Advies van het Europees Economisch en Sociaal Comité over de gezamenlijke mededeling aan het Europees Parlement en de Raad: Het EU-beleid op het gebied van cyberdefensie

(initiatiefadvies)

(2023/C 293/04)

Rapporteur: **Anastasis YIAPANIS**

Corapporteur: **Alberto MAZZOLA**

Besluit van de voltallige vergadering	20.9.2022
Rechtsgrond	Artikel 52, lid 2, van het reglement van orde
	Initiatiefadvies
Bevoegde afdeling	Adviescommissie Industriële Reconversie (CCMI)
Goedkeuring door de afdeling	27.3.2023
Goedkeuring door de voltallige vergadering	14.6.2023
Zitting nr.	579
Stemuitslag	
(voor/tegen/onthoudingen)	208/1/2

1. **Conclusies en aanbevelingen**

1.1. Het Europees Economisch en Sociaal Comité (EESC) steunt het voorgestelde EU-beleid op het gebied van cyberdefensie, maar had verwacht dat het maatschappelijk middenveld een prominentere rol zou krijgen bij de uitwerking van de desbetreffende voorstellen. Het EESC kan op dit moment moeilijk beoordelen of de in de gezamenlijke mededeling geschetste toekomstige initiatieven zullen worden uitgevoerd en de beoogde resultaten zullen opleveren. Het dringt er bij de EU-instellingen en de lidstaten op aan prioriteit te geven aan de aangekondigde initiatieven en er snel werk van te maken.

1.2. Het EESC benadrukt de noodzaak van aanvullende maatregelen om de EU beter in staat te stellen cyberdreigingen op te sporen, en zou graag zien dat O&O-financiering gericht wordt op de ontwikkeling van geavanceerde Europese capaciteit. Samenwerking tussen de particuliere en de openbare sector is essentieel en mag geen eenrichtingsverkeer zijn. Het EESC is van mening dat EU-coördinatie nodig is om versnippering tegen te gaan en samenwerking en gezamenlijke investeringen tussen de lidstaten te waarborgen.

1.3. Het EESC steunt de oprichting van het EU-coördinatiecentrum voor cyberdefensie. Daarnaast beveelt het aan dat de lidstaten zich ertoe verplichten 24/7 snel te reageren, en dat ze de cyberparaatheid en de prestaties van de EU-mechanismen voor respons op cybercrises evalueren, met bijzondere aandacht voor zowel de militaire capaciteit als de in de NIS2-richtlijn van het Europees Parlement en de Raad ([1]) genoemde kritieke sectoren. Het EESC is voorstander van de uitbreiding van het mandaat van het Europees Kenniscentrum voor cyberbeveiliging (ECCC) om het werk van het EU-coördinatiecentrum voor cyberdefensie te ondersteunen.

1.4. Het EESC is van mening dat een dynamisch platform om realtimetests uit te voeren en informatie te delen moet worden ontwikkeld, of van de particuliere sector moet worden overgenomen, teneinde de strategische autonomie en soevereiniteit van de Unie op het gebied van cyberbeveiliging te versterken en huidige hiaten in de bestaande capaciteit op te sporen. Zo'n platform kan ook worden gebruikt voor het uitwisselen van beste praktijken, het melden van cyberincidenten en het opstellen van een EU-lijst van alle cybercriminelen.

([1]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

1.5. Het EESC benadrukt de noodzaak van een betere voorbereiding op cyberaanvallen zoals de Russische in Oekraïne, die met name gericht zijn op kritieke infrastructuur. Samenwerking tussen civiele en militaire ecosystemen, ook bij gesimuleerde cyberaanvallen als test, is cruciaal voor efficiënt crisismanagement, interoperabiliteit en het voorkomen van dubbel werk en dubbele investeringen.

1.6. Bij investeringen in cyberdefensie zou voorrang moeten worden gegeven aan de bescherming van burgers en kritieke infrastructuur in de EU, onder meer door gebruik te maken van betrouwbare leveranciers van hardware en software. De EU en de lidstaten zouden in overleg met relevante particuliere stakeholders tijdig afspraken moeten maken over het bijwerken van prioriteiten en investeringen.

1.7. De EU moet de nodige capaciteit ontwikkelen en in stand houden om haar digitale economie, samenleving, democratie en kritieke technologieën te beveiligen, en om essentiële diensten op het gebied van cyberbeveiliging te leveren. Om de strategische autonomie van de EU te waarborgen, is het van vitaal belang dat de afhankelijkheid van derde landen wordt verminderd. Het EESC acht het essentieel dat de EU een middellangetermijnaanpak vaststelt voor autonomie op het gebied van sleuteltechnologieën, en pleit er sterk voor dat onderzoeks- en productiefaciliteiten worden opgericht door in de EU gevestigde bedrijven, met een passend Europees industriebeleid dat gericht is op een autonoom cyberecosysteem.

1.8. Kleine en middelgrote ondernemingen (kmo's) moeten specifieke steun krijgen en toegang hebben tot financieringsprogramma's die hun weerbaarheid tegen cyberaanvallen vergroten, alsook tot bijstand, opleiding en onderwijs op het gebied van cyberrisico's en de manier waarop zij zich daartegen kunnen beschermen. De EU moet een stimuleringsmechanisme creëren om ervoor te zorgen dat kmo's er geleidelijk mee vertrouwd raken en om de ontwikkeling van innovatieve kmo's te bevorderen.

1.9. Het EESC steunt het plan om een academie voor cybervaardigheden op te richten en verzoekt de Europese Commissie grootschalige opleidings- en beroepsonderwijsprogramma's te coördineren en te financieren waarbij alle lidstaten betrokken zijn. Met deze programma's zouden geschoolde arbeidskrachten moeten worden opgeleid voor alle agentschappen en organisaties die betrokken zijn bij cyberdefensie, alsook voor particuliere civiele netwerken.

1.10. Om de blootstelling aan cyberaanvallen te verminderen, is het van cruciaal belang dat burgers zich bewuster worden van cyberbeveiliging. Het EESC dringt dan ook aan op onderwijsprogramma's voor cyberbeveiliging en programma's voor een leven lang leren die gericht zijn op het verbeteren van cybervaardigheden en -kennis. Het EESC is er voorstander van dat cyberbeveiliging wordt geïntegreerd in al het toekomstige EU-beleid en dat het grote publiek over cyberdreigingen wordt voorgelicht.

1.11. Sterke samenwerking met de NAVO-bondgenoten op militair gebied moet gericht zijn op volledige coördinatie en wederkerigheid, gezamenlijke O&O&I-projecten, het delen van beste praktijken, grote opleidingsprogramma's en simulaties van cyberaanvallen, met als voornaamste doel de gezamenlijke reactiecapaciteit uit te breiden.

1.12. Het EESC verzoekt de hoge vertegenwoordiger de huidige bilaterale cyberdialogen onder de loep te nemen en bijkomende besprekingen met andere landen en relevante internationale organisaties te voeren om een mondiaal kader voor de naleving het internationaal recht in cyberspace tot stand te brengen, met een sterke nadruk op wederkerigheid. De EU zou heel goed het voortouw kunnen nemen bij internationale besprekingen over de toekomst van cyberbeveiliging, met name binnen de Verenigde Naties, aangezien zij sterk is gegrondvest op fundamentele democratische vrijheden.

1.13. De EU moet krachtig stelling nemen tegen elk systeem voor het beoordelen van burgers ("social scoring"). Het EESC wijst erop dat echte democratie niet kan bestaan zonder effectieve bescherming van persoonsgegevens en is van mening dat een verantwoordelijk en efficiënt beheer van data essentieel is om van hyperconnectiviteit een concurrentievoordeel te maken.

2. **Inleiding en algemene opmerkingen**

2.1. De digitale uitbreiding van samenlevingen gaat gepaard met een groot aantal bedreigingen voor de cyberveiligheid die het gevolg zijn van technologische verbeteringen. In de afgelopen jaren is het aantal cyberaanvallen aanzienlijk toegenomen en zijn ze steeds geavanceerder geworden, waardoor de veiligheid van zowel openbare als particuliere entiteiten wordt ondermijnd. Of het nu gaat om ransomware, malware, e-mailaanvallen, datalekken, desinformatie, DDoS-aanvallen (Distributed Denial-of-Service) of andere vormen van aanvallen, ze vormen allemaal een constante en voortdurende bedreiging voor de veiligheid van de EU als geheel.

2.2. Het EESC is ingenomen met de gezamenlijke mededeling over het EU-beleid op het gebied van cyberdefensie ([2]) en is van mening dat het hoog tijd is voor een gecoördineerd optreden op EU waarbij zowel de civiele als de militaire cyberspace-ecosystemen worden betrokken en waarmee een passend kader voor investeringen in cyberdefensiecapaciteit wordt geschapen. De mededeling behelst echter niet veel meer dan een statement om vastberaden op te treden en een lijst van toekomstige EU-initiatieven die resultaat moeten opleveren. Het EESC acht het onmogelijk te beoordelen of deze toezeggingen daadwerkelijk gestand zal worden gedaan, want de definitieve uitkomst van het EU-actieplan inzake cyberbeveiliging zal uiteraard mede afhangen van toekomstige onderhandelingen tussen de medewetgevers.

2.3. Cyberbeveiliging is bovenaan de lijst van veiligheidsbedreigingen in de EU komen te staan sinds de Russische aanval op het KA-SAT-satellietnetwerk, waardoor de communicatie tussen de Oekraïense strijdkrachten werd verstoord, en het recente schandaal waarbij Éric Léandri door sommige defensiebedrijven werd ingehuurd om namens hen cyberspionage te verrichten. De algemene verordening gegevensbescherming (AVG) is een degelijk stuk EU-wetgeving en is al enkele jaren van kracht, maar het is duidelijk dat de toenemende hoeveelheid beschikbare gegevens kwetsbaar is en dat het risico dat derden de grens van de legaliteit overschrijden met de dag groter wordt.

2.4. Gezien het transnationale karakter van cyberaanvallen is EU-coördinatie nodig om de huidige versnippering tegen te gaan en ervoor te zorgen dat de lidstaten bereid zijn samen te werken en gezamenlijk te investeren. Dit is met name van belang voor toekomstige gevallen waarin één lidstaat het doelwit kan zijn en alle andere lidstaten de mogelijkheid moeten hebben om onmiddellijk steun te verlenen.

3. **Samen werken aan een sterkere cyberdefensie**

3.1. Het EESC neemt kennis van de aangekondigde ambitieuze initiatieven om een EU-coördinatiecentrum voor cyberdefensie op te zetten, het CyDEf-X-project te ontwikkelen, snellereactieteams bij cyberincidenten op te richten, een EU-initiatief voor cybersolidariteit te ontplooien en de ontwikkeling van certificeringsregelingen voor cyberbeveiliging van ICT-producten, -diensten en -processen te onderzoeken. Alle lidstaten zouden zich moeten verbinden tot het streven om 24/7 snel te kunnen reageren, waarbij het EU-coördinatiecentrum wordt betrokken bij de beoordeling en opstelling van regelmatige verslagen over de cyberparaatheid van de lidstaten en de doeltreffendheid van het Europees mechanisme voor respons op cybercrises, met bijzondere aandacht voor zowel militaire capaciteit als de in de NIS2-richtlijn genoemde kritieke sectoren. Elke lidstaat moet beschikken over specialisten die specifiek zijn opgeleid om in te grijpen bij cyberincidenten, en moet regelmatig testen of zij in staat zijn in andere lidstaten in te grijpen.

3.2. De mededeling bevat een lange lijst van stapsgewijze verbeteringen, maar het EESC had gehoopt op een expliciete routekaart voor de implementatie van deze initiatieven, met duidelijke governancebepalingen en termijnen voor indiening en goedkeuring. Ook had het EESC verwacht dat het maatschappelijk middenveld een prominentere rol zou krijgen bij de uitwerking van de desbetreffende voorstellen.

3.3. Het EESC is van mening dat de lidstaten hun interne vermogen om cyberdreigingen tegen te gaan moeten versterken en tegelijkertijd samenwerkingsprojecten moeten opzetten en informatie en beste praktijken moeten uitwisselen met hun tegenhangers in andere lidstaten. Alle lidstaten moeten snel investeren in cyberdefensiecapaciteit, een versnelde uitrol van technologie ([3]) en gezamenlijke paraatheid om cyberaanvallen op te sporen, ervan te herstellen en zich ertegen te verdedigen. Ter wille van de autonomie van de Unie op het gebied van cyberbeveiliging moet een dynamisch platform om realtimetests uit te voeren en informatie te delen worden ontwikkeld, of van de particuliere sector worden overgenomen, zodat huidige hiaten in de bestaande capaciteit kunnen worden opgespoord.

3.4. Het EESC onderschrijft dat militaire operaties in cyberspace in dit stadium strikt onder de bevoegdheid van de lidstaten moeten blijven vallen. Het steunt de aangekondigde samenwerking tussen de militaire computercrisisteams van de EU (milCERT's), de Computer Security Incident Response Teams (CSIRT's) en het computercrisisresponsteam van de EU-IOA's (CERT-EU).

3.5. De onlangs goedgekeurde NIS2-richtlijn en de richtlijn betreffende de veerkracht van kritieke entiteiten (CER-richtlijn) ([4]) voorzien reeds in specifieke nationale en sectorale verplichtingen voor het EU-kader voor cyberdefensie. Verdere maatregelen zijn nodig om de collectieve opsporingscapaciteit van de EU te verbeteren, en het EESC dringt aan op O&O-investeringen voor de ontwikkeling van geavanceerde Europese capaciteit.

([2]) Mededeling van de Commissie over het EU-beleid op het gebied van cyberdefensie.
([3]) Zoals het NAVO-initiatief Diana (Defence Innovation Accelerator for the North Atlantic).
([4]) CER-richtlijn.

4. **Het defensie-ecosysteem van de EU beveiligen**

4.1. Door de inherente complexiteit en de snel evoluerende technologische uitdagingen is het defensie-ecosysteem veranderd en is cyberbeveiliging een gemeenschappelijk thema geworden voor zowel de militaire als de civiele sector, alsook voor de EU-burgers. Samenwerking tussen civiele en militaire ecosystemen is nu belangrijker dan ooit en moet voordelen opleveren in de zin van een doeltreffender crisismanagement, alsook continue vooruitgang en interoperabiliteit, waarbij wordt voorkomen dat er dubbel werk wordt geleverd of dat er onnodig dezelfde investeringen worden gedaan. De lidstaten moeten bereid zijn stresstests voor nationale kritieke infrastructuur uit te voeren teneinde de weerbaarheid tegen toekomstige cyberaanvallen te beoordelen en te vergroten.

4.2. Het EESC is van mening dat investeringen in cyberdefensie prioritair gericht moeten zijn op de bescherming van EU-burgers en kritieke infrastructuur. Gezien het hoge tempo van de digitale transformatie en de snelle ontwikkeling van het dreigingslandschap is het volgens het EESC absoluut zaak dat de EU en de lidstaten in nauw overleg met relevante particuliere stakeholders tijdig afspraken maken over het bijwerken van prioriteiten en investeringen. Apparaten in het kader van het internet der dingen (IoT) zijn vaak minder goed beschermd dan traditionele apparaten en het EESC dringt erop aan dat via IDAM-platforms een minimaal beveiligingsniveau wordt gewaarborgd. Daar certificering een belangrijke methode is om tot een hoger veiligheidsniveau te komen, zou het EESC tevens graag zien dat in de nieuwe benadering van EU-certificering meer nadruk wordt gelegd op de beveiliging van IoT.

4.3. De EU moet bouwen aan weerbaarheid tegen cyberaanvallen en zorgen voor een doeltreffende cyberafschrikking. Kritieke infrastructuur moet tegen alle soorten cyberaanvallen worden beschermd, ook door EU-defensiesystemen. Het is in het strategische belang van de EU om ervoor te zorgen dat de Unie de essentiële capaciteit ontwikkelt en in stand houdt om haar digitale economie, samenleving en democratie te beveiligen, om volledige digitale soevereiniteit te bereiken als de enige manier om kritieke technologieën te beschermen en om doeltreffende essentiële diensten op het gebied van cyberbeveiliging te leveren. Voor de strategische autonomie van de EU is het ook van essentieel belang dat de afhankelijkheid van derde landen wordt verminderd. Het EESC vindt dat sectorale EU-agentschappen (Enisa, EASA, ERA, EMA, EBA, ESA, Hadea enz.) bij het proces moeten worden betrokken en sturing moeten geven aan de ontwikkeling van cyberbeveiligingsregelingen.

4.4. De COVID-19 pandemie heeft de digitale transitie versneld en traditionele arbeid omgevormd tot hybride werk en/of telewerk. Dit heeft geleid tot nieuwe arbeidsverhoudingen en verwachtingen, alsook tot een nieuwe klasse van digitale nomaden, die steeds groter wordt. Het EESC wijst op de snelle veranderingen op de arbeidsmarkt, die tot gevolg hebben gehad dat bedrijven een "zero trust"-architectuur hebben ingevoerd via oplossingen voor identiteits- en toegangsbeheer (IAM, Identity Access Management) en het beheer van bevoorrechte toegang (PAM, Privileged Access Management). Dit soort beheer van bedrijfsmiddelen brengt nieuwe oplossingen op het gebied van cyberdreigingen met zich mee. Het EESC vindt dat particuliere bedrijven moeten worden gesteund om het veiligheidsniveau van hun innovatieve digitale oplossingen op te voeren.

4.5. De zin uit de Commissiemededeling "Samen met de lidstaten kan een uitvoeringsplan worden opgezet" is nogal teleurstellend. Volgens het EESC zou zo'n uitvoeringsplan verplicht moeten zijn, samen met de lidstaten moeten worden opgesteld en zo spoedig mogelijk moeten worden geïmplementeerd. Het EESC maakt zich zorgen over de lichtzinnige houding van de Commissie en dringt er bij de EU-instellingen en de lidstaten op aan om snel werk te maken van de aangekondigde initiatieven.

5. **Investeren in cyberdefensievermogens**

5.1. Door de snelle technologische ontwikkeling is cyberspace het nieuwste terrein van oorlogsvoering geworden, na land, zee, lucht en ruimte. Hierdoor hebben kwaadwillende cyberactoren, van onafhankelijke hackers tot beroepscriminelen en zelfs overheidsactoren, meer mogelijkheden gekregen om misdrijven te plegen.

5.2. Investeringen in O&O zijn van essentieel belang en het EESC is ingenomen met de bestaande specifieke fondsen binnen het programma Digitaal Europa, het Europees Defensiefonds, Horizon Europa en de nationale herstelprogramma's. Het EESC zou het echter op prijs stellen als er meer transnationale projecten zouden komen die gericht zijn op samenwerking en interoperabiliteit tussen cyberdefensiesystemen in alle lidstaten, en als er meer synergie tussen financieringsinstrumenten zou zijn, met name om innovatieve kmo's te begeleiden.

5.3. Volgens de EU-strategie inzake cyberbeveiliging uit 2020 is de deadline voor de oprichting van de gezamenlijke cybereenheid dit jaar. Het EESC wacht op nieuws over de afronding van het proces en de paraatheid van de EU om te reageren op grootschalige cyberincidenten. Het EESC gaat ervan uit dat de EU hiermee tot een beter besef van de situatie zal komen en beter in staat zal zijn om op cyberaanvallen te reageren en ervan te herstellen.

5.4. Het EESC steunt de uitbreiding van het mandaat van het ECCC om de activiteiten van het EU-coördinatiecentrum voor cyberdefensie te ondersteunen. Bovendien zou dit netwerk de Europese digitale soevereiniteit kunnen ondersteunen door een concurrerende Europese industriële basis voor belangrijke technologische vermogens te ontwikkelen, mede op basis van werk dat door contractuele publiek-private partnerschappen (PPP's) is ontwikkeld. PPP's zijn de meest doeltreffende aanpak gebleken om de cyberbeveiliging van het gehele digitale ecosysteem te verbeteren, maar er mag hier geen sprake zijn van eenrichtingsverkeer: openbare instellingen moeten hun informatie ook delen met de particuliere sector.

5.5. Het EESC merkt op dat de EU onverwijld moet investeren in geavanceerde technologieën zoals post-kwantum-cryptografie teneinde toekomstige pogingen om kwantumcomputers te hacken, aan te pakken. Het is absoluut zaak dat Europa een middellangetermijnaanpak hanteert om tot autonomie te komen. Het EESC pleit er nadrukkelijk voor dat onderzoeks- en productiefaciliteiten worden opgericht door in de EU gevestigde bedrijven. De EU moet meer middelen voor O&I op digitaal gebied uittrekken. Voorts moet er steun komen voor investeringen van exploitanten en aanbieders in nieuwe technische beveiligingsfuncties, ook in verband met nieuwe trends zoals "augmented reality" en het metaversum. Het is met name essentieel om een Europese "distributed cloud"-infrastructuur op te bouwen op basis van Europese regels voor onderwerpen als gegevensopslag en -verwerking ([5]).

5.6. Kmo's moeten specifieke aandacht krijgen en toegang hebben tot financieringsprogramma's die hun paraatheid op het gebied van cyberaanvallen vergroten, alsook tot bijstand, opleidingen en onderwijsprogramma's die hen helpen de cyberrisico's te begrijpen en zich te beschermen. De EU moet zorgen voor een stimuleringsmechanisme waardoor kmo's er geleidelijk mee vertrouwd raken.

5.7. De Commissie schat het huidige tekort aan vakkrachten op het gebied van cyberbeveiliging op een half miljoen mensen, en het EESC is ingenomen met het voorstel om een academie voor cybervaardigheden op te richten. Het is duidelijk dat inspanningen op het niveau van de lidstaten niet volstaan om de vaardigheidskloof te dichten. Derhalve stelt het EESC voor dat de Commissie, naast de oprichting van de academie, gebruikmaakt van de kans die met het Europees Jaar van de Vaardigheden wordt geboden en grootschalige opleidingsprogramma's en programma's voor beroepsonderwijs en -opleiding op EU-niveau coördineert en financiert waarbij alle lidstaten betrokken zijn. Met deze programma's zouden geschoolde arbeidskrachten moeten worden opgeleid voor alle agentschappen en organen die betrokken zijn bij cyberdefensie, alsook voor particuliere civiele netwerken. Bijzondere nadruk moet worden gelegd op de opleiding van arbeidskrachten, met name op het gebied van wetenschap, technologie, engineering en wiskunde (STEM).

5.8. Om de blootstelling aan cyberaanvallen te verminderen is het voorts van wezenlijk belang dat burgers bewuster worden gemaakt van cyberbeveiliging, met name wat betreft elementaire cybercriminaliteit die gericht is tegen het grote publiek. Het EESC dringt aan op onderwijsprogramma's voor cyberbeveiliging en opleidingsprogramma's voor een leven lang leren op het gebied van cyberbeveiliging die erop gericht zijn de cybervaardigheden te verbeteren en cyberbeveiliging vertrouwder en aantrekkelijker te maken voor burgers, met name de jongere generatie. Het EESC pleit ervoor om cyberbeveiligingoverwegingen in al het toekomstige EU-beleid op te nemen en om het grote publiek te informeren over cyberdreigingen, onder meer via gratis opleidingsprogramma's voor de burgers, gratis informatieapps op mobiele telefoons, of communicatie op tv in primetime. Tegelijkertijd met deze acties moet op alle niveaus van de samenleving een brede cultuuromslag in de richting van een "op cyberbeveiliging gerichte" benadering worden bevorderd.

5.9. Volgens het EESC is het van vitaal belang om het risicoprofiel van aanbieders te beoordelen en relevante beperkingen op te leggen aan aanbieders met een hoog risico. Het gaat hierbij onder meer om een noodzakelijk verbod op belangrijke middelen en toepassingen die in de gecoördineerde risicobeoordeling van de EU als cruciaal en gevoelig worden aangemerkt, en om het certificeren van betrouwbare leveranciers van hardware en software.

6. **Partnerschappen aangaan om gemeenschappelijke uitdagingen aan te pakken**

6.1. Het niveau van paraatheid bij toekomstige cyberaanvallen verschilt sterk per lidstaat. Het EESC is van mening dat er allereerst een communicatieplatform voor beste praktijken binnen de EU moet worden opgezet waar de lidstaten met de meeste kennis van cyberaanvallen hun knowhow met de andere landen kunnen delen, en kunnen faciliteren dat beste praktijken onverwijld worden overgenomen. Dit zou het wederzijds vertrouwen tussen de nationale entiteiten ten goede komen. Ten tweede pleit het EESC voor meer samenwerking tussen overheids- en niet-overheidsactoren in de EU om de cyberbeveiliging van producten en diensten op de eengemaakte markt te verbeteren. Het EESC stelt ook voor een gemeenschappelijk EU-platform op te richten voor het melden van cyberincidenten, inclusief een zwarte lijst van de EU waarop alle cybercriminelen voorkomen.

([5]) Zoals het Frans-Duitse initiatief Gaia-X.

6.2. Nauwe samenwerking met onze NAVO-bondgenoten op militair gebied moet niet alleen gericht zijn op capaciteitsopbouw en vroegtijdige opsporing, maar ook op gezamenlijke O&O&I-projecten, het delen van beste praktijken en uitwisselingen tussen deskundigen, grote opleidingsprogramma's en simulaties van cyberaanvallen. Voornaamste doel moet zijn het gemeenschappelijke reactievermogen uit te breiden en synergieën tot stand te brengen voor de bestrijding van toekomstige hybride dreigingen, in aansluiting op de gezamenlijke verklaringen van Warschau van 2016 en Brussel van 2018. De samenwerking tussen de EU en de NAVO biedt nog een aantal mogelijkheden die kunnen worden benut, en onmiddellijke vooruitgang kan een echt verschil maken wat betreft het waarborgen van de veiligheid van onze burgers en samenlevingen.

6.3. Besprekingen op mondiaal niveau en met onze internationale partners moeten het pad effenen voor het bevorderen van een mondiale en open cyberspace die de mensenrechten, de fundamentele vrijheden en de rechtsstaat beschermt, en gericht is op de ontwikkeling van bindende internationale normen in sectoren met een snelle digitale ontwikkeling. Het EESC adviseert de hoge vertegenwoordiger de bestaande bilaterale cyberdialogen onder de loep te nemen en verdere onderhandelingen met andere landen en relevante internationale organisaties aan te gaan om een mondiaal kader voor de toepassing van het internationaal recht in cyberspace te bevorderen, op basis van een strikte voorwaarde van wederkerigheid.

6.4. De EU is bij uitstek geschikt om de internationale debatten over de toekomst van cyberbeveiliging te leiden, met name binnen de VN, omdat zij sterk is gegrondvest op fundamentele democratische vrijheden. De EU moet ook de strijd aanbinden met totalitaire regimes die gegevens van burgers in de gaten houden en hun rechten en vrijheden schenden, en moet zich krachtig uitspreken tegen elk systeem voor het beoordelen van burgers ("social scoring"). Het EESC is van mening dat er zonder effectieve bescherming van persoonsgegevens geen echte democratie kan bestaan en dat een verantwoordelijk en efficiënt beheer van data essentieel is om van hyperconnectiviteit een troef te maken.

Brussel, 14 juni 2023.

De voorzitter
van het Europees Economisch en Sociaal Comité
Oliver RÖPKE