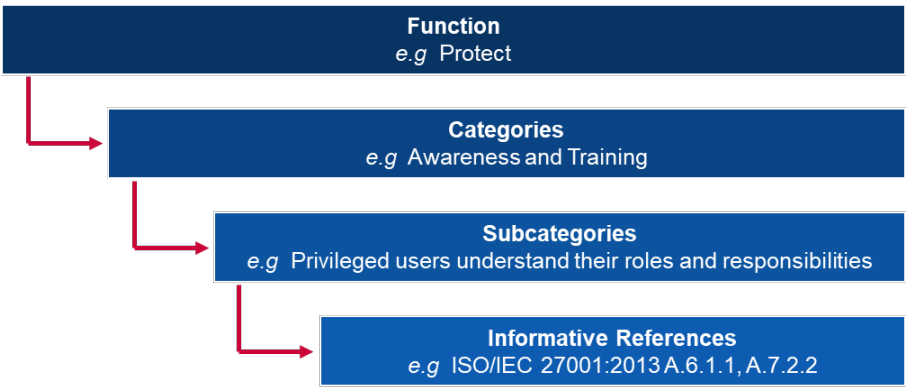
ii **Beschermen**: passende waarborgen ontwikkelen en uitvoeren voor de levering van kritieke diensten.
   - Subcategorieën: identificeren van beheer- en toegangscontrole; bewustmaking en opleiding; databeveiliging; processen en procedures voor informatiebescherming; onderhoud; en beschermingstechnologie

iii **Opsporen**: passende activiteiten ontwikkelen en uitvoeren om vast te stellen of zich een cyberbeveiligingsgebeurtenis heeft voorgedaan.
   - Subcategorieën: gebreken en gebeurtenissen; permanente bewaking van de beveiliging; en opsporingsprocessen.

iv **Reageren**: passende activiteiten ontwikkelen en uitvoeren om actie te ondernemen met betrekking tot een gedetecteerd cyberbeveiligingsincident.
   - Subcategorieën: responsplanning; communicatie; analyse; beperking; en verbeteringen.

v **Herstellen**: passende activiteiten ontwikkelen en uitvoeren om de plannen voor veerkracht te handhaven en de capaciteiten of diensten die als gevolg van een cyberbeveiligingsincident zijn aangetast, te herstellen.
   - Subcategorieën: herstelplanning; verbeteringen; en communicatie

Figuur 8: Voorbeeld van het kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur



Function e.g Project	**Functie** bv. beschermen
Categories e.g Awarness and Training	**Categorieën** bv. bewustwording en opleiding
Subcategories e.g Privileged useres understand their roles and responsibilities	**Subcategorieën**, bv. bevoorrechte gebruikers begrijpen hun rol en verantwoordelijkheden
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informatieve referenties** bv. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Niveaus

Het kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur berust op **vier niveaus**, die langs drie assen worden gedefinieerd: risicobeheerproces, geïntegreerd risicobeheerprogramma en externe participatie. De niveaus moeten niet worden beschouwd als maturiteitsniveaus, maar als een kader om organisaties een beeld te geven van hun visie op cyberbeveiligingsrisico's en de processen die zij hanteren om die risico's te beheren.

- **Niveau 1: Gedeeltelijk**
  - **Risicobeheerproces**: de risicobeheerpraktijken van de organisatie op het gebied van cyberbeveiliging zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd;
  - **Geïntegreerd risicobeheerprogramma**: er is een beperkt bewustzijn van cyberbeveiligingsrisico's op organisatorisch niveau. De organisatie voert het beheer van cyberbeveiligingsrisico's onregelmatig en per geval uit en beschikt mogelijk niet over processen die het delen van informatie over cyberbeveiliging binnen de organisatie mogelijk maken;
  - **Externe deelname**: de organisatie begrijpt niet welke rol zij speelt in het grotere ecosysteem, noch wat betreft haar afhankelijkheden, noch wat betreft haar afhankelijke partijen. De organisatie is zich doorgaans niet bewust van de cyberrisico's in de toeleveringsketen van de producten en diensten die zij levert en die zij gebruikt;
- **Niveau 2: Risicogeïnformeerd**
  - **Risicobeheerproces**: risicobeheerpraktijken worden door het management goedgekeurd, maar worden mogelijk niet als organisatiebreed beleid vastgesteld;
  - **Geïntegreerd risicobeheerprogramma**: er bestaat bewustzijn van het cyberbeveiligingsrisico op organisatieniveau, maar er is geen organisatiebrede aanpak voor het beheer van cyberbeveiligingsrisico's vastgesteld. Er vindt een cyberrisicobeoordeling van organisatorische en externe activa plaats, maar deze wordt doorgaans niet herhaald of kan doorgaans niet herhaald worden;
  - **Externe deelname**: over het algemeen begrijpt de organisatie haar rol in het grotere ecosysteem met betrekking tot ofwel haar eigen afhankelijkheden ofwel afhankelijke partijen, maar niet beide. Bovendien is de organisatie zich bewust van de cyberrisico's in de toeleveringsketen die verbonden zijn aan de producten en diensten die zij levert en gebruikt, maar handelt zij niet consequent of formeel naar deze risico's;
- **Niveau 3: Herhaalbaar**
  - **Risicobeheerproces**: de risicobeheerpraktijken van de organisatie worden formeel goedgekeurd en als beleid geformuleerd. De cyberbeveiligingspraktijken van de organisatie worden regelmatig bijgewerkt door de toepassing van risicobeheerprocessen op veranderingen in de bedrijfs-/opdrachtvereisten en een veranderend bedreigings- en technologielandschap;
  - **Geïntegreerd risicobeheerprogramma**: er is een organisatiebrede aanpak om cyberbeveiligingsrisico's te beheren. Er worden risicogeïnformeerde beleidslijnen, processen en procedures vastgesteld, uitgevoerd zoals bedoeld, en geëvalueerd. Hogere leidinggevenden zorgen ervoor dat cyberbeveiliging in alle geledingen van de organisatie in aanmerking wordt genomen;
  - **Externe deelname**: de organisatie begrijpt haar rol, afhankelijkheden en afhankelijke partijen in het grotere ecosysteem en kan bijdragen aan het bredere inzicht van de gemeenschap in risico's. De organisatie is zich bewust van de cyberrisico's in de toeleveringsketen in verband met de producten en diensten die zij levert en die zij gebruikt;

- **Niveau 4: Adaptief**
  - **Risicobeheerproces**: de organisatie past haar cyberbeveiligingspraktijken aan op basis van eerdere en huidige cyberbeveiligingsactiviteiten, met inbegrip van geleerde lessen en voorspellende indicatoren;
  - **Geïntegreerd risicobeheerprogramma**: er is een organisatiebrede aanpak voor het beheer van cyberbeveiligingsrisico's, waarbij gebruik wordt gemaakt van risicogeïnformeerd beleid, processen en procedures om potentiële cyberbeveiligingsgebeurtenissen aan te pakken; en
  - **Externe deelname**: de organisatie begrijpt haar rol, afhankelijkheden en afhankelijke partijen in het grotere ecosysteem en draagt bij aan het bredere inzicht van de gemeenschap in risico's.

Beoordelingsmethode

Het kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur is bedoeld om organisaties in staat te stellen zelf hun risico's te beoordelen, zodat hun aanpak en investeringen op het gebied van cyberbeveiliging rationeler, doeltreffender en waardevoller worden. Om de doeltreffendheid van investeringen te onderzoeken, moet een organisatie eerst een duidelijk inzicht hebben in haar organisatorische doelstellingen en in de relatie tussen die doelstellingen en de ondersteunende cyberbeveiligingsresultaten. De uitkomsten van de kaderkern ondersteunen de zelfbeoordeling van de doeltreffendheid van investeringen en van cyberbeveiligingsactiviteiten.

A.4 Qatar-maturiteitsmodel inzake cyberbeveiliging (Q-C2M2)

Het Qatar-maturiteitsmodel inzake cyberbeveiliging (Qatar Cybersecurity Capability Maturity Model – Q-C2M2) is in 2018 ontwikkeld door het College of Law van de Qatar University. Het Q-C2M2 is gebaseerd op diverse bestaande modellen om een uitgebreide beoordelingsmethode te ontwikkelen om het cyberbeveiligingskader van Qatar te verbeteren.

Eigenschappen/dimensies

Het Q-C2M2 volgt de aanpak van het kader van het NIST waarbij vijf kernfuncties als de belangrijkste domeinen van het model worden gebruikt. De vijf kernfuncties zijn toepasbaar in de context van Qatar omdat zij in alle sectoren met kritieke infrastructuur voorkomen, een belangrijk element in het Qatarese kader voor cyberbeveiliging. Het Q-C2M2 is gebaseerd op **vijf domeinen**; elk domein is onderverdeeld in verschillende **subdomeinen** die alle maturiteitsmogelijkheden inzake cyberbeveiliging bestrijken.

De vijf domeinen worden hieronder gespecificeerd:

i. Het **domein Begrijpen** omvat vier subdomeinen: cyberbeleid, -activa, -risico's en -opleiding;
ii. De subdomeinen onder het **domein Beveiligen** omvatten Gegevensbeveiliging, Technologiebeveiliging, Beveiliging van toegangscontrole, Communicatiegerelateerde beveiliging en Persoonsgerelateerde beveiliging;
iii. Het **domein Blootstellen** omvat de subdomeinen Monitoring, Incidentenbeheer, Opsporing, Analyse, en Blootstelling;
iv. Het **domein Reageren** omvat Reactieplanning, Beperking en Reactiecommunicatie; en
v. Het **domein In stand houden** omvat Herstelplanning, Continuïteitsbeheer, Verbetering en Externe afhankelijkheden.

Maturiteitsniveaus

Het Q-C2M2 maakt gebruik van **vijf maturiteitsniveaus** om de capaciteitsmaturiteit van een overheidsinstantie of niet-overheidsorganisatie op kernfunctieniveau te meten. Deze niveaus zijn bedoeld om de maturiteit in de vijf in het vorige punt genoemde domeinen te beoordelen.

- **Initiëren**: maakt gebruik van ad-hoccyberbeveiligingspraktijken en -processen in het kader van sommige van de domeinen;

- **Implementeren**: heeft beleid aangenomen om alle cyberbeveiligingsactiviteiten in het kader van de domeinen uit te voeren, met als doel de implementatie op een bepaald tijdstip te voltooien;
- **Ontwikkelen**: heeft beleid en praktijken ten uitvoer gelegd om cyberbeveiligingsactiviteiten in het kader van de domeinen te ontwikkelen en te verbeteren, met als doel nieuwe activiteiten uit te voeren;
- **Adaptief**: bekijkt cyberbeveiligingsactiviteiten en beoordeelt deze, en hanteert praktijken op basis van voorspellende indicatoren die zijn afgeleid van eerdere ervaringen en maatregelen; en
- **Flexibel**: blijft de adaptieve fase uitvoeren met een extra nadruk op flexibiliteit en snelheid bij het uitvoeren van activiteiten in de domeinen.

Beoordelingsmethode

Het Q-C2M2 bevindt zich in een vroeg stadium van onderzoek en is nog niet gebouwd voor uitvoering. Het is een kader dat kan worden gebruikt om in de toekomst een gedetailleerd beoordelingsmodel voor Qatarese organisaties uit te voeren.

A.5 Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)

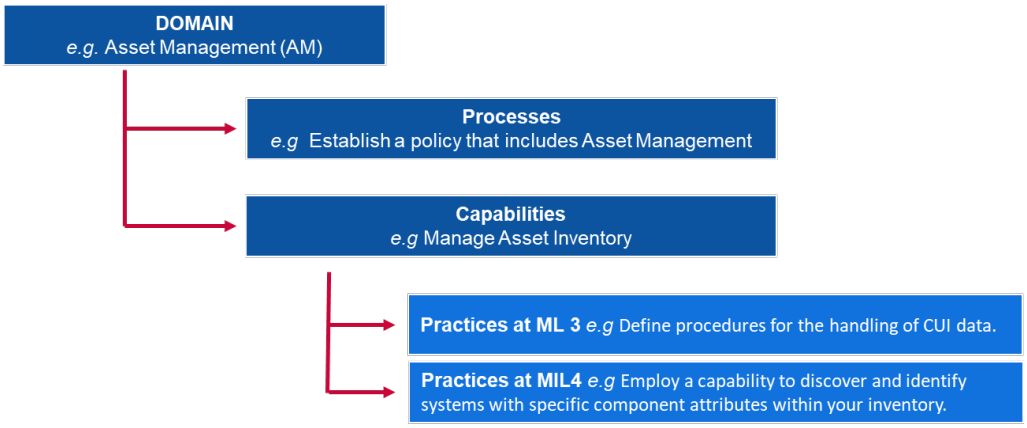
De certificering van het maturiteitsmodel inzake cyberbeveiliging (Cybersecurity Maturity Model Certification – CMMC) werd ontwikkeld door het Amerikaanse ministerie van Defensie (Department of Defense – DoD) in samenwerking met de Carnegie Mellon University en het Johns Hopkins University Applied Physics Laboratory. De belangrijkste doelstelling van het DoD bij het ontwerpen van dit model is het beschermen van informatie uit de defensiesector (Defense Industrial Base – DIB). De informatie waarop het CMMC zich richt, is geclassificeerd als “Federal Contract Information”, informatie die in het kader van een contract wordt verstrekt door of gegenereerd voor de overheid en die niet bestemd is om openbaar te worden gemaakt, of als “Controlled Unclassified Information”, informatie die moet worden beveiligd of verspreid krachtens en in overeenstemming met wet- en regelgeving en overheidsbreed beleid. Het CMMC meet de cyberbeveiligingsmaturiteit en biedt beste praktijken samen met een certificeringselement om de uitvoering van praktijken met betrekking tot elk maturiteitsniveau te garanderen. De laatste versie van het CMMC is uitgebracht in 2020.

Eigenschappen/dimensies

Het CMMC omvat **17 domeinen** die clusters van cyberbeveiligingsprocessen en -capaciteiten vertegenwoordigen. Elk domein wordt dan opgesplitst in meerdere **processen** die gelijkaardig zijn voor verschillende domeinen; en in één tot vele **capaciteiten** die zich uitstrekken over vijf maturiteitsniveaus. De capaciteiten worden vervolgens gespecificeerd in **praktijken** voor elk relevant maturiteitsniveau.

Het verband tussen deze begrippen is als volgt:

Figuur 9: Voorbeeld van CMMC-indicatoren



DOMAIN e.g. Asset Management (AM)	**DOMEIN** , bv. Activabeheer (AM)
Processes e.g Establish a policy that includes Asset Management	**Processen** bv. een beleid vaststellen dat activabeheer omvat
Capabilities e.g Manage Asset Inventory	**Capaciteiten** bv. beheer van inventarisatie van activa
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Praktijken op MIL3** bv. het vaststellen van procedures voor de behandeling van CUI-gegevens
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Praktijken op MIL4** bv. een capaciteit om systemen met specifieke componenteigenschappen binnen de inventaris te ontdekken en te identificeren

De 17 domeinen worden hieronder gespecificeerd:

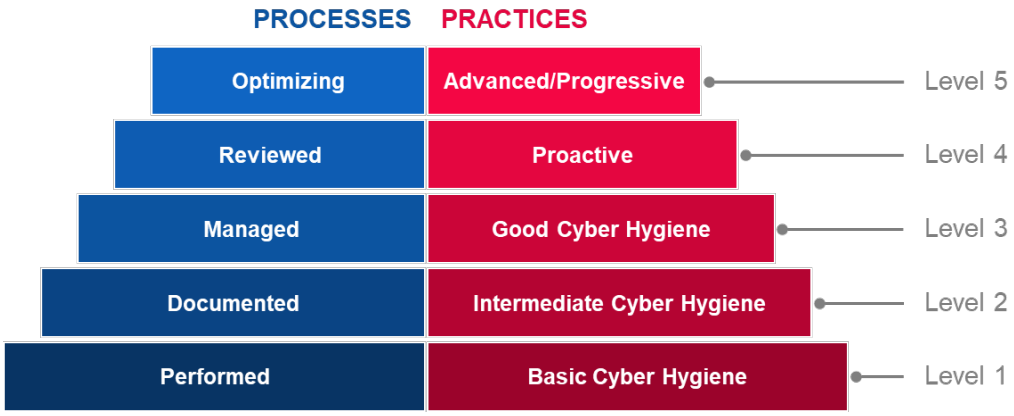
i Toegangscontrole (AC);
ii Activabeheer (AM);
iii Audit en verantwoordingsplicht (AU);
iv Bewustmaking en opleiding (AT);
v Configuratiebeheer (CM);
vi Identificatie en authenticatie (IA);
vii Incidentenrespons (IR);
viii Onderhoud (MA);
ix Mediabescherming (MP);
x Persoonlijke beveiliging (PS);
xi Fysieke bescherming (PE);
xii Herstel (RE);
xiii Risicobeheer (RM);
xiv Beveiligingsbeoordeling (CA);
xv Situationeel bewustzijn (SA);
xvi Systeem- en communicatiebescherming (SC); en
xvii Systeem- en informatie-integriteit (SI).

Maturiteitsniveaus

Het CMMC hanteert **vijf maturiteitsniveaus**, die gedefinieerd worden op basis van processen en praktijken. Om in het CMMC een bepaald maturiteitsniveau te bereiken, moet een organisatie voldoen aan de voorwaarden voor de processen en de praktijken voor dat niveau

zelf. Dit houdt tevens in dat voldaan moet worden aan de voorwaarden van alle niveaus onder dat niveau.

Figuur 10: Maturiteitsniveaus van het CMMC



PROCESSES	Processen
Optimizing	Optimaliseren
Reviewed	Beoordeeld
Managed	Beheerd
Documented	Gedocumenteerd
Performed	Uitgevoerd
PRACTICES	PRAKTIJKEN
Advanced/Progressive	Gevorderd/Progressief
Proactive	Proactief
Good Cyber Hygiene	Goede cyberhygiëne
Intermediate Cyber Hygiene	Intermediaire cyberhygiëne
Basic Cyber Hygiene	Elementaire cyberhygiëne
Level 5	Niveau 5
Level 4	Niveau 4
Level 3	Niveau 3
Level 2	Niveau 2
Level 1	Niveau 1

- **Niveau 1**
  - **Processen – Uitgevoerd**: omdat de organisatie deze praktijken mogelijk alleen op een ad-hocmanier kan uitvoeren en al dan niet kan vertrouwen op documentatie. De procesmaturiteit wordt niet beoordeeld voor niveau 1;
  - **Praktijken – Elementaire cyberhygiëne**: niveau 1 richt zich op de bescherming van FCI (Federal Contract Information) en bestaat alleen uit praktijken die overeenkomen met de basisbeschermingsvereisten;
- **Niveau 2**
  - **Processen – Gedocumenteerd**: niveau 2 vereist dat een organisatie praktijken en beleidslijnen vaststelt en documenteert om de uitvoering van hun CMMC-inspanningen te sturen. Het documenteren van praktijken stelt mensen in staat ze op herhaalbare wijze uit te voeren. Organisaties creëren ontwikkelde capaciteiten door hun processen te documenteren en ze vervolgens in praktijk te brengen zoals gedocumenteerd;
  - **Praktijken – Intermediaire cyberhygiëne**: niveau 2 dient als overgang van niveau 1 naar niveau 3 en bestaat uit een subset van de in NIST SP 800-171

gespecificeerde beveiligingseisen, alsmede uit praktijken van andere normen en referenties;

- **Niveau 3**
  - **Processen – Beheerd**: niveau 3 vereist dat een organisatie een plan opstelt, onderhoudt en van middelen voorziet waaruit het beheer van de activiteiten voor de uitvoering van een praktijk blijkt. Het plan kan informatie bevatten over missies, doelstellingen, projectplannen, middelen, vereiste opleiding, en betrokkenheid van relevante belanghebbenden;
  - **Praktijken – Goede cyberhygiëne**: niveau 3 is gericht op de bescherming van gecontroleerde niet-gerubriceerde gegevens ("Controlled Unclassified Information" – CUI) en omvat alle in NIST SP 800-171 gespecificeerde beveiligingseisen, alsmede aanvullende praktijken uit andere normen en referenties om bedreigingen te beperken;
- **Niveau 4**
  - **Processen – Beoordeeld**: niveau 4 vereist dat een organisatie de praktijken op hun doeltreffendheid toetst en meet. Naast het meten van de doeltreffendheid van praktijken, zijn organisaties op dit niveau in staat corrigerende maatregelen te nemen wanneer dat nodig is en het hoger management op terugkerende basis te informeren over de status of problemen;
  - **Praktijken – Proactief**: niveau 4 is gericht op de bescherming van CUI en omvat een subset van de verbeterde beveiligingseisen. Deze praktijken verbeteren de opsporings- en reactiecapaciteit van een organisatie om de veranderende tactieken, technieken en procedures aan te pakken en zich eraan aan te passen;
- **Niveau 5**
  - **Processen – Optimaliseren**: niveau 5 vereist dat een organisatie de uitvoering van processen in de hele organisatie standaardiseert en optimaliseert; en
  - **Praktijken – Gevorderd/Proactief**: niveau 5 is gericht op de bescherming van CUI. De aanvullende praktijken vergroten de diepgang en het verfijning van de cyberbeveiligingscapaciteiten.

Beoordelingsmethode

Het CMMC is een relatief jong model, dat in het eerste kwartaal van 2020 werd afgerond. Tot dusver is het nog niet in organisaties uitgevoerd. Niettemin verwachten de DoD-contractanten dat zij voor het uitvoeren van audits een beroep zullen doen op gecertificeerde externe onderzoekers. Het DoD verwacht van zijn contractanten dat zij beste praktijken toepassen om de cyberbeveiliging en de bescherming van gevoelige informatie te bevorderen.

A.6 Communautair maturiteitsmodel voor cyberbeveiliging (CCSMM)

Het communautair maturiteitsmodel voor cyberbeveiliging (CCSMM) werd ontwikkeld door het Centre for Infrastructure Assurance and Security van de Universiteit van Texas. Het doel van het CCSMM is beter methoden te definiëren om de huidige status van een gemeenschap qua cyberparaatheid te bepalen en een routekaart te bieden die gemeenschappen kunnen volgen bij hun voorbereidingen. De gemeenschappen waarop het CCSMM zich richt, zijn hoofdzakelijk plaatselijke of deelstaatoverheden. Het CCSMM werd ontworpen in 2007.

Eigenschappen/dimensies

De maturiteitsniveaus worden gedefinieerd volgens **zes hoofddimensies** die de verschillende aspecten van cyberbeveiliging binnen gemeenschappen en organisaties bestrijken. Deze dimensies worden duidelijk vastgesteld voor elk maturiteitsniveau (gespecificeerd in Figuur 11: Samenvatting van de **dimensies** van het CCSMM) De zes dimensies zijn:

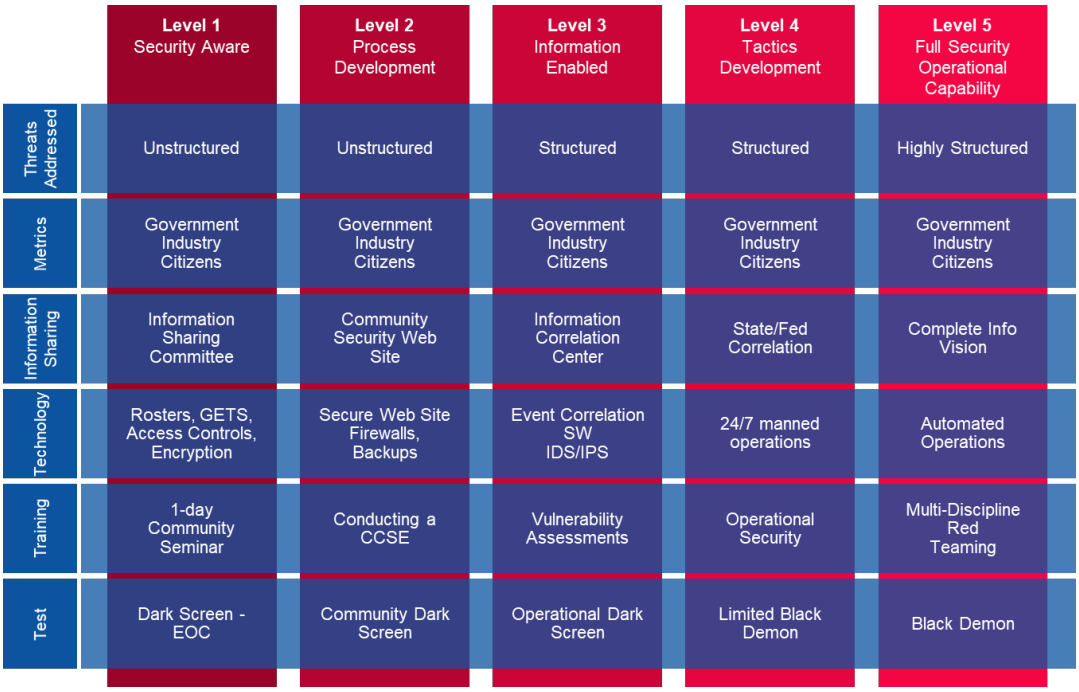
i Aangepakte bedreigingen;
ii Meetwaarden;
iii Delen van informatie;
iv Technologie;
v Opleiding; en
vi Toetsing.

Maturiteitsniveaus

Het CCSMM berust op **vijf maturiteitsniveaus**, gebaseerd op de belangrijkste soorten dreigingen en activiteiten die op het niveau worden aangepakt:

- **Niveau 1: beveiligingsbewust**
  Het belangrijkste thema van activiteiten op dit niveau is personen en organisaties bewust te maken van de dreigingen en problemen met betrekking tot cyberbeveiliging;
- **Niveau 2: procesontwikkeling**
  Dit niveau is bedoeld om gemeenschappen te helpen bij het vaststellen en verbeteren van beveiligingsprocessen die nodig zijn om cyberbeveiligingskwesties doeltreffend aan te pakken;
- **Niveau 3: informatiegestuurd**
  Ontworpen om de mechanismen voor informatie-uitwisseling binnen de gemeenschap te verbeteren, zodat de gemeenschap ogenschijnlijk ongelijksoortige informatie doeltreffend kan correleren.
- **Niveau 4: tactiekontwikkeling**
  De elementen van dit niveau zijn bedoeld om betere en meer proactieve methoden te ontwikkelen om aanvallen op te sporen en erop te reageren. Op dit niveau zouden de meeste preventiemethoden in werking moeten zijn.
- **Niveau 5: volledige operationele beveiligingscapaciteit**
  Dit niveau vertegenwoordigt de elementen die aanwezig moeten zijn, wil een organisatie zichzelf als volledig operationeel gereed beschouwen om elk type cyberdreiging het hoofd te bieden.

Figuur 11: Samenvatting van de dimensies van het CCSMM per niveau



Level 1 Security Aware	Niveau 1 Beveiligingsbewust
Level 2 Process Development	Niveau 2 Procesontwikkeling
Level 3 Information Enabled	Niveau 3 Informatiegestuurd
Level 4 Tactics Development	Niveau 4 Tactiekontwikkeling
Level 5 Full Security Operational Capability	Niveau 5 Volledige operationele beveiligingscapaciteit

Threats Addressed	Aangepakte bedreigingen
Metrics	Meetwaarden
Information sharing	Delen van informatie
Technology	Technologie
Training	Training
Test	Toetsing
Unstructured	Ongestructureerd
Governement Industry Citizens	Overheid Sector Burgers
Information Sharing Committee	Comité voor het delen van informatie
Rosters, GETS, Assess Controls, Encryption	Roosters, GETS, controles beoordelen, encryptie
1-dat Community Seminar	Eendaags communautair seminar
Dark Screen – EOC	Donker scherm – EOC
Unstructured	Ongestructureerd
Governement Industry Citizens	Overheid Sector Burgers
Community Security Web site	Website voor beveiliging van de gemeenschap
Secure Web Site Firewalls, Backups	Veilige websitefirewalls, back-ups
Conudcting a CCSE	Een CCSE uitvoeren
Community Dark Screen	Community Dark Screen
Structured	Gestructureerd
Governement Industry Citizens	Overheid Sector Burgers
Information Correlation Center	Centrum voor informatiecorrelatie
Event Correlation SW IDS/IPS	Gebeurteniscorrelatie SW IDS/IPS
Vulnerability Assessment	Kwetsbaarheidsbeoordeling
Operational Dark Screen	Operational Dark Screen
Structured	Gestructureerd
Governement Industry Citizens	Overheid Sector Burgers
State/Fed Correlation	Correlatie tussen staat/fed
24/7 manned operations	24/7 bemande operaties
Operational Security	Operationele veiligheid
Limited Black Demon	Limited Black Demon
Highly Structured	Zeer gestructureerd
Governement Industry Citizens	Overheid Sector Burgers
Complete Info Vision	Compleet infobeeld
Automated Operations	Geautomatiseerde operaties
Multi-Discipline Red Teaming	Multidisciplinair red teaming
Black Demon	Black Demon

Beoordelingsmethode

Het CCSMM is als evaluatiemethode bedoeld om te worden toegepast door gemeenschappen met inbreng van nationale en federale rechtshandhavingsautoriteiten. Het is bedoeld de gemeenschap te helpen bepalen wat het belangrijkste is, wat de meest waarschijnlijke doelen zijn, en wat moet worden beschermd (en in welke mate). Met deze doelstellingen voor ogen kunnen plannen worden ontwikkeld om elk aspect van de gemeenschap op het vereiste niveau van cyberbeveiligingsmaturiteit te brengen. De specifieke inlichtingen die het CCSMM oplevert, helpen bij het bepalen van de doelstellingen van diverse tests en oefeningen die kunnen worden gebruikt om de doeltreffendheid van gevestigde programma's te meten.

A.7 Maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (ISMM)

Het maturiteitsmodel inzake informatiebeveiliging (ISMM) is ontwikkeld binnen het College van computerwetenschappen en technologie van de King Fahd-Universiteit voor Aardolie en Mineralen in Saoedi-Arabië. Het voorziet in een nieuw model voor capaciteitsmaturiteit om de uitvoering van cyberbeveiligingsmaatregelen te meten. Het doel van het ISMM is organisaties in staat te stellen de voortgang van hun uitvoering in de tijd te meten door op regelmatige basis hetzelfde meetinstrument te gebruiken om ervoor te zorgen dat de gewenste beveiligingsmaturiteit wordt gehandhaafd. Het ISMM werd ontwikkeld in 2017.

Eigenschappen/dimensies

Het ISMM bouwt voort op de bestaande beoordeelde gebieden van het NIST-kader en voegt een dimensie toe over nalevingsbeoordeling. Dit brengt het model op **23 beoordeelde gebieden** voor de beveiligingsmaturiteit van een organisatie. De 23 beoordeelde gebieden zijn:

i Activabeheer;
ii Bedrijfsomgeving;
iii Beleid;
iv Risicobeoordeling;
v Strategie voor risicobeheer;
vi Nalevingsbeoordeling;
vii Toegangscontrole;
viii Bewustmaking en opleiding;
ix Gegevensbeveiliging;
x Processen en procedures voor informatiebescherming;
xi Onderhoud;
xii Beschermende technologie;
xiii Gebreken en gebeurtenissen;
xiv Permanente bewaking van de beveiliging;
xv Opsporingsprocessen;
xvi Responsplanning;
xvii Responscommunicatie;
xviii Responsanalyse;
xix Responsbeperking;
xx Responsverbeteringen;
xxi Herstelplanning;
xxii Herstelverbeteringen; en
xxiii Herstelcommunicatie.

Maturiteitsniveaus

Het ISMM berust op **vijf maturiteitsniveaus**, die in de beschikbare documentatie helaas niet nader worden uitgewerkt.

- **Niveau 1:** uitgevoerd proces;
- **Niveau 2:** beheerd proces;
- **Niveau 3:** tot stand gebracht proces;
- **Niveau 4:** voorspelbaar proces; en
- **Niveau 5:** optimaliseren van het proces.

Beoordelingsmethode

Het ISMM stelt geen specifieke methode voor om de beoordeling voor organisaties uit te voeren.

A.8 Model voor interne controlecapaciteit voor de publieke sector (IA-CM) voor de publieke sector

Het model voor interne controlecapaciteit voor de publieke sector (Internal Audit Capability Model – IA-CM) werd ontwikkeld door de Institute of Internal Auditors Research Foundation met de bedoeling capaciteit op te bouwen en bewustzijn te creëren door middel van zelfevaluatie in de publieke sector. Het IA-CM is gericht op auditprofessionals en biedt een overzicht van het model zelf, samen met een toepassingsgids die dient als ondersteuning bij het gebruik van het model als een instrument voor zelfbeoordeling.

Hoewel het IA-CM gericht is op interne-auditcapaciteit, en niet op de opbouw van cyberbeveiligingscapaciteit, is het model ontworpen als een instrument voor zelfbeoordeling van de maturiteit van entiteiten in de publieke sector, dat wereldwijd kan worden toegepast om processen en doeltreffendheid te verbeteren. Aangezien het toepassingsgebied niet op cyberbeveiliging is toegespitst, zullen de eigenschappen niet worden geanalyseerd. Het IA-CM werd in 2009 voltooid.

Maturiteitsniveaus

Het model voor interne controlecapaciteit voor de publieke sector (IA-CM) omvat **vijf maturiteitsniveaus**, die elk de kenmerken en capaciteiten van een interne-auditactiviteit op dat niveau beschrijven. De capaciteitsniveaus in het model bieden een routekaart voor voortdurende verbetering.

- **Niveau 1: initieel**
  Geen duurzame, herhaalbare capaciteiten - afhankelijk van individuele inspanningen
  - Ad hoc of ongestructureerd.
  - Geïsoleerde afzonderlijke audits of controles van documenten en transacties op nauwkeurigheid en naleving.
  - Output afhankelijk van de vaardigheden van de specifieke persoon die de positie bekleedt.
  - Geen andere beroepspraktijken vastgesteld dan die van beroepsverenigingen.
  - Financieringsgoedkeuring door het management, indien nodig.
  - Ontbreken van infrastructuur.
  - Auditors maken waarschijnlijk deel uit van een grotere organisatorische eenheid.
  - De institutionele capaciteit is niet ontwikkeld.
- **Niveau 2: infrastructuur**
  Duurzame en herhaalbare praktijken en procedures
  - De belangrijkste vraag of uitdaging voor niveau 2 is hoe de herhaalbaarheid van processen en dus een herhaalbare capaciteit tot stand kan worden gebracht en in stand kan worden gehouden.
  - Er worden rapportagerelaties, beheers- en administratieve infrastructuren voor interne controle en beroepspraktijken en -procedures tot stand gebracht (internecontrolerichtsnoeren, -processen en -procedures).
  - Auditplanning voornamelijk gebaseerd op managementprioriteiten.
  - Voortdurend vertrouwen, hoofdzakelijk op de vaardigheden en bekwaamheden van specifieke personen.
  - Gedeeltelijke overeenstemming met de normen.
- **Niveau 3: geïntegreerd**
  Beheer en beroepspraktijken uniform toegepast
  - Beleid, processen en procedures voor interne controle worden vastgesteld, gedocumenteerd en geïntegreerd in elkaar en in de infrastructuur van de organisatie.
  - Het beheer en de beroepspraktijken op het gebied van interne controle zijn goed ingeburgerd en worden uniform toegepast voor de hele internecontroleactiviteit.
  - De interne controle begint zich af te stemmen op de activiteiten van de organisatie en de risico's waarmee zij wordt geconfronteerd.
  - De interne controle evolueert van het uitvoeren van uitsluitend traditionele interne audits naar het integreren als teamspeler en het verstrekken van advies over prestaties en risicobeheer.
  - De nadruk ligt op teambuilding en de capaciteit van de internecontroleactiviteit en haar onafhankelijkheid en objectiviteit.

- Meestal in overeenstemming met de normen.

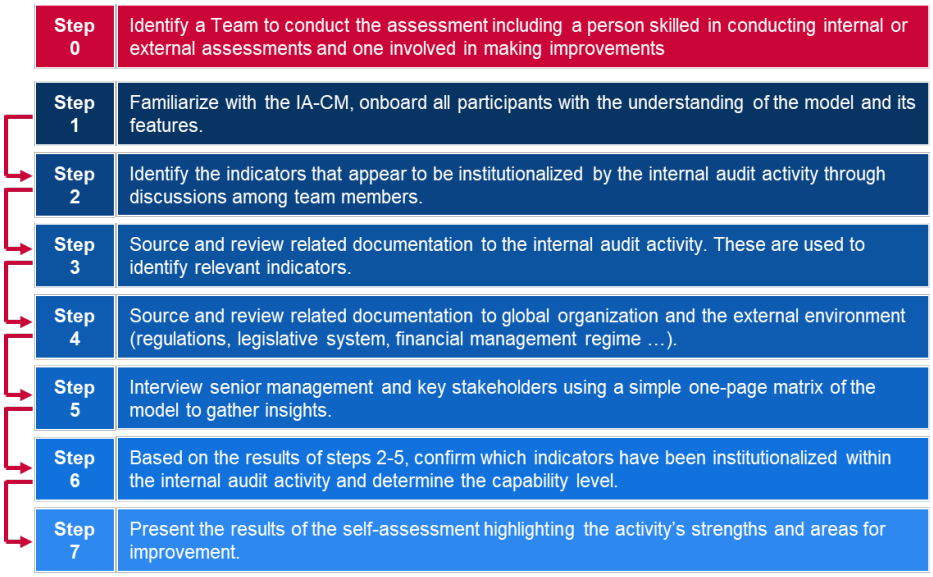
- **Niveau 4: beheerd**
  Integreert informatie uit de hele organisatie om het beleid en het risicobeheer te verbeteren
  - De verwachtingen van de interne controle en de voornaamste belanghebbenden zijn op elkaar afgestemd.
  - Er bestaan prestatiemeetwaarden om de internecontroleprocessen en -resultaten te meten en te monitoren.
  - Er wordt erkend dat de interne controle een belangrijke bijdrage levert aan de organisatie.
  - Interne controle fungeert als integraal onderdeel van het beleid en het risicobeheer van de organisatie.
  - Interne controle is een goed beheerde bedrijfseenheid.
  - Risico's worden kwantitatief gemeten en beheerd.
  - De vereiste vaardigheden en competenties zijn aanwezig, met een capaciteit voor vernieuwing en kennisdeling (binnen interne audit en in de hele organisatie).

- **Niveau 5: optimaliseren**
  Binnen en buiten de organisatie leren met het oog op voortdurende verbetering
  - Interne controle is een leerproces met voortdurende procesverbeteringen en innovatie.
  - Bij interne controle wordt gebruikgemaakt van informatie van binnen en buiten de organisatie om bij te dragen tot de verwezenlijking van de strategische doelstellingen.
  - Prestatie van wereldklasse/aanbevolen/beste praktijken.
  - Interne controle is een essentieel onderdeel van de beleidsstructuur van de organisatie.
  - Professionele en gespecialiseerde vaardigheden van topniveau.
  - De prestatiemaatstaven op individueel, eenheids- en organisatorisch niveau worden volledig geïntegreerd om
  - de prestaties te verbeteren.

Beoordelingsmethode

Het model voor interne controlecapaciteit is duidelijk bedoeld voor zelfbeoordeling. Het bevat gedetailleerde stappen voor het gebruik van het IA-CM en diaset met voorbeeldslides die kunnen worden aangepast. Voordat met de zelfbeoordeling wordt begonnen, moet een specifiek team worden samengesteld dat ten minste één persoon bevat die deskundige is op het gebied van het uitvoeren van interne of externe beoordelingen van interne controles, alsook één persoon die betrokken is bij het aanbrengen van verbeteringen op dit gebied.

Figuur 12: Stappen voor zelfbeoordeling van het IA-CM



Step 0	Stap 0
Step 1	Stap 1
Step 2	Stap 2
Step 3	Stap 3
Step 4	Stap 4
Step 5	Stap 5
Step 6	Stap 6
Step 7	Stap 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Een team samenstellen om de beoordeling uit te voeren, waaronder een persoon met ervaring in het uitvoeren van interne of externe beoordelingen en een persoon die betrokken is bij het aanbrengen van verbeteringen.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Vertrouwd raken met het IA-CM, alle deelnemers vertrouwd maken met het model en de kenmerken ervan.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	De indicatoren aanwijzen die door de internecontroleactiviteit geïnstitutionaliseerd lijken te zijn via besprekingen onder teamleden.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Gerelateerde documentatie voor de internecontroleactiviteit verkrijgen en beoordelen. Deze worden gebruikt om relevante indicatoren te bepalen.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Gerelateerde documentatie voor de mondiale organisatie en de externe omgeving (regelgeving, wetgevingssysteem, financieel beheer enz.) verkrijgen en beoordelen.
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Het hoger management en de belangrijkste belanghebbenden interviewen aan de hand van een eenvoudige matrix van het model van één bladzijde om inzichten te verzamelen.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Op basis van de resultaten van de stappen 2-5 bevestigen welke indicatoren binnen de internecontroleactiviteit zijn geïnstitutionaliseerd en het capaciteitsniveau bepalen.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	De resultaten van de zelfbeoordeling presenteren met focus op de sterke punten van de activiteit en de gebieden die voor verbetering vatbaar zijn.

A.9 De wereldwijde index voor cyberbeveiliging (GCI)

De wereldwijde index voor cyberbeveiliging (Global Cybersecurity Index – GCI) is een initiatief van de Internationale Telecommunicatie-unie (ITU) dat tot doel heeft de betrokkenheid en de situatie op het gebied van cyberbeveiliging in alle ITU-regio's te evalueren: Afrika, Noord- en Zuid-Amerika, de Arabische staten, Azië-Stille Oceaan, het GOS en Europa, en zet landen met een grote betrokkenheid en aanbevelenswaardige praktijken in de schijnwerpers. Het doel van de GCI is om landen te helpen bij het vaststellen van verbeterpunten op het gebied van cyberbeveiliging en hen te motiveren actie te ondernemen om hun rangschikking te verbeteren en zo het algehele niveau van cyberbeveiliging wereldwijd te helpen verhogen.

Aangezien de GCI een index is en geen maturiteitsmodel, wordt er geen gebruik gemaakt van maturiteitsniveaus maar van een score om de globale betrokkenheid met betrekking tot cyberbeveiliging van landen en regio's te rangschikken en te vergelijken.

Eigenschappen/dimensies

De wereldwijde index voor cyberbeveiliging (GCI) is gebaseerd op de vijf pijlers van de Global Cybersecurity Agenda (GCA). Deze pijlers vormen de vijf subindexen van de GCI en omvatten elk een reeks indicatoren. De vijf pijlers en indicatoren zijn als volgt:

i **Juridisch**: maatregelen gebaseerd op het bestaan van juridische instellingen en kaders die zich bezighouden met cyberbeveiliging en cybercriminaliteit.
- wetgeving inzake cybercriminaliteit;
- regelgeving inzake cyberbeveiliging; en
- indamming van spamwetgeving.

ii **Technisch**: maatregelen gebaseerd op het bestaan van technische instellingen en kaders die zich bezighouden met cyberbeveiliging.
- CERT/CIRT/CSRIT;
- uitvoeringskader voor normen;
- normalisatie-instelling;
- technische mechanismen en capaciteiten om spam aan te pakken;
- gebruik van de cloud voor cyberbeveiligingsdoeleinden; en
- mechanismen voor online bescherming van kinderen.

iii **Organisatorisch**: maatregelen gebaseerd op het bestaan van instellingen voor beleidscoördinatie en strategieën voor de ontwikkeling van cyberbeveiliging op nationaal niveau.
- nationale strategie voor cyberbeveiliging;
- verantwoordelijke instantie; en
- cyberbeveiliging.

iv **Capaciteitsopbouw**: maatregelen gebaseerd op het bestaan van onderzoek en ontwikkeling, onderwijs- en opleidingsprogramma's, gecertificeerde professionals en openbare instanties die de capaciteitsopbouw bevorderen.
- openbare bewustmakingscampagnes;
- kader voor de certificering en accreditering van cyberbeveiligingsprofessionals;
- beroepsopleidingen op het gebied van cyberbeveiliging;
- onderwijsprogramma's of academische leerplannen op het gebied van cyberbeveiliging;
- O&O-programma's op het gebied van cyberbeveiliging; en
- stimuleringsmechanismen.

v **Samenwerking:** maatregelen gebaseerd op het bestaan van partnerschappen, samenwerkingsverbanden en netwerken voor informatie-uitwisseling.
- bilaterale overeenkomsten;
- multilaterale overeenkomsten;
- deelname aan internationale fora/verenigingen;
- publiek-private partnerschappen;
- partnerschappen binnen en tussen instanties; en
- beste praktijken.

Beoordelingsmethode

De GCI is een instrument voor zelfbeoordeling dat werd ontwikkeld via een enquête[30] van binaire, vooraf gecodeerde en open vragen. Het gebruik van binaire antwoorden sluit op meningen gebaseerde evaluatie en mogelijke vooringenomenheid uit ten aanzien van bepaalde soorten antwoorden. De voorgecodeerde antwoorden besparen tijd en maken een nauwkeurigere gegevensanalyse mogelijk. Bovendien maakt een eenvoudige dichotome schaal een snellere en complexere evaluatie mogelijk, omdat er geen lange antwoorden nodig zijn, waardoor het proces van antwoorden geven en verdere evaluatie wordt versneld en

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

gestroomlijnd. De respondent dient alleen de aanwezigheid van, of het ontbreken van, bepaalde vooraf geïdentificeerde cyberbeveiligingsoplossingen te bevestigen. Via een online-enquêtemechanisme, dat wordt gebruikt voor het verzamelen van antwoorden en het uploaden van relevant materiaal, kunnen goede praktijken en een reeks thematische kwalitatieve evaluaties door een groep van deskundigen worden geëxtraheerd.

Het algemene GCI-proces wordt als volgt uitgevoerd:

- Aan alle deelnemers wordt een uitnodigingsbrief gestuurd, waarin zij worden geïnformeerd over het initiatief en waarin wordt gevraagd een steunpunt aan te wijzen dat verantwoordelijk is voor het verzamelen van alle relevante gegevens en voor het invullen van de online GCI-vragenlijst. Tijdens de online-enquête wordt het goedgekeurde steunpunt officieel door de ITU uitgenodigd om de vragenlijst te beantwoorden;
- Primaire gegevensverzameling (voor landen die de vragenlijst niet beantwoorden):
  - ITU werkt een eerste ontwerp-antwoord op de vragenlijst uit met behulp van openbaar beschikbare gegevens en online-onderzoek;
  - De ontwerp-vragenlijst wordt ter beoordeling aan de steunpunten toegezonden;
  - De steunpunten verbeteren de nauwkeurigheid en sturen vervolgens de ontwerp-vragenlijst terug;
  - De gecorrigeerde ontwerp-vragenlijst wordt ter definitieve goedkeuring aan elk steunpunt toegezonden; en
  - De gevalideerde vragenlijst wordt gebruikt voor analyse, scoring en rangschikking.
- Secundaire gegevensverzameling (voor landen die de vragenlijst beantwoorden):
  - ITU identificeert alle ontbrekende antwoorden, ondersteunende documenten, links, enz.;
  - Het steunpunt verbetert de nauwkeurigheid van de antwoorden waar nodig;
  - De gecorrigeerde ontwerp-vragenlijst wordt ter definitieve goedkeuring aan elk steunpunt toegezonden; en
  - De gevalideerde vragenlijst wordt gebruikt voor analyse, scoring en rangschikking.

A.10 Index voor cybermacht (CPI)

De index voor cybermacht (Cyber Power Index – CPI) werd in 2011 gecreëerd door het onderzoeksprogramma van de Economist Intelligence Unit, dat wordt gesponsord door Booz Allen Hamilton. De CPI is een “dynamisch kwantitatief en kwalitatief model, [...] dat specifieke kenmerken van de cyberomgeving meet aan de hand van vier drijvende krachten achter cybermacht: wet- en regelgevingskader; economische en sociale context; technologische infrastructuur; en toepassing in de sector, waarbij de digitale vooruitgang in belangrijke sectoren wordt onderzocht”[31]. Het doel van de Cyber Power Index is om het vermogen van de G20-landen te benchmarken om cyberaanvallen te weerstaan en de vereiste digitale infrastructuur in te zetten voor een bloeiende en veilige economie. De door de CPI verschafte benchmark richt zich op 19 landen van de G20 (met uitzondering van de EU). De index geeft vervolgens een rangschikking van landen voor elke indicator.

Eigenschappen/dimensies

De Cyber Power Index (CPI) is gebaseerd op vier bepalende factoren voor cyberpower. Elke categorie wordt vervolgens gemeten aan de hand van meerdere indicatoren om elk land een specifieke score te geven. De categorieën en pijlers zijn als volgt:

i **Wet en regelgeving**
  - Engagement van de regering voor cyberontwikkeling

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Beleid voor cyberbeveiliging
- Cybercensuur (of het gebrek daaraan)
- Politieke doeltreffendheid
- Bescherming van intellectuele eigendom

ii **Economische en sociale context**

- Opleidingsniveaus
- Technische vaardigheden
- Openheid van handel
- Mate van innovatie in het ondernemingsklimaat

iii **Technologie-infrastructuur**

- Toegang tot informatie- en communicatietechnologie
- Kwaliteit van informatie- en communicatietechnologie
- Betaalbaarheid van informatie- en communicatietechnologie
- Uitgaven voor informatietechnologie
- Aantal beveiligde servers

iv **Sectortoepassing**

- Slimme netten
- E-gezondheid
- E-commerce
- Intelligent vervoer
- E-overheid

Beoordelingsmethode

De CPI is een kwantitatief en kwalitatief scoremodel. De beoordeling is uitgevoerd door The Economist Intelligence Unit, waarbij gebruik is gemaakt van kwantitatieve indicatoren uit beschikbare statistische bronnen en van ramingen wanneer gegevens ontbraken. De voornaamste gebruikte bronnen zijn de Economist Intelligence Unit; de Organisatie van de VN voor Onderwijs, Wetenschap en Cultuur (UNESCO); de Internationale Telecommunicatie-unie (ITU); en de Wereldbank.

A.11 De Cyber Power Index (CPI)

In dit deel worden de belangrijkste bevindingen van de analyse van de bestaande maturiteitsmodellen samengevat. Tabel 5: Overzicht van geanalyseerde maturiteitsmodellen geeft een overzicht van de belangrijkste kenmerken van elk model volgens het gewijzigde model van Becker. Tabel 6 Vergelijking van maturiteitsniveaus bevat de definities op hoog niveau van de maturiteitsniveaus van de geanalyseerde modellen. Tabel 7 geeft een overzicht van de dimensies of eigenschappen die in elk model worden gebruikt.

Tabel 5: Overzicht van geanalyseerde maturiteitsmodellen

Naam model	Bron (instelling)	Doel	Target	Aantal niveaus	Aantal eigenschappen	Beoordelingsmethode	Weergave van de resultaten
Maturiteitsmodel inzake cyberbeveiliging voor naties (CMM)	Mondiaal capaciteitscentrum voor cyberbeveiliging Universiteit van Oxford	De schaal en doeltreffendheid van de internationale capaciteitsopbouw op het gebied van cyberbeveiliging vergroten	Landen	5	5 hoofddimensies	Samenwerking met lokale organisatie om het model te verfijnen alvorens het toe te passen op de nationale context	Vijfdelige radar
Maturiteitsmodel inzake cyberbeveiligingscapaciteit (C2M2)	Amerikaans ministerie van Energie (DoE)	Organisaties helpen om hun cyberbeveiligingsprogramma's te evalueren en te verbeteren en hun operationele veerkracht te versterken	Organisaties van alle sectoren, soorten en maten	4	10 hoofddomeinen	Methode en toolkit voor zelfevaluatie	Scorekaart met cirkeldiagrammen
Kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur	National Institute of Standards and Technology (NIST)	Kader voor het sturen van cyberbeveiligingsactiviteiten en het beheren van risico's binnen organisaties	Organisaties	n.v.t. (4 niveaus)	5 kernfuncties	Zelfbeoordeling	-
Qatar-maturiteitsmodel inzake cyberbeveiliging (Q-C2M2)	College of Law van de Universiteit van Qatar	Een werkbaar model aanreiken dat kan worden gebruikt om het cyberbeveiligingskader van Qatar te benchmarken, te meten en te ontwikkelen	Qatarese organisaties	5	5 hoofddomeinen	-	-
Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)	Amerikaans ministerie van Defensie (DoD)	Beste praktijken op het gebied van cyberbeveiliging bevorderen om informatie te beschermen	Organisaties in de defensiesector (DIB)	5	17 hoofddomeinen	Beoordeling door externe controleurs	-
Communautair maturiteitsmodel voor cyberbeveiliging (CCSMM))	Centrum voor infrastructuurgarantie en -beveiliging, Universiteit van Texas	De huidige status van een gemeenschap in haar cyberparaatheid bepalen en een routekaart opstellen die gemeenschappen kunnen volgen bij hun voorbereidingen	Gemeenschappen (lokale of deelstaatoverheden)	5	6 hoofddimensies	Beoordeling binnen gemeenschappen met input van de staats- en federale rechtshandhavingsautoriteiten	-
Maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (ISMM)	College van computerwetenschappen en technologie King Fahd-Universiteit voor Aardolie en Mineralen, Dhahran, Saoedi-Arabië	Organisaties in staat stellen de voortgang van hun implementatie in de loop van de tijd te meten om ervoor te zorgen dat zij de gewenste beveiligingsmaturiteit behouden	Organisaties	5	23 beoordeelde gebieden	-	-
Model voor interne controlecapaciteit voor de publieke sector (IA-CM) voor de publieke sector	Het Institute of Internal Auditors Research Foundation	Interne auditcapaciteit opbouwen en bewustzijn creëren door zelfevaluatie in de publieke sector	Organisaties uit de publieke sector	5	6 elementen	Zelfbeoordeling	-

Wereldwijde index voor cyberbeveiliging (GCI)	Internationale Telecommunicatie-unie (ITU)	Het engagement en de situatie wat betreft cyberbeveiliging evalueren en landen helpen bij het vaststellen van gebieden waarop verbetering op het gebied van cyberbeveiliging mogelijk is	Landen	n.v.t.	5 pijlers	Zelfbeoordeling	Ranglijst
Index voor cybermacht (CPI)	De Economist Intelligence Unit & Booz Allen Hamilton	De capaciteit van de G20-landen benchmarken om cyberaanvallen te weerstaan en de vereiste digitale infrastructuur in te zetten voor een bloeiende en veilige economie.	G20-landen	n.v.t.	4 categorieën	Benchmarking door de Economist Intelligence Unit	Ranglijst

Tabel 6 Vergelijking van maturiteitsniveaus

Model	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Maturiteitsmodel inzake cyberbeveiliging voor naties (CMM)	**Initieel** De cyberbeveiligingsmaturiteit is ofwel nihil ofwel nog zeer embryonaal van aard. Er zijn weliswaar eerste besprekingen over capaciteitsopbouw op het gebied van cyberbeveiliging, maar er werden geen concrete acties ondernomen. In deze fase is er geen waarneembaar bewijs.	**Formatief** Sommige kenmerken van de aspecten beginnen te groeien en worden onder woorden gebracht, maar kunnen ad hoc, ongeorganiseerd, slecht gedefinieerd – of gewoon 'nieuw' zijn. Deze activiteit kan echter duidelijk aangetoond worden.	**Vastgesteld** De elementen van het aspect zijn operationeel en werken. Er is echter niet goed nagedacht over de relatieve toewijzing van middelen. Er zijn weinig afwegingen gemaakt met betrekking tot de 'relatieve' investering in de verschillende elementen van het aspect. Het aspect is echter functioneel en vastgesteld.	**Strategisch** Er zijn keuzes gemaakt over welke delen van het aspect belangrijk zijn, en welke minder belangrijk zijn voor de specifieke organisatie of natie. De strategische fase weerspiegelt het feit dat deze keuzes zijn gemaakt, afhankelijk van de omstandigheden van de natie of organisatie.	**Dynamisch** Er zijn duidelijke mechanismen voorhanden om de strategie te wijzigen afhankelijk van de heersende omstandigheden, zoals de technologie van de bedreigingsomgeving, een wereldwijd conflict of een significante verandering op een bepaald gebied (bv. cybercriminaliteit of privacy). Dynamische organisaties hebben methoden ontwikkeld om strategieën soepel te wijzigen. Snelle besluitvorming, herverdeling van middelen en voortdurende aandacht voor de veranderende omgeving zijn kenmerken van deze fase.
Maturiteitsmodel inzake cyberbeveiligingscapaciteit (C2M2)	**MIL0** Er worden geen praktijken uitgevoerd.	**MIL1** Er worden initiële praktijken uitgevoerd, maar dit kan op ad-hocbasis zijn.	**MIL2** Kenmerken van het beheer: praktijken worden gedocumenteerd; er worden passende middelen ter beschikking gesteld om het proces te ondersteunen; het personeel dat de praktijken uitvoert, beschikt over voldoende vaardigheden en kennis; en er worden verantwoordelijkheid en bevoegdheid voor de uitvoering van de praktijken toegewezen.	**MIL3** Kenmerken van het beheer: activiteiten worden gestuurd door beleid (of andere richtlijnen van de organisatie); er worden prestatiedoelstellingen voor domeinactiviteiten vastgesteld en gemonitord om de prestaties te volgen; en gedocumenteerde praktijken voor domeinactiviteiten worden gestandaardiseerd en verbeterd binnen de onderneming.	-

			Kenmerken van de aanpak: de praktijken zijn vollediger of geavanceerder dan op MIL1.	Kenmerken van de aanpak: de praktijken zijn vollediger of geavanceerder dan op MIL2.	
Maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (ISMM)	**Uitgevoerd proces**	**Beheerd proces**	**Tot stand gebracht proces**	**Voorspelbaar proces**	**Optimaliseren van het proces**
Qatar-maturiteitsmodel inzake cyberbeveiliging (Q-C2M2)	**Initiëren** Maakt gebruik van ad-hoccyberbeveiligingspraktijken en -processen in het kader van sommige van de domeinen.	**Ontwikkelen** Heeft beleid en praktijken ten uitvoer gelegd om cyberbeveiligingsactiviteiten in het kader van de domeinen te ontwikkelen en te verbeteren, met als doel nieuwe activiteiten te implementeren.	**Implementeren** Heeft beleid aangenomen om alle cyberbeveiligingsactiviteiten in het kader van de domeinen uit te voeren, met als doel de implementatie op een bepaald tijdstip te voltooien.	**Adaptief** Herbekijkt en beoordeelt cyberbeveiligingsactiviteiten en hanteert praktijken op basis van voorspellende indicatoren die zijn afgeleid van eerdere ervaringen en maatregelen.	**Flexibel** Blijft de adaptieve fase uitvoeren met extra nadruk op flexibiliteit en snelheid bij het uitvoeren van activiteiten in de domeinen.
Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)	**Processen: uitgevoerd** Omdat de organisatie deze praktijken mogelijk alleen op een ad-hocmanier kan uitvoeren en zich al dan niet kan verlaten op documentatie wordt de procesmaturiteit niet beoordeeld voor Niveau 1. **Praktijken: elementaire cyberhygiëne** Niveau 1 richt zich op de bescherming van FCI (Federal Contract Information) en bestaat alleen uit praktijken die overeenkomen met de beschermingsvereisten.	**Processen: gedocumenteerd** Niveau 2 vereist dat een organisatie praktijken en beleidslijnen vaststelt en documenteert om de uitvoering van hun CMMC-inspanningen te sturen. Het documenteren van praktijken stelt mensen in staat ze op herhaalbare wijze uit te voeren. Organisaties ontwikkelen volwassen capaciteiten door hun processen te documenteren en ze vervolgens in praktijk te brengen zoals gedocumenteerd. **Praktijken: intermediaire cyberhygiëne** Niveau 2 dient als overgang van niveau 1 naar niveau 3 en bestaat uit een subset van de in NIST SP 800-171 gespecificeerde beveiligingseisen, alsmede uit praktijken van andere normen en referenties.	**Processen: beheerd** Niveau 3 vereist dat een organisatie een plan opstelt, onderhoudt en van middelen voorziet waaruit de activiteiten voor de uitvoering van een praktijk blijkt. Het plan kan informatie bevatten over missies, doelstellingen, projectplannen, middelen, vereiste opleiding, en relevante betrokkenen. **Praktijken: goede cyberhygiëne** Niveau 3 is gericht op de bescherming van gecontroleerde niet-gerubriceerde gegevens (Controlled Unclassified Information – CUI) en omvat alle in NIST SP 800-171 gespecificeerde beveiligingseisen, alsmede aanvullende praktijken uit andere normen en referenties om bedreigingen te beperken.	**Processen: beoordeeld** Niveau 4 vereist dat een organisatie de praktijken op hun doeltreffendheid toetst en meet. Naast het meten van de doeltreffendheid van praktijken, zijn organisaties op dit niveau in staat corrigerende maatregelen te nemen wanneer dat nodig is en het hoger management op terugkerende basis te informeren over de status of problemen. **Praktijken: proactief** Niveau 4 is gericht op de bescherming van gecontroleerde niet-gerubriceerde gegevens (CUI) en omvat een subset van de verbeterde beveiligingseisen. Deze praktijken verbeteren de opsporings- en responscapaciteit van een organisatie om de veranderende tactieken, technieken en procedures aan te pakken en zich eraan aan te passen.	**Processen: optimaliseren** Niveau 5 vereist dat een organisatie de uitvoering van processen in de hele organisatie standaardiseert en optimaliseert. **Praktijken: gevorderd/proactief** Niveau 5 is gericht op de bescherming van CUI. De aanvullende praktijken vergroten de diepgang en verfijning van de cyberbeveiligingscapaciteiten.
Communautair maturiteitsmodel voor	**Beveiligingsbewust** Het belangrijkste thema van de activiteiten op dit niveau is personen en organisaties bewust	**Procesontwikkeling** Niveau bedoeld om gemeenschappen te helpen bij het vaststellen en verbeteren van	**Informatiegestuurd** Ontworpen om de mechanismen voor het delen van informatie binnen de gemeenschap te	**Tactiekontwikkeling** De elementen van dit niveau zijn bedoeld om betere en meer proactieve methoden om	**Volledige operationele beveiligingscapaciteit** Dit niveau vertegenwoordigt de elementen die aanwezig moeten

cyberbeveiliging (CCSMM)	te maken van de dreigingen en problemen in verband met cyberbeveiliging.	beveiligingsprocessen die nodig zijn om cyberbeveiligingskwesties doeltreffend aan te pakken.	verbeteren, zodat de gemeenschap ogenschijnlijk ongelijksoortige informatie doeltreffend kan correleren.	aanvallen op te sporen en erop te reageren. Op dit niveau zouden de meeste preventiemethoden in werking moeten zijn.	zijn, wil een organisatie zichzelf als volledig operationeel gereed beschouwen om elk type cyberdreiging het hoofd te bieden.
Model voor interne controlecapaciteit voor de publieke sector (IA-CM) voor de publieke sector	**Initieel** Geen duurzame, herhaalbare capaciteiten – afhankelijk van individuele inspanningen	**Infrastructuur** Duurzame en herhaalbare praktijken en procedures	**Geïntegreerd** Beheer en beroepspraktijken uniform toegepast	**Beheerd** Integreert informatie uit de hele organisatie om het beleid en het risicobeheer te verbeteren	**Optimaliseren** Binnen en buiten de organisatie leren met het oog op voortdurende verbetering

Tabel 7: Vergelijking van eigenschappen/dimensies

	Maturiteitsmodel inzake cyberbeveiliging voor naties (CMM)	Maturiteitsmodel inzake cyberbeveiligingscapaciteit (C2M2)	Qatar-maturiteitsmodel inzake cyberbeveiliging (Q-C2M2)	Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)	Certificering van het maturiteitsmodel inzake cyberbeveiliging (CMMC)	Maturiteitsmodel inzake informatiebeveiliging voor NIST-kader voor cyberbeveiliging (ISMM)	Kader voor de verbetering van de cyberbeveiliging van kritieke infrastructuur	Wereldwijde index voor cyberbeveiliging (GCI)	Index voor cybermacht (CPI)
Niveaus	Vijf dimensies onderverdeeld in verschillende factoren die zelf meerdere aspecten en indicatoren omvatten (Figuur 4)	Tien domeinen, met één enkele beheer-doelstelling en verscheidene benaderingsdoelstellingen (Figuur 6)	Vijf domeinen onderverdeeld in subdomeinen	Zeventien domeinen gedetailleerd in processen en één tot vele capaciteiten die vervolgens in Praktijken worden gespecificeerd (Figuur 9).	Zes hoofddimensies	Drieëntwintig beoordeelde gebieden	Vijf functies met onderliggende hoofdcategorieën en subcategorieën (Figuur 8).	Vijf pijlers met diverse indicatoren	Vier categorieën met verschillende indicatoren
Eigenschappen/dimensies	i ontwikkelen van beleid en strategie inzake cyberbeveiliging; ii aanmoedigen van een verantwoordelijke cyberbeveiligingscultuur binnen de samenleving; iii ontwikkelen van kennis op het gebied van cyberbeveiliging; iv creëren van doeltreffende wet- en regelgevingskaders; en v beheersen van risico's via normen, organisaties en technologieën.	i risicobeheer; ii activa-, wijzigings- en configuratiebeheer; iii identiteits- en toegangsbeheer; iv beheer van bedreigingen en kwetsbaarheden; v situationeel bewustzijn; vi reactie op gebeurtenissen en incidenten; vii beheer van toeleveringsketens en externe afhankelijkheden; viii personeelsbeheer; ix cyberbeveiligingsarchitectuur; x beheer van het cyberbeveiligingsprogramma.	i begrijpen (cyberbeleid, -activa, -risico's en -opleiding); ii beveiligen (gegevensbeveiliging, technologiebeveiliging, beveiliging van toegangscontrole, beveiliging van communicatie en beveiliging van personeel); iii blootstellen (monitoring, incidentenbeheer, opsporing, analyse en blootstelling); iv reageren (responsplanning, beperking en responscommunicatie); v in stand houden (herstelplanning, continuïteitsbeheer, verbetering en externe afhankelijkheden).	i toegangscontrole; ii activabeheer; iii controle en verantwoordingsplicht; iv bewustmaking en opleiding; v configuratiebeheer; vi identificatie en authenticatie; vii incidentenrespons; viii onderhoud; ix mediabescherming; x persoonsgerelateerde beveiliging; xi fysieke bescherming; xii herstel; xiii risicobeheer; xiv beveiligingsbeoordeling; xv situationeel bewustzijn; xvi systeem- en communicatiebescherming; xvii systeem- en informatie-integriteit.	i aangepakte bedreigingen; ii meetwaarden; iii delen van informatie; iv technologie; v training; vi toetsing.	i activabeheer; ii bedrijfsomgeving; iii beleid; iv risicobeoordeling; v strategie voor risicobeheer; vi nalevingsbeoordeling; vii toegangscontrole; viii bewustmaking en opleiding; ix gegevensbeveiliging; x processen en procedures voor informatiebescherming; xi onderhoud; xii beschermende technologie; xiii gebreken en gebeurtenissen; xiv permanente bewaking van de beveiliging; xv opsporingsprocessen; xvi responsplanning; xvii responscommunicatie; xviii responsanalyse; xix responsbeperking; xx responsverbeteringen; xxi herstelplanning; xxii herstelverbeteringen; xxiii herstelcommunicatie.	i identificeren; ii beschermen; iii opsporen; iv reageren; v herstellen.	i juridisch; ii technisch; iii organisatorisch; iv capaciteitsopbouw; v samenwerking.	i wet- en regelgeving; ii economische en sociale context; iii technologie-infrastructuur; iv sectortoepassing.

BIJLAGE B – BIBLIOGRAFIE DESKRESEARCH

Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (2012), NCSS: Practical Guide on Development and Execution. Heraklion: Enisa.

Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (2012), NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: Enisa.

Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (2016), Guidelines for SMEs on the security of personal data processing.

Almuhammadi, S. and Alsaleh, M. (2017), 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Beschikbaar op: https://airccj.org/CSCP/vol7/csit76505.pdf

Almuhammadi, S. en Alsaleh, M. (2017), 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Anna, S. et al. (2016), Stocktaking, analysis and recommendations on the protection of CIIs. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009), Developing Maturity Models for IT Management – A Procedure Model and its Application. Beschikbaar op: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgische overheid (2012), cyberbeveiligingsstrategie. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018), Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Beschikbaar op: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bondskanselarij van de Republiek Oostenrijk (2013), Cyberbeveiligingsstrategie van Oostenrijk. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Bondsraad (2018), Nationale strategie voor de bescherming van Zwitserland tegen cyberrisico's.

Bourgue, R. (2012), 'Introduction to Return on Security Investment'.

Britse nationale cyberveiligheidsstrategie 2016-2021 (2016). Beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Bureau van de commissaris voor elektronische communicatie en postvoorschriften (2012), Cyberbeveiligingsstrategie van de Republiek Cyprus.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019), 'Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Beschikbaar op https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Centrum voor beveiligingsstudies (CSS), ETH Zürich (2019), National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Beschikbaar op: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Creese, S. (2016), Cybersecurity Capacity Maturity Model for Nations (CMM). Universiteit van Oxford.

CSIRT Maturity – Self-assessment Tool (geen datum). Beschikbaar op: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA-project van de Raad van Europa en de Europese Unie, wereldwijd project op het gebied van cybercriminaliteit van de Rad van Europa en de EU-taskforce cybercriminaliteit (2011), gespecialiseerde eenheden voor cybercriminaliteit – Studie naar goede praktijken. Beschikbaar op: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (no date) 'Welcome to the NCSS Training Tool'.

Deense regering – Ministerie van Financiën (2018), Deense strategie voor cyber- en informatiebeveiliging. Beschikbaar op: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Dekker, M. A. C. (2014), Technical Guideline on Incident Reporting. Beschikbaar op: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014), Technical Guideline on Security Measures. Beschikbaar op: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015), Guideline on Threats and Assets. Beschikbaar op: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016), Cybersecurity Strategy. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014), *Privacy and data protection by design - from policy to engineering.* Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Europese Commissie (2012), Verordening van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32014R0910

Federaal ministerie van Binnenlandse Zaken (2011), Cyberbeveiligingsstrategie van Duitsland. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016), NIS Directive and national (2015), Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:NL:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015), The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:NL:HTML

Frans kabinet van de premier (2014), Franse nationale digitale beveiligingsstrategie. Beschikbaar op: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015), Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:NL:HTML

Guidelines for SMEs on the security of personal data processing (2016), NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: Enisa.

Guidelines for SMEs on the security of personal data processing (2017), Handbook on security of personal data processing. Beschikbaar op: http://dx.publications.europa.eu/10.2824/569768

Guidelines for SMEs on the security of personal data processing (2014), *Enisa CERT inventory inventory of CERT teams and activities in Europe*. Beschikbaar op: http://www.Enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Het Witte Huis (2018), Nationale Cyberstrategie van de Verenigde Staten van Amerika. Beschikbaar op: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Institute of Internal Auditors (ed.) (2009), Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Internationale Telecommunicatie-unie (ITU) (2018), Guide to developing a national cybersecurity strategy. Beschikbaar op: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Internationale Telecommunicatie-unie (ITU) (2018), The Global Cybersecurity Index. Beschikbaar op: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

J.D., R. D. B. (2019), 'Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework', International Review of Law.

Liveri, D. et al. (2014), An evaluation framework for national cyber security strategies. Heraklion: Enisa. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:NL:HTML.

Luxemburgse regeringsraad (2018), Nationale strategie voor cyberbeveiliging. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Mattioli, R. *et al.* (2014), *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:NL:HTML

Ministerie van Concurrentievermogen en Digitale, Maritieme en Diensteneconomie (2016), Cyberveiligheidsstrategie van Malta. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministerie van Economische Zaken en Communicatie (2019), Cyberbeveiligingsstrategie van de Republiek Estland. Beschikbaar op: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministerie van Nationale Defensie van de Republiek Litouwen (2018), Nationale strategie voor cyberbeveiliging

Nationaal Centrum voor Cyberbeveiliging (2015), Nationale strategie voor cyberbeveiliging van de Tsjechische Republiek. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cybersecurity Strategies Evaluation Tool (2018). Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Beschikbaar op: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Nationale strategieën voor cyberbeveiliging – Interactieve kaart (geen datum). Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Nederlandse regering (2018), Nationale agenda voor cyberbeveiliging. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Object Management Group (2008), Business Process Maturity Model. Beschikbaar op: https://www.omg.org/spec/BPMM/1.0/PDF

OESO, Europese Unie en het Gemeenschappelijk Centrum voor onderzoek – Europese Commissie (2008), Handbook on Constructing Composite Indicators: Methodology and User Guide. OESO. Beschikbaar op: https://www.oecd.org/sdd/42495745.pdf.

Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) (2012), Cybersecurity policy making at a turning point. Beschikbaar op: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012), 'National Cyber Security Strategies – Practical Guide on Development and Execution'.

Ouzounis, E. (2012), Good Practice Guide on National Exercises.

Portesi, S. (2017), Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Publicatieblad van de Europese Unie (2008) RICHTLIJN 2008/114/EG VAN DE RAAD van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren. Beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Raad van Ministers (2019) Portugees Staatsblad, reeks 1 – nr. 108 – Resolutie van de Raad van Ministers nr. 92/2019. Beschikbaar op: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Rady Ministrów (2019), Dziennik Urzędowy Rzeczypospolitej Polskiej. Beschikbaar op: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Regering van Bulgarije (2015), Nationale strategie voor cyberbeveiliging – Cyberbestendig Bulgarije 2020.

Regering van Griekenland (2017), Nationale strategie voor cyberbeveiliging Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Regering van Hongarije (2018), Strategie voor de beveiliging van netwerk- en informatiesystemen. Beschikbaar op: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Regering van Ierland (2019), Nationale strategie voor cyberbeveiliging. Beschikbaar op: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Regering van Kroatië (2015), Nationale strategie voor cyberbeveiliging van de Republiek Kroatië. Beschikbaar op: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Regering van Letland (2014), cyberbeveiligingsstrategie van Letland. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Regering van Spanje (2019), Nationale strategie voor cyberbeveiliging. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Roemeense regering (2013), Cyberbeveiligingsstrategie van Roemenië. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. en European Union Agency for Cybersecurity (2019), Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Beschikbaar op: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariat of the Security Committee (2019), Cyberbeveiligingsstrategie van Finland 2019. Beschikbaar op: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slowaakse regering (2015), Cyberbeveiligingsconcept van de Slowaakse Republiek. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015), Richtlijn 2014/89/EU van het Europees Parlement en de Raad van 7 juli 2010.

Smith, R. (2016), 'Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016', in Smith, R., Core EU Legislation. London: Macmillan Education. Beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017), European Cyber Security Month 2017.

Systeem voor de rapportage en analyse van incidenten op het gebied van cyberbeveiliging – tool voor visuele analyse (geen datum). Beschikbaar op: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Trimintzios, P., et al. (2011), Cyber Europe Report. Beschikbaar op: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. en European Network and Information Security Agency (2013), *National-level risk assessments: an analysis report.* Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:NL:HTML

Trimintzios, P., Gavrila, R., et al. (2015), Report on cyber-crisis cooperation and management. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:NL:HTML

Trimintzios, P., Ogee, A., et al. (2015), Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Beschikbaar op: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:NL:HTML

Uitvoerend bureau van de president (2015), Memorandum voor hoofden van uitvoerende departementen en agentschappen. Beschikbaar op: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Universiteit van Gent et al. (2017), 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. Beschikbaar op: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

University of Innsbruck et al. (2009), Understanding Maturity Models.

Voorzitterschap van de Raad van Ministers (2017), Italiaanse actieplan voor cyberbeveiliging. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Wamala, D. F. (2011), 'ITU National Cybersecurity Strategy Guide. Beschikbaar op: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007), 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

Zweedse regering (2017), Nationell strategi för samhällets informations- och cybersäkerhet. Beschikbaar op: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

BIJLAGE C – OVERIGE BESTUDEERDE DOELSTELLINGEN

De hieronder beschreven doelstellingen zijn bestudeerd in het kader van de deskresearchfase en de door Enisa gehouden interviews. De volgende doelstellingen maken geen deel uit van het beoordelingskader voor nationale capaciteiten, maar zij werpen een licht op thema's die een discussie waard zijn. In elk van de volgende subhoofdstukken zal worden toegelicht waarom de doelstelling werd verworpen.

- sectorspecifieke cyberbeveiligingsstrategieën ontwikkelen;
- strijden tegen desinformatiecampagnes;
- het beveiligen van geavanceerde technologieën (5G, KI, quantum computing enz.);
- gegevenssoevereiniteit waarborgen; en
- stimulansen bieden voor de ontwikkeling van de cyberverzekeringssector.

Sectorspecifieke cyberbeveiligingsstrategieën ontwikkelen

De hantering van sectorspecifieke strategieën die gericht zijn op sectorale steunmaatregelen en stimulansen zorgt zeker voor een sterkere gedecentraliseerde capaciteit. Dit is met name geschikt voor lidstaten waarvan de aanbieders van essentiële diensten te maken hebben met verschillende kaders en regelgevingen en waar er veel afhankelijkheden zijn vanwege het transversale karakter van cyberbeveiliging. In verscheidene lidstaten zijn er immers tientallen nationale autoriteiten en regelgevende instanties met kennis van de specifieke kenmerken van elke sector, die een mandaat hebben om specifieke regelgeving voor elke sector te handhaven.

Zo heeft Denemarken zes gerichte strategieën gelanceerd voor cyber- en informatiebeveiliging in de meest kritieke sectoren, om een sterkere gedecentraliseerde capaciteit op het gebied van cyber- en informatiebeveiliging te ontwikkelen. Elke 'sectorale eenheid' zal onder meer bijdragen aan dreigingsevaluaties op sectoraal niveau, monitoring, paraatheidsoefeningen, het opzetten van beveiligingssystemen, kennisuitwisseling en instructies. De sectorspecifieke strategieën hebben betrekking op de volgende sectoren:

- energie;
- gezondheidszorg;
- vervoer;
- telecommunicatie;
- financiën; en
- zeevaart.

Andere lidstaten toonden belangstelling voor sectorspecifieke cyberbeveiligingsstrategieën die alle regelgevingsvereisten weerspiegelen. Er zij echter op gewezen dat een dergelijke doelstelling wellicht niet voor alle lidstaten geschikt is, afhankelijk van hun grootte, nationaal beleid en maturiteit. De grote moeilijkheid om ervoor te zorgen dat het kader rekenschap kan geven van alle specifieke kenmerken, heeft Enisa ertoe gebracht deze doelstelling niet in het kader op te nemen.

Strijden tegen desinformatiecampagnes

De lidstaten integreren de bescherming van fundamentele beginselen zoals mensenrechten, transparantie en publiek vertrouwen in hun nationale cyberbeveiligingsstrategieën. Dit is zeer belangrijk, vooral wanneer het gaat om desinformatie die via de traditionele nieuwsmedia of socialemediaplatforms wordt verspreid. Bovendien is cyberbeveiliging momenteel een van de grootste electorale uitdagingen. In de aanloop naar belangrijke verkiezingen werden in verschillende landen inderdaad activiteiten zoals het verspreiden van valse informatie of negatieve propaganda vastgesteld. Deze dreiging kan het democratiseringsproces in de EU ondermijnen. Op Europees niveau heeft de Commissie een actieplan[32] opgesteld om de inspanningen ter bestrijding van desinformatie in Europa op te voeren: dit plan is toegespitst op 4 kerngebieden (opsporing, samenwerking, samenwerking met onlineplatforms en bewustmaking) en dient om de capaciteiten van de EU op te bouwen en de samenwerking tussen de lidstaten te versterken.

Vier van de 19 geïnterviewde landen hebben verklaard voornemens te zijn de kwestie van desinformatie en propaganda in hun NCSS aan te pakken.

De Franse NCSS[33] stelt bijvoorbeeld: “Het is de verantwoordelijkheid van de staat om de burgers te informeren over de risico’s van manipulatie en propagandatechnieken die door kwaadwillende spelers op het internet worden gebruikt. Zo heeft de regering na de terroristische aanslagen tegen Frankrijk in januari 2015 een informatieplatform opgericht over de risico’s in verband met islamitische radicalisering via elektronische communicatienetwerken: « Stop-djihadisme.gouv.fr.” Deze aanpak zou kunnen worden uitgebreid om propaganda- en destabilisatieverschijnselen het hoofd te bieden.

Een ander voorbeeld is de de Poolse NCSS 2019-2024[34]: “Tegen manipulatieve activiteiten zoals desinformatiecampagnes zijn systematische acties nodig om het bewustzijn van de burgers te ontwikkelen in de context van het verifiëren van de authenticiteit van informatie en het reageren op pogingen om die informatie te vervormen.”

Tijdens door Enisa afgenomen interviews gaven verschillende lidstaten echter te kennen dat zij de kwestie niet als een bedreiging van de cyberveiligheid in het kader van hun NCSS aanpakken, maar eerder op een breder maatschappelijk niveau, bijvoorbeeld via beleidsinitiatieven.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Het beveiligen van geavanceerde technologieën (5G, KI, quantum computing enz.)

Aangezien het huidige cyberdreigingslandschap zich blijft uitbreiden, zal de ontwikkeling van nieuwe technologieën hoogstwaarschijnlijk resulteren in een toename van de intensiteit en het aantal cyberaanvallen en een diversificatie van de methoden, middelen en doelwitten die door dreigingsactoren worden gehanteerd. Intussen hebben deze nieuwe technologische oplossingen in de vorm van geavanceerde technologieën het potentieel om de bouwstenen van de Europese Digitale Markt te worden. Om de toenemende digitale afhankelijkheid van de lidstaten en de opkomst van nieuwe technologieën veilig te stellen, moeten er stimulansen en een volwaardig beleid komen ter ondersteuning van de veilige en betrouwbare ontwikkeling en toepassing van deze technologieën in de EU.

Tijdens de deskresearchfase op het gebied van de nationale cyberbeveiligingsstrategieën van de lidstaten werden de volgende geavanceerde technologieën naar voren geschoven als belangrijk voor de lidstaten: 5G, KI, quantumcomputing, cryptografie, edgecomputing, verbonden en autonome voertuigen, big en smart data, blockchain, robotica en IoT.

Meer in het bijzonder heeft de Europese Commissie begin 2020 een mededeling gepubliceerd waarin zij de lidstaten oproept stappen te ondernemen om de reeks maatregelen uit te voeren die worden aanbevolen in de conclusies van de 5G-toolbox[35]. Deze 5G-toolbox volgt op Aanbeveling (EU) 2019/534 over de cyberbeveiliging van 5G-netwerken, die in 2019 door de Commissie is vastgesteld en waarin wordt opgeroepen tot een uniforme Europese aanpak van de beveiliging van 5G-netwerken[36].

Tijdens door Enisa afgenomen interviews werd benadrukt dat dit onderwerp meer een transversaal thema is dat in de nationale cyberbeveiligingsstrategieën wordt behandeld, dan een specifieke doelstelling op zich.

Het waarborgen van gegevenssoevereiniteit

Enerzijds kan de cyberspace worden gezien als een enorme wereldwijde gemeenschappelijke ruimte die gemakkelijk toegankelijk is, een hoge mate van connectiviteit verschaft en grote mogelijkheden voor sociaaleconomische groei kan bieden. Anderzijds wordt de cyberspace ook gekenmerkt door haar zwakke jurisdictie, de moeilijkheid om acties toe te wijzen, het ontbreken van grenzen, en onderling verbonden systemen die poreus kunnen zijn en waarvan de gegevens kunnen worden gestolen of zelfs worden geraadpleegd door buitenlandse regeringen. Naast deze twee perspectieven wordt het digitale ecosysteem gekenmerkt door de concentratie van platforms voor onlinediensten en infrastructuur in de handen van een zeer klein aantal belanghebbenden. Alle bovengenoemde aspecten brengen de lidstaten ertoe digitale soevereiniteit te bevorderen. Digitale soevereiniteit bereiken betekent dat burgers en bedrijven zich ten volle kunnen ontplooien door gebruik te maken van digitale diensten en ICT-producten die betrouwbaar zijn, zonder te hoeven vrezen voor hun persoonsgegevens of digitale activa, economische autonomie of politieke invloed.

Gegevenssoevereiniteit of digitale soevereiniteit wordt door de lidstaten verdedigd op nationaal en Europees niveau. Hoewel de lidstaten de kwestie in hun NCSS niet rechtstreeks als een specifieke doelstelling lijken te behandelen, behandelen zij deze als een transversaal beginsel

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[36] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32019H0534

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

of geven zij in ad-hocpublicaties aan dat zij voornemens zijn digitale soevereiniteit op nationaal niveau te waarborgen door zich te concentreren op sleuteltechnologieën. In de Franse strategische evaluatie van cyberdefensie van 2018 wordt bijvoorbeeld gesteld dat “het beheersen van de volgende technologieën van het grootste belang is om de digitale soevereiniteit te waarborgen: communicatie-encryptie, opsporing van cyberaanvallen, Private Mobile Radio, cloud computing en kunstmatige intelligentie”[37].

Op Europees niveau nemen de lidstaten actief deel aan het bepalen van de Europese strategie voor gegevens (COM/2020/66 final) en de opbouw van het EU-certificeringskader voor digitale ICT-producten, -diensten en -processen dat is vastgesteld bij de EU-cyberbeveiligingsverordening (2019/881) om te zorgen voor strategische digitale autonomie op Europees niveau.

Uit de interviews met de lidstaten is gebleken dat ‘digitale soevereiniteit’ vaak wordt beschouwd als een bredere kwestie dan een kwestie die beperkt blijft tot cyberbeveiliging. Daarom behandelen de lidstaten dit punt niet in hun nationale cyberbeveiligingsstrategieën en de weinige lidstaten die dat wel doen, behandelen het niet als een specifieke doelstelling op zich.

Stimulansen bieden aan de ontwikkeling van de cyberverzekeringssector

Uit de huidige stand van zaken in de cyberverzekeringssector blijkt dat de wereldmarkt ontegenzeggelijk is gegroeid. De sector staat echter nog in de kinderschoenen omdat er gegevens moeten worden verzameld en er nog veel precedenten moeten worden geschapen (bv. stille dekking, systemische cyberrisico’s). Bovendien liggen de geraamde verliezen als gevolg van cyberaanvallen over de hele wereld vele malen hoger dan de huidige dekkingscapaciteit van de cyberverzekeringssector (IMF Working Paper – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). De ontwikkeling van de cyberverzekeringssector kan echter zeker voordelen opleveren en de basis leggen voor deugdelijke mechanismen. Cyberverzekeringsmechanismen kunnen namelijk helpen bij:

- het creëren van bewustzijn over de risico’s van cyberbeveiliging in bedrijven;
- het kwantitatief evalueren van de blootstelling aan cyberrisico’s;
- het verbeteren van het risicobeheer op het gebied van cyberbeveiliging;
- het verlenen van steun aan organisaties die het slachtoffer zijn van cyberaanvallen; en
- het dekken van de (al dan niet materiële) schade ten gevolge van een cyberaanval.

Sommige lidstaten zijn begonnen met werkzaamheden op dit gebied. Bijvoorbeeld:

- Estland heeft in zijn NCSS een afwachtende houding aangenomen: “Om de cyberrisico’s in de particuliere sector in het algemeen te beperken, zullen de vraag naar en het aanbod van cyberverzekeringsdiensten in Estland worden geanalyseerd. Op basis daarvan zullen samenwerkingsbeginselen voor de betrokken partijen worden overeengekomen, waaronder het delen van informatie, het opstellen van een risicobeoordeling, enz. Op dit moment zijn er maar weinig aanbieders van cyberverzekeringsdiensten op de Estse markt en is het noodzakelijk om eerst in kaart te brengen wie wat aanbiedt. De complexiteit van de verzekeringsbescherming wordt vaak beschouwd als een belemmering voor de ontwikkeling van de cyberverzekeringsmarkt.”

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

- Luxemburg steunt in zijn NCSS specifiek de ontwikkeling van de cyberverzekeringssector: “Doelstelling 1: nieuwe producten en diensten creëren. Om risico’s te bundelen en slachtoffers van digitale cyberincidenten aan te moedigen de hulp van deskundigen in te roepen om het incident te beheersen en een door een kwaadwillige handeling getroffen systeem te herstellen, zullen verzekeringsmaatschappijen worden aangemoedigd specifieke producten te creëren op het vlak van cyberverzekeringen.”

De reacties van de ondervraagden over dit onderwerp liepen nogal uiteen: sommige lidstaten verklaarden dat ‘cyberverzekering’ sinds kort een thema van discussie is, terwijl andere lieten weten dat het thema weliswaar veelbelovend is, maar dat de sector nog niet genoeg ontwikkeld is. Een groot aantal ondervraagden verklaarde echter dat het thema niet wordt behandeld als onderdeel van de NCSS, hetzij omdat het te specifiek wordt geacht, hetzij omdat het niet binnen het toepassingsgebied van de NCSS valt.

TP-02-21-253-NL-N

Over het Agentschap van de Europese Unie voor cyberbeveiliging

Het Agentschap van de Europese Unie voor cyberbeveiliging, Enisa, streeft ernaar een hoog niveau van cyberbeveiliging in heel Europa te bereiken. Enisa is opgericht in 2004 en heeft een sterker fundament gekregen door de cyberbeveiligingsverordening van de EU. Het Agentschap draagt bij aan het cyberbeveiligingsbeleid van de EU, vergroot de betrouwbaarheid van ICT-producten, -diensten en -processen door middel van certificeringsprogramma's voor cyberbeveiliging, werkt samen met de lidstaten en instanties van de EU en helpt Europa zich voor te bereiden op de cyberuitdagingen van morgen. Door middel van kennisdeling, capaciteitsopbouw en bewustmaking werkt Enisa samen met zijn belangrijkste belanghebbenden om het vertrouwen in de verbonden economie te versterken, de veerkracht van de infrastructuur van de Unie te vergroten en uiteindelijk de Europese samenleving en burgers digitaal veilig te stellen. Zie voor meer informatie www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-490-9
DOI: 10.2824/962331