Publicatieblad
van de Europese Unie

NL
L-serie

2024/2659

16.10.2024

AANBEVELING (EU) 2024/2659 VAN DE COMMISSIE

van 11 oktober 2024

betreffende richtsnoeren, uit hoofde van artikel 5 van Verordening (EU) 2021/821 van het Europees Parlement en de Raad, voor de uitvoer van producten voor cybersurveillance

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Overwegende hetgeen volgt:

(1) Verordening (EU) 2021/821 van het Europees Parlement en de Raad ([1]) stelt een Unieregeling in voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik.

(2) In Verordening (EU) 2021/821 wordt ingegaan op het risico dat producten voor cybersurveillance worden gebruikt in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van mensenrechten en het internationaal humanitair recht.

(3) Overeenkomstig artikel 5, lid 2, en artikel 26, lid 1, van Verordening (EU) 2021/821 moeten de Commissie en de Raad richtsnoeren voor exporteurs beschikbaar stellen met betrekking tot niet in de lijst van de bijlage bij die Verordening opgenomen producten voor cybersurveillance, met het oog op de noodzaak om de efficiëntie van de uitvoercontroleregeling van de Unie inzake cyberbeveiliging en de consistentie bij de toepassing van Verordening (EU) 2021/821 te waarborgen.

(4) Deze aanbeveling en de daarbij gevoegde richtsnoeren hebben tot doel exporteurs te ondersteunen bij de toepassing van controles op niet in de lijst opgenomen producten voor cybersurveillance, met inbegrip van onder meer zorgvuldigheidsmaatregelen bij de risicobeoordeling in verband met de uitvoer van dergelijke producten.

(5) Over de bij deze aanbeveling gevoegde richtsnoeren is in 2022 en 2023 uitvoerig overleg gepleegd in de deskundigengroep inzake surveillancetechnologie en is rekening gehouden met de opmerkingen die zijn ontvangen tijdens een in het tweede kwartaal van 2023 gehouden openbare raadpleging ([2]).

(6) Er zij aan herinnerd dat deze aanbeveling en de bijgevoegde richtsnoeren niet bindend zijn. De exporteurs moeten derhalve verantwoordelijk blijven voor het voldoen aan hun verplichtingen uit hoofde van Verordening (EU) 2021/821, terwijl de Commissie ervoor zorg moet dragen dat deze aanbeveling in de loop van de tijd relevant blijft,

([1]) Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (PB L 206 van 11.6.2021, blz. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

Aanbevolen wordt dat de bevoegde autoriteiten van de lidstaten en exporteurs de richtsnoeren in de bijlage bij deze aanbeveling in aanmerking nemen om te voldoen aan hun verplichtingen krachtens artikel 5, lid 2, van Verordening (EU) 2021/821.

Gedaan te Brussel, 11 oktober 2024.

Voor de Commissie
Valdis DOMBROVSKIS
Uitvoerend vicevoorzitter

BIJLAGE

INHOUD

Bladzijde

Inleiding 4

1. Relevante wettelijke bepalingen, definities en sleutelbegrippen 4

1.1. Overzicht van relevante wettelijke bepalingen 4

1.2. Belangrijke definities 5

1.2.1. “Speciaal ontworpen” 5

1.2.2. “Heimelijk surveilleren” 6

1.2.3. “Natuurlijke personen” 6

1.2.4. “Monitoren, extraheren, verzamelen, analyseren van gegevens” 6

1.2.5. “Uit informatie- en telecommunicatiesystemen” 7

1.2.6. “Kennis dragen van” en “bestemd zijn voor” 7

1.3. Binnenlandse repressie, ernstige schendingen van de mensenrechten en het internationaal humanitair recht 7

1.3.1. Binnenlandse repressie 8

1.3.2. Het plegen van ernstige schending van de mensenrechten 8

1.3.3. Het plegen van ernstige schending van het internationaal humanitair recht 9

2. Werkingssfeer in technische zin 9

2.1. In de lijst opgenomen producten voor cybersurveillance 9

2.2. Mogelijk niet in de lijst opgenomen producten voor cybersurveillance 9

2.2.1. Technologie voor gezichts- en emotieherkenning 10

2.2.2. Plaatsbepalingsapparatuur 10

2.2.3. Videobewakingssystemen 10

3. Zorgvuldigheidsmaatregelen 10

Vereisten uit hoofde van artikel 5, lid 2, van Verordening (EU) 2021/821 14

4. Aanhangsel 12

In de lijst opgenomen producten voor cybersurveillance waarop bijlage I bij Verordening (EU) 2021/821 betrekking heeft 14

Systemen voor interceptie van telecommunicatie (5A001.f.) 14

Systemen voor internetsurveillance (5A001.j.) 15

“Inbraakprogrammatuur” (4A005, 4D004 en daarmee verband houdende controles als bedoeld onder 4E001.a. en 4E001.c.) 15

Programmatuur voor communicatiemonitoring (5D001.e.) 16

Producten voor cryptoanalyse (5A004.a.) 16

Forensische/onderzoeksinstrumenten (5A004.b., 5D002.a.3.b. en 5D002.c.3.b.) 16

INLEIDING

Het bij Verordening (EU) 2021/821 vastgestelde Uniekader voor uitvoercontrole ("de verordening") heeft tot doel ervoor te zorgen dat de internationale verplichtingen en verbintenissen van de Unie en haar lidstaten, onder meer met betrekking tot regionale vrede, veiligheid en stabiliteit, worden nagekomen, en dat de mensenrechten en het internationaal humanitair recht worden geëerbiedigd. De Unie en haar lidstaten hebben derhalve uitvoering gegeven aan de besluiten in het kader van de multilaterale uitvoercontroleregelingen en de controlelijst van de Unie in bijlage I bij de verordening dienovereenkomstig bijgewerkt ([1]). Bovendien hadden de bevoegde autoriteiten van de lidstaten de uitvoer van bepaalde in de lijst opgenomen producten die voor surveillance zouden kunnen worden gebruikt, reeds voordat artikel 5 van de verordening van toepassing was, aan controle onderworpen ([2]), rekening houdend met het risico van misbruik in bepaalde specifieke omstandigheden. Ingeval van uitzonderlijk ernstige omstandigheden heeft de Unie sancties opgelegd om de uitvoer van bepaalde surveillance-uitrusting te beperken ([3]).

De verordening weerspiegelt de toezegging van de Unie om het risico dat producten voor cybersurveillance worden gebruikt in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht doeltreffend aan te pakken. De verordening voert met name nieuwe bepalingen in voor de controle op de uitvoer van niet in de lijst opgenomen producten voor cybersurveillance, waaronder een verplichting voor exporteurs om, indien zij er volgens de resultaten van hun zorgvuldigheidsonderzoek kennis van dragen dat niet in de lijst opgenomen producten voor cybersurveillance die zij voornemens zijn uit te voeren, geheel of ten dele bestemd zijn voor gebruik in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht, dat mee te delen aan de bevoegde autoriteit. In de verordening worden de Commissie en de Raad voorts opgeroepen richtsnoeren voor exporteurs beschikbaar te stellen ter ondersteuning van de doeltreffende uitvoering van de nieuwe controles ten aanzien van niet in de lijst opgenomen producten voor cybersurveillance.

Deze richtsnoeren zijn derhalve bedoeld om exporteurs te ondersteunen bij de toepassing van controles op niet in de lijst opgenomen producten voor cybersurveillance, waaronder zorgvuldigheidsmaatregelen ter beoordeling van de risico's in verband met de uitvoer van dergelijke producten naar eindgebruikers en met eindgebruik in het kader van de nieuwe bepalingen van de verordening.

1. RELEVANTE WETTELIJKE BEPALINGEN, DEFINITIES EN SLEUTELBEGRIPPEN

1.1. Overzicht van relevante wettelijke bepalingen

Bij de verordening zijn nieuwe bepalingen ingevoerd die specifiek voorzien in controles op de uitvoer van producten voor cybersurveillance die niet in de lijst van bijlage I bij de verordening zijn opgenomen, indien de producten geheel of gedeeltelijk bestemd zijn of kunnen zijn voor gebruik in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht. De relevante overwegingen en artikelen luiden als volgt:

a) overweging 8: "Om het risico te ondervangen dat bepaalde niet in de lijst opgenomen producten voor cybersurveillance die vanuit het douanegebied van de Unie zijn uitgevoerd, misbruikt worden door personen die medeplichtig zijn aan of verantwoordelijk zijn voor het aansturen of het plegen van ernstige schendingen van de mensenrechten of het internationaal humanitair recht, is het passend controle op de uitvoer van dergelijke producten uit te oefenen. De daaraan verbonden risico's hebben met name betrekking op gevallen waarin de producten voor

([1]) Zie met name controles met betrekking tot systemen voor interceptie van telecommunicatie (5A001.f), internetbewakingssystemen (5A001.j.), inbraakprogrammatuur (4A005, 4D004 en daarmee verband houdende controles als bedoeld onder 4E001.a en 4E001.c) en programmatuur voor monitoring door rechtshandhavingsinstanties (5D001.e). Zie voorts, op basis van een beoordeling per geval, controles met betrekking tot bepaalde forensische/onderzoeksinstrumenten (5A004.b 5D002.a.3.b en 5D002.c.3.b).

([2]) Met name systemen voor informatiebeveiliging.

([3]) Zie Verordening (EG) nr. 765/2006 van de Raad van 18 mei 2006 betreffende beperkende maatregelen met het oog op de situatie in Belarus en de betrokkenheid van Belarus bij de Russische agressie tegen Oekraïne (PB L 134 van 20.5.2006, blz. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Verordening (EU) nr. 359/2011 van de Raad van 12 april 2011 betreffende beperkende maatregelen tegen bepaalde personen, entiteiten en lichamen in verband met de situatie in Iran (PB L 100 van 14.4.2011, blz. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Verordening (EU) nr. 36/2012 van de Raad van 18 januari 2012 betreffende beperkende maatregelen in het licht van de situatie in Syrië en tot intrekking van Verordening (EU) nr. 442/2011 (PB L 16 van 19.1.2012, blz. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Verordening (EU) nr. 401/2013 van de Raad van 2 mei 2013 betreffende beperkende maatregelen in het licht van de situatie in Myanmar/Birma en tot intrekking van Verordening (EG) nr. 194/2008 (PB L 121 van 3.5.2013, blz. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj), en Verordening (EU) 2017/2063 van de Raad van 13 november 2017 betreffende beperkende maatregelen in het licht van de situatie in Venezuela (PB L 295 van 14.11.2017, blz. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

cybersurveillance speciaal zijn ontworpen om binnendringing in of "deep packet inspection" van de informatie- en telecommunicatiesystemen mogelijk te maken, teneinde natuurlijke personen te schaduwen door gegevens, met inbegrip van biometrische gegevens, uit die systemen te monitoren, te extraheren, te verzamelen of te analyseren. Producten die worden gebruikt voor puur commerciële toepassingen zoals facturering, marketing, kwaliteitsdiensten, gebruikerstevredenheid of netwerkbeveiliging worden over het algemeen niet geacht dergelijke risico's met zich mee te brengen";

b) overweging 9: "Om de doeltreffende controle op de uitvoer van niet in de lijst opgenomen producten voor cybersurveillance te versterken, is het van essentieel belang de toepassing van vangnetcontroles (catch-all controls) op dat gebied verder te harmoniseren. Daartoe verbinden de lidstaten zich ertoe dergelijke controles te ondersteunen door onderling en met de Commissie informatie uit te wisselen, met name over technologische ontwikkelingen op het gebied van producten voor cybersurveillance, en door waakzaamheid te betrachten bij de toepassing van dergelijke controles om een uitwisseling op het niveau van de Unie te bevorderen.";

c) artikel 2, punt 20), dat "producten voor cybersurveillance" als volgt definieert: "producten voor tweeërlei gebruik die speciaal zijn ontworpen om het heimelijk surveilleren van natuurlijke personen mogelijk te maken door gegevens uit informatie- en telecommunicatiesystemen te monitoren, te extraheren, te verzamelen of te analyseren";

d) artikel 5, waarbij een vergunningsvereiste is ingevoerd voor de uitvoer van niet op de lijst in bijlage I voorkomende producten voor cybersurveillance, indien de exporteur door de bevoegde autoriteit is meegedeeld dat de producten in kwestie geheel of gedeeltelijk bestemd zijn of kunnen zijn voor gebruik in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht (artikel 5, lid 1). Op grond van dit artikel moeten exporteurs voorts, wanneer zij er volgens de resultaten van hun zorgvuldigheids-onderzoek kennis van dragen dat de producten geheel of ten dele bestemd zijn voor gebruik in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht, dat meedelen aan de bevoegde autoriteit (artikel 5, lid 2). Die bevoegde autoriteit moet beslissen of voor de betrokken uitvoer een vergunning wordt vereist, en

e) artikel 5, lid 2, dat voorts bepaalt: "De Commissie en de Raad stellen richtsnoeren beschikbaar voor exporteurs, als bedoeld in artikel 26, lid 1.".

1.2. **Belangrijke definities**

De verordening bevat specifieke overwegingen en bepalingen die specifieke, voor controles op de uitvoer van niet in de lijst opgenomen producten voor cybersurveillance relevante termen verduidelijken, en die voor exporteurs belangrijk zijn voor een helder begrip teneinde passende zorgvuldigheid te betrachten en doeltreffend controles uit te voeren. Van bijzonder belang is artikel 2, punt 20), dat de volgende nauwkeurige definitie van "producten voor cybersurveillance" bevat: "producten voor tweeërlei gebruik die speciaal zijn ontworpen om het heimelijk surveilleren van natuurlijke personen mogelijk te maken door gegevens uit informatie- en telecommunicatiesystemen te monitoren, te extraheren, te verzamelen of te analyseren".

Voor de toepassing van deze richtsnoeren moeten specifieke aspecten van die definitie worden verduidelijkt.

1.2.1. *"Speciaal ontworpen"*

Een product is ontworpen voor heimelijk surveilleren wanneer de technische kenmerken ervan geschikt zijn voor het heimelijk surveilleren van natuurlijke personen en dit objectief gezien mogelijk maken. Derhalve wordt onder de term "speciaal ontworpen" verstaan dat het heimelijk surveilleren van natuurlijke personen het hoofddoel van de ontwikkeling en het ontwerp van het product moet zijn geweest. Deze term stelt echter niet de voorwaarde dat het product uitsluitend voor het heimelijk surveilleren van natuurlijke personen kan worden gebruikt.

Zoals verduidelijkt in overweging 8 van de verordening, zijn producten die worden gebruikt voor puur commerciële toepassingen, zoals facturering, marketing, kwaliteitsdiensten, gebruikerstevredenheid of netwerkbeveiliging, niet speciaal ontworpen voor heimelijke surveillance van natuurlijke personen en vallen zij dus niet onder de definitie van producten voor cybersurveillance. Hoewel bijvoorbeeld producten voor het bewaken van besturingssystemen in de industrie of voor de monitoring van gebruikersverkeer kunnen worden gebruikt voor surveillancedoeleinden, zijn die producten geen producten voor cybersurveillance in de zin van de definitie, aangezien zij niet speciaal zijn ontworpen om heimelijke surveillance van natuurlijke personen mogelijk te maken.

1.2.2. *"Heimelijk surveilleren"*

Producten maken heimelijk surveilleren met name mogelijk indien het surveilleren niet duidelijk waarneembaar is voor de desbetreffende natuurlijke persoon. Dit zou het geval zijn wanneer de betrokken personen geen kennis dragen van het aanwezig en/of actief zijn van producten voor cybersurveillance en dus niet de mogelijkheid hebben zichzelf uit die surveillance te verwijderen of ten minste hun gedrag dienovereenkomstig aan te passen. Zelfs indien het surveilleren plaatsvindt door middel van in de openbare ruimte geïnstalleerde of daarin werkende producten, kan het vergaren van gegevens in bepaalde gevallen als relevant voor heimelijk surveilleren worden beschouwd; met name kunnen de verzamelde gegevens worden onttrokken, beoordeeld of verwerkt voor andere doeleinden dan die waarvan de betrokken natuurlijke persoon in kennis zijn gesteld. Met andere woorden, wanneer een natuurlijke persoon niet objectief kan verwachten dat hij onder surveillance staat, kan de surveillance overeenkomstig artikel 2, punt 20), van de verordening als heimelijk worden beschouwd.

1.2.3. *"Natuurlijke personen"*

De term "natuurlijke persoon" refereert aan een levend mens, in tegenstelling tot een rechtspersoon of een entiteit, waarvoor de bepalingen dus niet gelden. De term bestrijkt niet de surveillance van voorwerpen, locaties of machines als zodanig.

1.2.4. *"Monitoren, extraheren, verzamelen, analyseren van gegevens"*

Volgens het "Oxford English Dictionary" hebben de woorden monitoren, extraheren, verzamelen en analyseren de volgende taalkundige betekenis:

— "monitoren": toezicht houden; surveillance, meeluisteren;

— "extraheren": onttrekken;

— "verzamelen": vergaren, bijeenbrengen;

— "analyseren": het onderscheiden of herkennen van de elementen van iets (complex), om de structuur of de aard ervan te bepalen, en het aldus te verduidelijken of te begrijpen; het nauwgezet en methodisch met het oog op uitlegging onderzoeken; het onderwerpen aan kritische of computeranalyses.

Deze termen houden in dat de voor surveillance gebruikte producten precieze technische capaciteiten moeten hebben waarmee gegevens kunnen worden gemonitord, verzameld, geëxtraheerd of geanalyseerd, zoals bijvoorbeeld de volgende producten:

a) producten die worden gebruikt om gegevens uit informatie- en telecommunicatiesystemen te monitoren [4] (bijvoorbeeld bestandsgrootte of pakketverkeer van de gegevens die in een dergelijk systeem worden verzonden);

b) producten die door binnendringing en extractie gegevens uit informatie- en telecommunicatiesystemen extraheren (bijvoorbeeld inbraakprogrammatuur");

c) producten die een analyse mogelijk maken van gegevens die zijn geëxtraheerd uit informatie- en telecommunicatiesystemen, met inbegrip van die waarmee camera-beelden kunnen worden verwerkt die in die systemen zijn opgeslagen (bijvoorbeeld bepaalde soorten data-analysetechnologieën die in het kader van gezichtsherkennings-systemen worden gebruikt).

Producten die worden gebruikt om eenvoudig informatiesystemen te monitoren of om de bevolking via videocamera's te bekijken en die het mogelijk maken gesprekken, uitwisselingen van data, bewegingen en individueel gedrag vast te leggen, vallen niet onder de definitie van "producten voor cybersurveillance" van de verordening, omdat zij niet speciaal zijn ontworpen voor dit doel en met andere technologieën, zoals artificiële intelligentie of big data, moeten worden gebruikt. Het systeem in zijn geheel (dat samen met andere technologieën zoals artificiële intelligentie of big-datatechnologieën functioneert) een product voor cybersurveillance kunnen zijn volgens de definitie van artikel 2, punt 20), van de verordening.

Belangrijk is dat deze voorbeelden nuttig zijn ter illustratie, maar dat zij de definitie en de reikwijdte van het begrip "producten voor cybersurveillance" niet beperken, aangezien artikel 5 tot doel heeft een doeltreffende uitvoercontrole op niet in de lijst opgenomen producten mogelijk te maken.

[4] Zie voor de definitie punt 1.2.5.

Zoals uit het gebruik van het voegwoord "of" in de definitie blijkt, moeten de vermelde technische capaciteiten worden beschouwd als alternatieven, en is het niet noodzakelijk dat een product beschikt over alle technische capaciteiten die nodig zijn voor monitoring, extractie, verzameling of analyse van gegevens. Het volstaat met andere woorden dat een product beschikt over een van die technische capaciteiten, opdat het onder de definitie van product voor cybersurveillance van artikel 2, punt 20), kan vallen.

1.2.5. *"Uit informatie- en telecommunicatiesystemen"*

Deze termen hebben betrekking op systemen die elektronisch informatie verwerken, bijvoorbeeld programmeren/coderen, pc-systeembeheer (hardware) en andere vormen van informatiebeheer, waaronder programmatuurtechnologie, webtechnologie, computertechnologie, opslagtechnologie enz., en op aan aantal systemen die informatie over een afstand overbrengen, zoals technische systemen die geluiden, signalen, tekst, andere tekens en/of beelden via zowel bedrade als draadloze kanalen, via optische vezels, radio en andere elektromagnetische systemen verzenden. Samen omvatten deze twee begrippen een breed scala aan systemen voor het verzenden of verwerken van informatie. Er zij op gewezen dat de term betrekking heeft op systemen en niet op uitrusting.

1.2.6. *"Kennis dragen van" en "bestemd zijn voor"*

Overeenkomstig artikel 5, lid 2, van de verordening moet een exporteur, indien hij er "kennis van draagt dat producten voor cybersurveillance […] bestemd zijn voor [gebruik in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht]", dat aan de bevoegde autoriteit meedelen.

Het begrip "kennis dragen van" is geen nieuw juridisch begrip, maar is en wordt gebruikt in verband met vergunningsvereisten voor eindgebruik (zogenoemde "vangnetcontroles") in overeenstemming met de artikelen 4, 6, 7 en 8 van de verordening. "Kennis dragen van" houdt in dat de exporteur kennis heeft van het voorgenomen misbruik. De enkele mogelijkheid van een dergelijk risico volstaat niet om vast te stellen dat er sprake is van kennis dragen van. Het begrip "kennis dragen van" kan echter niet worden gelijkgesteld met passiviteit: voor "kennis dragen van" is vereist dat de exporteur stappen heeft ondernomen om voldoende en adequate kennis te vergaren om de risico's in verband met de uitvoer te kunnen beoordelen en de naleving van de verordening te waarborgen.

De vermelding dat er sprake van moet zijn dat de producten "bestemd zijn voor" een relevant gevoelig eindgebruik houdt in dat de exporteur het eindgebruik van geval tot geval moet beoordelen, in het licht van de specifieke omstandigheden van dat geval. A contrario zou een theoretisch risico, dat wil zeggen niet gebaseerd op een feitelijke beoordeling van het geval, dat de voorwerpen zouden kunnen worden gebruikt op een wijze die mensenrechten schendt, niet volstaan om aan te nemen dat zij "bestemd zijn voor" een specifiek misbruik in de zin van artikel 5.

1.3. **Binnenlandse repressie, ernstige schendingen van de mensenrechten en het internationaal humanitair recht**

Volgens artikel 15 van de verordening, waarin de overwegingen voor de beoordeling van een vergunning worden uiteengezet, houden de lidstaten rekening met alle relevante overwegingen, met inbegrip van die welke Gemeenschappelijk Standpunt 2008/944/GBVB van de Raad ([5]) behelst.

Artikel 5 van de verordening breidt de controles uit tot de uitvoer van niet in de lijst opgenomen producten voor cybersurveillance, rekening houdend met het risico dat die producten worden gebruikt in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht. Gemeenschappelijk Standpunt 2008/944/GBVB en de Gids voor de gebruiker bij dit Gemeenschappelijk Standpunt ([6]) bieden nuttige richtsnoeren in dit verband.

([5]) Gemeenschappelijk Standpunt 2008/944/GBVB van de Raad van 8 december 2008 tot vaststelling van gemeenschappelijke voorschriften voor de controle op de uitvoer van militaire goederen en technologie (PB L 335 van 13.12.2008, blz. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Zie Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB van de Raad tot vaststelling van gemeenschappelijke voorschriften voor de controle op de uitvoer van militaire goederen en technologie, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Binnenlandse repressie*

Artikel 2, lid 2, van Gemeenschappelijk Standpunt 2008/944/GBVB bepaalt het volgende: "Binnenlandse onderdrukking omvat onder meer foltering en andere wrede, onmenselijke en onterende behandeling of bestraffing, standrechtelijke of willekeurige executies, verdwijningen, willekeurige gevangenneming en andere ernstige schendingen van de mensenrechten en de fundamentele vrijheden die staan omschreven in de desbetreffende internationale mensenrechteninstrumenten, waaronder de Universele Verklaring van de Rechten van de Mens en het Internationaal Verdrag inzake burgerrechten en politieke rechten (ICCPR)." De Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB bevat richtsnoeren voor de elementen waarmee rekening moet worden gehouden bij de beoordeling door de exporteur, waaronder de "huidige en vroegere staat van dienst van de voorgestelde eindgebruiker met betrekking tot de eerbiediging van de mensenrechten en die van het ontvangende land in het algemeen".

1.3.2. *Het plegen van ernstige schending van de mensenrechten*

Het misbruik van niet in de lijst opgenomen producten voor cybersurveillance kan negatieve gevolgen hebben voor een breed spectrum van mensenrechten en maakt rechtstreeks inbreuk op het recht op privacy en gegevensbescherming. Willekeurige of onrechtmatige surveillance kan ook een schending inhouden van andere mensenrechten, zoals het recht op vrijheid van meningsuiting, op vrijheid van vereniging en vergadering, op vrijheid van gedachte, geweten en godsdienst, op gelijke behandeling of het verbod op discriminatie, en het recht op vrije, gelijke en geheime verkiezingen. In bijzondere gevallen kan de surveillance, met inbegrip van het monitoren of verzamelen van informatie over natuurlijke personen, zoals mensenrechtenverdedigers, activisten, politieke figuren, kwetsbare bevolkingsgroepen en journalisten, leiden tot intimidatie, onderdrukking, willekeurige detentie, foltering of zelfs buitengerechtelijke executies. Daarom moeten exporteurs deze aspecten die verband houden met ernstige schendingen van de mensenrechten, in hun beoordelingen opnemen.

Uit de internationale praktijk blijkt dat enige beperking van de mensenrechten "passend" moet zijn en in overeenstemming met de internationale mensenrechtennormen. In de praktijk betekent dit dat er passende waarborgen zijn om te waarborgen dat beperkingen bij wet worden gesteld en dat de wezenlijke inhoud van de rechten behouden blijft. Met inachtneming van het evenredigheidsbeginsel kunnen beperkingen uitsluitend worden gesteld indien zij noodzakelijk zijn en daadwerkelijk een legitiem doel dienen — bijvoorbeeld de nationale of openbare veiligheid, de openbare orde, de bescherming van de volksgezondheid of de bescherming van de rechten en vrijheden van anderen.

Producten voor cybersurveillance kunnen legitieme en gereguleerde instrumenten voor rechtshandhavingstoepassingen omvatten, zoals voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, onder meer op het gebied van terrorismebestrijding, of de tenuitvoerlegging van straffen in het kader van strafrechtelijke handhaving. Tegelijkertijd kunnen producten voor cybersurveillance ook worden misbruikt om ernstige schendingen van de mensenrechten en het internationaal humanitair recht te begaan wanneer zij worden uitgevoerd naar repressieve regimes of particuliere eindgebruikers en/of naar conflictgebieden.

Dit vereist een beoordeling per geval van de omstandigheden van een geval, met inbegrip van de toepassing van relevante regelgeving in het licht van enige melding van ernstige schendingen van de mensenrechten door de bevoegde instanties van bijvoorbeeld de Verenigde Naties, de Unie of de Raad van Europa. Een aanwijzing voor de "ernst" van mensenrechtenschendingen kan zijn gelegen in de erkenning van die schendingen in door de bevoegde instanties van de Verenigde Naties, de Unie of de Raad van Europa gepubliceerde informatie. Een dergelijke expliciete erkenning door die instanties is niet absoluut noodzakelijk, maar is een belangrijke factor om aan de criteria te voldoen.

Volgens de bewoordingen van artikel 5 moet de schending van de mensenrechten "ernstig" zijn. Nuttige richtsnoeren om mogelijke schendingen van de mensenrechten als "ernstig" aan te merken, zijn te vinden in de Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB. Volgens deze gids zijn de aard en de gevolgen van de schending doorslaggevend. Systematische en/of wijdverbreide schendingen van de mensenrechten worden regelmatig als ernstig beschouwd; maar ook schendingen die niet systematisch of wijdverbreid zijn, kunnen als "ernstig" worden beschouwd, bijvoorbeeld vanwege de ernst van de interventie voor de getroffen personen.

Bijlage II bij de Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB bevat een niet-uitputtende lijst van de belangrijkste internationale en regionale mensenrechteninstrumenten, waaronder het Internationaal Verdrag inzake burgerrechten en politieke rechten (ICCPR), het Verdrag tegen foltering en andere wrede, onmenselijke of onterende behandeling of bestraffing, het Europees Verdrag tot bescherming van de rechten van de mens (het verdrag) en het Handvest van de grondrechten (het handvest), die belangrijke richtsnoeren kunnen bieden voor de interpretatie en toepassing van de criteria ter ondersteuning van robuuste mensenrechtenbeoordelingen. Deze instrumenten en de bijbehorende aanvullende protocollen zijn de belangrijkste internationale normen en standaarden op het gebied van de mensenrechten en de fundamentele vrijheden.

1.3.3. *Het plegen van ernstige schending van het internationaal humanitair recht*

Het internationaal humanitair recht (ook wel het "recht van Genève" of het "recht inzake gewapende conflicten" genoemd) is ontwikkeld door middel van een reeks internationale verdragen, met name de Haagse Reglementen, de Verdragen van Genève en de twee aanvullende protocollen van 1977, en stelt regels vast die in tijden van gewapend conflict dienen ter bescherming van mensen die niet of niet langer deelnemen aan vijandelijkheden (bijvoorbeeld burgers en gewonden, zieken of gevangengenomen strijders) en de oorlogvoerende partijen beperkingen opleggen met betrekking tot de middelen en methoden van oorlogvoering (wet van Den Haag).

Het gebruik van niet in de lijst opgenomen producten voor cybersurveillance moet in overeenstemming zijn met het internationaal humanitair recht wanneer zij worden ingezet als zij in het kader van een gewapend conflict worden ingezet als middel en methoden voor oorlogsvoering. In dergelijke omstandigheden is het risico van ernstige schendingen van het internationaal humanitair recht een overweging in het kader van de verordening en moet het, net als voor het plegen van ernstige schendingen van de mensenrechten, in het specifieke geval worden beoordeeld in het licht van het beoogde eindgebruik van de producten. De Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB bevat richtsnoeren voor de elementen die in aanmerking moeten worden genomen, waaronder de vroegere en huidige staat van dienst van de ontvanger met betrekking tot de eerbiediging van het internationale humanitaire recht, de bedoelingen van de ontvanger als kenbaar gemaakt via formele toezeggingen, en het vermogen van de ontvanger om ervoor te zorgen dat de overgedragen goederen of technologie worden gebruikt op een wijze die in overeenstemming is met het internationaal humanitair recht, en niet worden omgeleid of overgebracht naar andere bestemmingen waar zij voor ernstige schendingen van dit recht zouden kunnen worden gebruikt.

Volgens artikel 5 moet de schending van het internationaal humanitair recht "ernstig" zijn. Richtsnoeren zijn te vinden in de Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB, waarin het volgende wordt erkend: "Indien in geïsoleerde gevallen het internationaal humanitair recht wordt geschonden zegt dit niet per se iets over hoe het ontvangende land aankijkt tegen dit recht", alsmede: "Indien er echter een bepaald patroon van schendingen kan worden onderscheiden of het ontvangende land nalaat passende maatregelen te nemen om schendingen te bestraffen, kan dit aanleiding geven tot ernstige bezorgdheid". Het Internationaal Comité van het Rode Kruis (ICRC) heeft richtsnoeren verstrekt voor de beoordeling, met het oog op uitvoercontrole, van schendingen van het internationaal humanitair recht. Volgens het ICRC zijn "schendingen van het internationaal humanitair recht ernstig wanneer zij beschermde personen (bijvoorbeeld burgers, krijgsgevangenen, gewonden en zieken) of voorwerpen (bijvoorbeeld civiele objecten of infrastructuur) in gevaar brengen of belangrijke universele waarden schenden". Oorlogsmisdaden zijn bijvoorbeeld ernstige schendingen van het internationaal humanitair recht. Het ICRC noemt voorts soortgelijke factoren om in aanmerking te nemen als die welke de Gids voor de gebruiker bij Gemeenschappelijk Standpunt 2008/944/GBVB behelst, waaronder formele toezeggingen om de regels van het internationaal humanitair recht toe te passen, passende maatregelen om de verantwoordingsplicht voor schendingen van het internationaal humanitair recht te waarborgen, opleiding voor het leger in het internationaal humanitair recht en een verbod op het ronselen van kinderen voor strijdkrachten.

2. **WERKINGSSFEER IN TECHNISCHE ZIN**

2.1. **In de lijst opgenomen producten voor cybersurveillance**

Het aanhangsel van deze richtsnoeren bevat informatie over in bijlage I bij de verordening opgenomen producten voor cybersurveillance, teneinde exporteurs te helpen bij de identificatie van mogelijke niet in de lijst opgenomen producten voor cybersurveillance.

2.2. **Mogelijke niet in de lijst opgenomen producten voor cybersurveillance**

Hoewel het per definitie onmogelijk is om een uitputtende lijst op te stellen van die producten die krachtens artikel 5 als "niet in de lijst opgenomen producten" aan controle kunnen worden onderworpen, kunnen de volgende producten mogelijk voor surveillance worden gebruikt en in het kader van de verordening aanleiding geven tot bijzondere waakzaamheid.

Zoals verduidelijkt in overweging 8 van de verordening, worden producten die worden gebruikt voor puur commerciële toepassingen zoals facturering, marketing, kwaliteitsdiensten, gebruikerstevredenheid of netwerkbeveiliging, over het algemeen niet geacht een risico van misbruik als relevant in het kader van ernstige schendingen van de mensenrechten of het internationaal humanitair recht mee te brengen, en zijn zij over het algemeen geen voorwerp van controle in het kader van artikel 5. Veel van deze producten hebben functionaliteiten voor informatiebeveiliging (cryptografisch of zelfs cryptoanalytisch) die voldoen aan de controleparameters van categorie 5, deel 2, van de tekst inzake de controles in bijlage I bij de verordening. Beveiligingsnetwerkuitrusting — met inbegrip van routers, schakelaars of relais, waarbij de functionaliteit voor informatiebeveiliging is beperkt tot de taken van "Bediening, beheer en onderhoud" waarbij alleen gepubliceerde of commerciële cryptografische normen worden toegepast — valt evenmin onder de definitie van "producten voor cybersurveillance", hoewel exporteurs waakzaam moeten blijven in het licht van verschillende rapportages over misbruik van dergelijke producten op het vlak van schendingen van mensenrechten.

2.2.1. *Technologie voor gezichts- en emotieherkenning*

Technologieën voor gezichts- en emotieherkenning hebben meerdere andere toepassingen dan cybersurveillance — bijvoorbeeld voor identificatie of authenticatie — en zouden niet automatisch onder de definitie vallen. In bepaalde omstandigheden kunnen technologieën voor gezichts- en emotieherkenning echter wel binnen de werkingssfeer van artikel 2, punt 20), van de verordening vallen.

Technologieën voor gezichts- en emotieherkenning die kunnen worden gebruikt om opgeslagen videobeelden te monitoren of te analyseren, zouden onder de definitie van product voor cybersurveillance kunnen vallen. Echter, zelfs indien aan de voornoemde criteria is voldaan, moet zorgvuldig worden onderzocht of de programmatuur speciaal voor heimelijke surveillance is ontworpen.

2.2.2. *Plaatsbepalingsapparatuur*

Met plaatsbepalingsapparatuur kan de fysieke locatie van een apparaat in de loop van de tijd worden gevolgd, en sommige plaatsbepalingstechnologieën worden al enige tijd door rechtshandhavings- en inlichtingendiensten gebruikt. Het potentieel ervan voor doelgerichte en grootschalige surveillance is aanzienlijk geëvolueerd, aangezien de plaatsbepalingstechnologieën geavanceerder zijn geworden — met inbegrip van satellietgebaseerde plaatsbepaling, plaatsbepaling op basis van zendmasten, wifi- en Bluetooth transceivers — en omdat "volgapparaten" zoals smartphones en andere elektronische apparaten (bijvoorbeeld boordsystemen in auto's) wijdverbreid zijn geworden.

Plaatsbepalingsapparatuur wordt gebruikt door rechtshandhavings- en inlichtingendiensten, bijvoorbeeld om bewijsmateriaal te verzamelen in de loop van een onderzoek of om verdachten te traceren, maar ook door bedrijven voor commerciële doeleinden, bijvoorbeeld het rapporteren over geaggregeerde verplaatsingspatronen in winkelstraten, het volgen van werknemers die buiten de locatie werken, of voor op locatie gebaseerde reclame.

2.2.3. *Videobewakingssystemen*

Om exporteurs te helpen mogelijke cybersurveillance te identificeren, is het ook nuttig te verduidelijken welke producten niet onder de definitie zouden vallen. In die zin vallen bijvoorbeeld videobewakingssystemen en camera's — met inbegrip van camera's met hoge resolutie — die worden gebruikt voor het filmen van mensen in openbare ruimten, niet onder de definitie van producten voor cybersurveillance, aangezien zij geen gegevens uit informatie- en telecommunicatiesystemen monitoren of verzamelen.

3. **ZORGVULDIGHEIDSMAATREGELEN**

Overweging 7 van de verordening luidt als volgt: "De bijdrage van exporteurs […] aan het algemene doel van de handelscontrole is van cruciaal belang. Om hen in staat te stellen in overeenstemming met deze verordening te handelen, moet de beoordeling van de risico's in verband met de onder deze verordening vallende transacties worden uitgevoerd door middel van transactiescreening, ook bekend als het zorgvuldigheidsbeginsel (het due diligence-beginsel), als onderdeel van een intern nalevingsprogramma (ICP)."

Volgens artikel 2, punt 21), wordt onder "intern nalevingsprogramma" of "ICP" (internal compliance programme) verstaan: "aanhoudende doeltreffende, passende en evenredige beleidsmaatregelen en procedures die door exporteurs zijn vastgesteld om de naleving van de bepalingen en doelstellingen van deze verordening en de voorwaarden van de uit hoofde van deze verordening vastgestelde vergunningen te vergemakkelijken, met inbegrip van onder meer zorgvuldigheidsmaatregelen (due diligence-maatregelen) ter beoordeling van risico's in verband met de uitvoer van de producten naar bepaalde eindgebruikers en in verband met de uiteindelijke doeleinden".

Aanbeveling (EU) 2019/1318 van de Commissie ([7]) biedt een kader om exporteurs te helpen de risico's in verband met de controle op de handel in producten voor tweeërlei gebruik in kaart te brengen, te beheren en te beperken en de naleving van de relevante Unie- en nationale wet- en regelgeving te waarborgen.

Deze richtsnoeren kunnen exporteurs ondersteunen bij het screenen van transacties, ook gekend als het zorgvuldigheidsbeginsel, als onderdeel van een ICP.

Op grond van artikel 5, lid 2, van Verordening (EU) 2021/821 moeten exporteurs van niet in de lijst opgenomen producten voor cybersurveillance passende zorgvuldigheid betrachten door middel van transactiescreening, d.w.z. het nemen van stappen met betrekking tot de indeling van producten en de risicobeoordeling van transacties. In de praktijk worden exporteurs aangemoedigd de volgende toetsingen door te voeren:

([7]) Aanbeveling (EU) 2019/1318 van de Commissie van 30 juli 2019 inzake interne nalevingsprogramma's voor controles op de handel in producten voor tweeërlei gebruik uit hoofde van Verordening (EG) nr. 428/2009 van de Raad (PB L 205 van 5.8.2019, blz. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Toetsing of het niet in de lijst opgenomen, voor uitvoer bestemde product een "product voor cybersurveillance" zou kunnen zijn, dat wil zeggen speciaal ontworpen om het heimelijk surveilleren van natuurlijke personen mogelijk te maken door gegevens uit informatie- en telecommunicatiesystemen te monitoren, te extraheren, te verzamelen of te analyseren**

Deze stap betreft de vaststelling van de aard van het product in het kader van de bepalingen die van toepassing zijn op producten voor cybersurveillance. Dit omvat een onderzoek van de technische kenmerken van de producten, op basis van de technische parameters die in bijlage I bij de verordening voor de in de lijst opgenomen producten worden vermeld, en in het licht van de specifieke termen en concepten in de definitie van producten voor cybersurveillance voor niet in de lijst opgenomen producten, en de daaropvolgende classificatie van het product (goederen, technologie of programmatuur).

3.2. **Toetsing van de mogelijkheden van het betrokken product, om vast te stellen of er mogelijk misbruik van kan worden gemaakt in het kader van binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht door buitenlandse eindgebruikers**

Exporteurs moeten een beoordeling uitvoeren om vast te stellen of het product zou kunnen worden misbruikt voor binnenlandse repressie, schending van mensenrechten, met inbegrip van het recht op leven, vrijwaring van foltering, onmenselijke en vernederende behandeling, het recht op privacy, het recht op vrijheid van meningsuiting, het recht op vereniging en vergadering, het recht op vrijheid van gedachte, geweten en godsdienst, het recht op gelijke behandeling of het verbod op discriminatie of het recht op vrije, gelijke en geheime verkiezingen.

Dit omvat ook een beoordeling om vast te stellen of het product zou kunnen worden gebruikt als deel of onderdeel van een systeem dat tot dezelfde schendingen en/of hetzelfde misbruik kan leiden.

Exporteurs moeten bij hun beoordeling zogenaamde rode vlaggen gebruiken, die wijzen op abnormale omstandigheden in een transactie die erop wijzen dat de uitvoer bestemd kan zijn voor een ongepast eindgebruik, een niet-geschikte eindgebruiker of een niet-geschikte bestemming.

Rode vlaggen:

a) het product wordt in de handel gebracht met informatie die verband houdt met het mogelijke gebruik ervan voor heimelijke surveillance;

b) informatie die erop wijst dat een soortgelijk voorwerp is misbruikt in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht (zie punt 1.3);

c) informatie die erop wijst dat het voorwerp onrechtmatig is gebruikt bij surveillanceactiviteiten tegen een lidstaat of in verband met onrechtmatige surveillance van een EU-burger;

d) informatie die erop wijst dat de transactie voorwerpen omvat die zouden kunnen worden gebruikt om een systeem op te zetten, aan te passen of te configureren waarvan bekend is dat het wordt misbruikt in verband met binnenlandse repressie en/of het plegen van ernstige schendingen van de mensenrechten en het internationaal humanitair recht (zie punt 1.3);

e) het product of een soortgelijk product staat op de lijst die overeenkomstig artikel 5, lid 6, van de verordening in de C-serie van het *Publicatieblad van de Europese Unie* is bekendgemaakt.

3.3. **Toetsing, ter ondersteuning van de bevoegde autoriteiten, van de bij de transactie betrokken belanghebbenden (met inbegrip van eindgebruikers en geadresseerden zoals distributeurs en wederverkopers)**

Exporteurs moeten, ter ondersteuning van de bevoegde autoriteiten en voor zover mogelijk:

a) vóór en tijdens elke transactie toetsen hoe de geadresseerden en/of eindgebruikers voornemens zijn het product of de dienst te gebruiken, op basis van verklaringen inzake het eindgebruik;

b) vertrouwd raken met de situatie op de relevante bestemming van de producten, met name de algemene toestand van de mensenrechten, aangezien dit een belangrijke indicator is voor het risico van ernstige schendingen van de mensenrechten en het internationaal humanitair recht in verband met export;

c) de risico's toetsen dat het product of de dienst wordt omgeleid naar een andere niet-gemachtigde eindgebruiker, op basis van de hieronder vermelde rode vlaggen.

Rode vlaggen:

a) de eindgebruiker heeft een duidelijke relatie met een buitenlandse overheid die een reputatie heeft op het gebied van binnenlandse repressie en/of ernstige schendingen van de mensenrechten en het internationaal humanitair recht;

b) de eindgebruiker maakt structureel deel uit van de strijdkrachten of een andere groep die betrokken is bij een gewapend conflict waarbij in het verleden sprake is geweest van binnenlandse repressiemaatregelen en/of ernstige schendingen van de mensenrechten en het internationaal humanitair recht;

c) de eindgebruiker heeft in het verleden producten voor cybersurveillance uitgevoerd naar landen waar het gebruik van dergelijke producten heeft geleid tot binnenlandse repressiemaatregelen en/of ernstige schendingen van de mensenrechten en het internationaal humanitair recht.

3.4. De resultaten van het zorgvuldigheidsonderzoek gebruiken voor het opstellen van plannen om potentiële negatieve effecten in de toekomst te voorkomen en te beperken

Exporteurs moeten, op basis van de resultaten van hun zorgvuldigheidsonderzoek, de activiteiten stopzetten die negatieve effecten in verband met de mensenrechten veroorzaken of daartoe bijdragen, en een actieplan met corrigerende maatregelen ontwikkelen en ten uitvoer leggen. Deze maatregelen kunnen onder meer het volgende omvatten:

a) actualisering van het beleid van de onderneming om richtsnoeren te verstrekken over de wijze waarop negatieve effecten in de toekomst kunnen worden voorkomen en aangepakt, en om de uitvoering ervan te waarborgen;

b) zich baseren op de bevindingen van de risicobeoordeling om de beheersystemen te actualiseren en te versterken om informatie beter te traceren en risico's te signaleren voordat zich negatieve effecten voordoen;

c) informatie verzamelen om inzicht te krijgen in de grote risico's van negatieve effecten in verband met de sector;

d) de bevoegde autoriteiten van de lidstaten in kennis stellen van de resultaten van zorgvuldigheidsonderzoeken om de informatiestroom met betrekking tot bepaalde producten, eindgebruikers en bestemmingen te vergemakkelijken.

Vereisten uit hoofde van artikel 5, lid 2, van Verordening (EU) 2021/821



4. AANHANGSEL

In de lijst opgenomen producten voor cybersurveillance waarop bijlage I bij Verordening (EU) 2021/821 betrekking heeft

— **Systemen voor interceptie van telecommunicatie (5A001.f.)**

In de meeste landen, waaronder de lidstaten, wordt de vertrouwelijkheid van communicatie wettelijk beschermd, maar kan het heimelijk elektronisch surveilleren van communicatie door overheidsinstanties binnen een wettelijk kader worden toegestaan (de zogenaamde legale interceptie ("LI", legale onderschepping). Met het digitale tijdperk is de grootschalige inzet van interceptietechnologieën echter mogelijk geworden. Het gebruik van interceptie-instrumenten door het Libische regime heeft duidelijk gemaakt dat deze technologieën op grote schaal kunnen worden ingezet en heeft in 2012 de invoering van uitvoercontroles op systemen voor telecommunicatie-interceptie bespoedigd.

Deze controle is van toepassing op uitrusting die is ontworpen voor de extractie van de inhoud van communicatie (spraak of data), abonnee-identificatoren of andere metagegevens die via de lucht via draadloze communicatie worden verzonden, en op uitrusting voor radiofrequentiemonitoring. Deze controle is bijvoorbeeld van toepassing op IMSI-catchers (International Mobile Subscriber Identity), die mobieletelefoonverkeer onderscheppen en de bewegingen van gebruikers van mobiele telefoons volgen, of op uitrusting die nepwifi-hotspots creëert welke IMSI-nummers uit een telefoon kunnen extraheren, alsook op bepaalde soorten producten die speciaal zijn ontworpen om "deep packet inspection" in telecommunicatiesystemen mogelijk te maken. Uitrusting voor het storen van mobiele telecommunicatie valt niet onder de reikwijdte van het begrip "producten voor cybersurveillance", aangezien dergelijke uitrusting geen gegevens verzamelt.

Hoewel technologie die is bedoeld voor algemene doeleinden, kan worden gebruikt om dergelijke systemen op te bouwen, zal hun vermogen om op grote schaal te onderscheppen afhankelijk zijn van specifieke onderdelen en onderdelen, waaronder bijvoorbeeld specifieke programmatuur, geavanceerde of toepassingsspecifieke geïntegreerde schakelingen (bijvoorbeeld FGPA's, ASICs enz) om het aantal pakketten of communicatiesessies dat per seconde kan worden verwerkt, te verhogen.

— **Systemen voor internetsurveillance (5A001.j.)**

Hoewel normaal gesproken veel internetcommunicatie tegenwoordig standaard wordt versleuteld, kan het onderscheppen van verkeersgegevens (metagegevens) over communicatie — zoals IP-adressen en de frequentie en de omvang van gegevensuitwisseling — nog steeds worden gebruikt om verbanden tussen personen en domeinnamen te achterhalen. Regeringen kunnen deze systemen rechtmatig en onder gerechtelijk toezicht gebruiken voor legitieme doeleinden, zoals het identificeren van personen die domeinen bezoeken die verband houden met criminele of terroristische inhoud. De monitoring en analyse van het internetverkeer op basis van etnische, religieuze, politieke of sociale kenmerken kan er echter toe leiden dat de bevolking en sociale groeperingen van een land verregaand in kaart worden gebracht met het oog op het controleren van de bevolking en repressie, alsook voor andere doeleinden, zoals het identificeren van politieke dissidenten. Los van kwesties in verband met mensenrechten en binnenlandse repressie kunnen deze producten ook bijdragen aan het versterken van capaciteiten op het militaire en veiligheidsvlak.

De controle als bedoeld onder 5A001.j is van toepassing op internetsurveillancesystemen die op een "carrier-grade IP-network" (bijvoorbeeld national-grade-IP-netwerk) werken om verzonden metadata-inhoud (spraak, video, berichten, bijlagen) te analyseren, te extraheren en te indexeren op basis van "hard selectors", en die het relationele netwerk van mensen in kaart te brengen. Dit zijn producten waarmee "heimelijk surveilleren" plaatsvindt aangezien de personen waarop de surveillance betrekking heeft geen kennis dragen van de onderschepping van communicatie. Controles zijn daarentegen niet gericht op systemen waarbij sprake is van een handeling van of interactie met een gebruiker of abonnee, en zijn bijvoorbeeld niet van toepassing op sociale netwerken of commerciële zoekmachines. Bovendien zijn controles van toepassing op systemen die gegevens verwerken die afkomstig zijn van een kernnetwerk van een internetprovider, en niet op sociale netwerken of commerciële zoekmachines die gegevens verwerken welke door gebruikers zijn verstrekt.

— **"Inbraakprogrammatuur" (4A005, 4D004 en daarmee verband houdende controles als bedoeld onder 4E001.a. en 4E001.c.)**

Inbraakprogrammatuur stelt de bediener in staat op afstand heimelijk toegang te verkrijgen tot een elektronisch apparaat, zoals een smartphone, laptop, server of een apparaat voor het internet der dingen, om op het apparaat opgeslagen gegevens te verkrijgen, af te luisteren via een camera of microfoon die in het apparaat is ingebouwd of daarmee is verbonden, en het apparaat te gebruiken als vertrekpunt voor aanvallen op uitrusting waarmee het apparaat is verbonden, of tegen contacten van de gebruiker ("hacking via apparaten van derden"). Hoewel er rechtmatig gebruik ([8]) kan worden gemaakt van inbraakprogrammatuur, zoals door IT-afdelingen gebruikte "programmatuur voor toegang op afstand", kunnen het heimelijke karakter van de surveillance en de omvang van de mogelijk verzamelde informatie een hoog risico meebrengen op schending van het recht op privacy en bescherming van persoonsgegevens, en kunnen deze het recht op vrijheid van meningsuiting ernstig ondermijnen.

([8]) Voor alle duidelijkheid: voor in de lijst opgenomen producten voor cybersurveillance waarop bijlage I bij de verordening inzake tweeërlei gebruik betrekking heeft, is een vergunning nodig voor uitvoer naar derde landen, ongeacht of het gebruik van het product rechtmatig is.

De controle als bedoeld onder 4A005 e.v. omvat zowel programmatuur als systemen, uitrusting, onderdelen en aanverwante technologie die speciaal zijn ontworpen of aangepast voor het maken, besturen en controleren of leveren van "inbraakprogrammatuur", maar is niet van toepassing op "inbraakprogrammatuur" als zodanig zoals in bijlage I bij de verordening gedefinieerd. Deze cyberinstrumenten worden gecontroleerd in het licht van de mogelijke verstoring en schade die zij kunnen veroorzaken als zij met succes worden gebruikt en toegepast, maar de controles zijn niet bedoeld om invloed uit te oefenen op de activiteiten van bijvoorbeeld cyberbeveiligingsonderzoekers en -bedrijven, aangezien zij informatie over inbraakprogrammatuur moeten delen om oplossingen voor problemen met hun producten te kunnen ontwikkelen en deze beschikbaar te hebben voordat een kwetsbaarheid openbaar wordt gemaakt.

— **Programmatuur voor communicatiemonitoring (5D001.e.)**

Deze programmatuur is ontworpen voor monitoring en analyse door bevoegde rechtshandhavingsinstanties van gegevens die zijn verzameld door middel van gerichte interceptiemaatregelen op verzoek van een aanbieder van communicatiediensten. Deze programmatuur maakt zoekopdrachten mogelijk op basis van "hard selectors" met betrekking tot de inhoud van communicatie of metadata, waarbij gebruik wordt gemaakt van een interface voor legale interceptie, en het in kaart brengen van het relationele netwerk of het traceren van de verplaatsingen van specifieke personen op basis van de resultaten van de zoekopdrachten. Deze programmatuur is bedoeld voor "heimelijk surveilleren", omdat zij gebruikmaakt van gegevens die door interceptie van communicatie zijn verkregen, zonder dat personen daarvan kennis dragen. Voorts analyseert deze programmatuur gegevens die via "telecommunicatiesystemen" zijn verzameld. De programmatuur wordt geïnstalleerd met toestemming van de overheid (bijvoorbeeld de monitoringfaciliteit voor rechtshandhaving (LEMF)), en de controle is niet van toepassing op de systemen voor naleving van legale interceptie (LI) (bijvoorbeeld beheersystemen en bemiddelingsapparatuur in verband met LI) die commercieel worden ontwikkeld en geïnstalleerd in het domein van de aanbieder van communicatiediensten (bijvoorbeeld geïntegreerd in het communicatienetwerk) en die de dienstverlener exploiteert en onderhoudt. Zoals in de tekst inzake de controles wordt verduidelijkt, hebben de controles geen betrekking op "programmatuur" die speciaal is ontworpen of aangepast voor zuiver commerciële doeleinden, zoals de kwaliteit van de dienstverlening ("Quality of Service" of "QoS") van factureringsnetwerken, de kwaliteit van de ervaring ("Quality of Experience" of "QoE"), bemiddelingstoestellen of het gebruik van mobiele betaling of mobiel bankieren.

— **Producten voor cryptoanalyse (5A004.a.)**

Deze controle is van toepassing op producten die zijn ontworpen voor het verslaan van cryptoanalytische mechanismen teneinde vertrouwelijke variabelen of gevoelige gegevens te verkrijgen, met inbegrip van niet-gecodeerde tekst, wachtwoorden of cryptografische sleutels. Cryptografie wordt gebruikt om de vertrouwelijkheid van informatie in doorvoer en rust te waarborgen. Cryptoanalyse wordt gebruikt om deze vertrouwelijkheid te verslaan, waardoor deze technologie derhalve "in staat stelt" heimelijk te surveilleren door gegevens uit informatie- en telecommunicatiesystemen te monitoren, te extraheren, te verzamelen of te analyseren.

— **Forensische/onderzoeksinstrumenten (5A004.b., 5D002.a.3.b. en 5D002.c.3.b.)**

Forensische/onderzoeksinstrumenten zijn ontworpen om ruwe gegevens uit een apparaat te extraheren (bijvoorbeeld uit een computer- of communicatieapparaat), zodat de gegevens niet worden gemanipuleerd of beschadigd en kunnen worden gebruikt voor gerechtelijke doeleinden, d.w.z. in het kader van een strafrechtelijk onderzoek of in een gerechtelijke instantie. Deze producten omzeilen controles in het kader van de "authenticatie" of autorisatie van een toestel, zodat de ruwe gegevens uit het apparaat kunnen worden geëxtraheerd. Deze producten worden gebruikt door de overheid en rechtshandhavingsinstanties, alsmede door strijdkrachten om gegevens van in beslag genomen apparaten te extraheren en te analyseren. Hoewel er rechtmatig gebruik van kan worden gemaakt, kunnen zij ook worden misbruikt en dus een risico vormen voor gevoelige of commerciële gegevens.

Forensische/onderzoeksinstrumenten die niet "speciaal ontworpen" zijn voor heimelijke surveillance, vallen echter niet onder de definitie van producten voor cybersurveillance van artikel 2, punt 20). Tevens is het zo dat de tekst inzake de controles in 5A004.b e.v. geen betrekking heeft op forensische/onderzoeksinstrumenten die enkel gebruikersgegevens extraheren of waarbij de gegevens op het apparaat niet beschermd zijn. Tegelijkertijd zijn de controles niet van toepassing met betrekking tot productie- of testuitrusting van de fabrikant, systeembeheerinstrumenten of producten die uitsluitend bestemd zijn voor de commerciële detailhandel, zoals producten voor het ontgrendelen van mobiele telefoons. Gezien de verscheidenheid van deze soorten technologie hangt de toepasselijkheid van controles derhalve af van een beoordeling per geval van elk product.

Tot slot zij erop gewezen dat er in bijlage I bij de verordening andere surveillanceproducten zijn opgenomen die niet moeten worden beschouwd als onder de definitie van producten voor cybersurveillance vallend, zoals uitrusting voor het storen van mobiele telecommunicatie (5A001.f.) die is ontworpen om communicatie of systemen te beschadigen of te verstoren, inbraakprogrammatuur die een systeem wijzigt (4D004), en laserakoestische detectieapparatuur (6A005.g.) die audiogegevens verzamelt met een laser, of die het mogelijk maakt gesprekken op afstand te beluisteren (soms "lasermicrofoon" genoemd). Evenzo zou het gebruik van in de lijst opgenomen UAV's voor surveillancedoeleinden deze producten niet onder de definitie van producten voor cybersurveillance brengen.