Datum
16 december 2024

Onderwerp
Rondetafelgesprek 'aanpak van hybride dreigingen'

Geachte leden van de vaste Kamercommissie voor Defensie,

Bedankt voor uw uitnodiging voor het rondetafelgesprek over hybride dreigingen in Europa, meer in het bijzonder over de aanpak daarvan. In dit *position paper* richt ik me op het fenomeen 'hybride dreiging' dat vaak vooraf aan een militair conflict gaat.[1] Daarbij bespreek ik de bescherming van kwetsbare Nederlandse netwerk- en informatiesystemen uit verschillende sectoren tegen dit type dreigingen dat momenteel een groot gevaar vormt voor niet alleen de nationale maar ook internationale veiligheid. In dit verband besteed ik voornamelijk aandacht aan offensieve cyberoperaties die tegenwoordig niet zelden door verschillende statelijke en niet-statelijke actoren als onderdeel van hybride aanvallen worden uitgevoerd. Te denken valt aan *cyberattacks*, zoals *Distributed Denial of Service* (DDoS)-aanvallen en *ransomware*-infecties behorende tot de grootste cyberdreigingen ter wereld, zoals de LockBit-gijzelsoftware[2] die als 'ransomware-as-a-service' door cybercriminelen wordt aangeboden.

Hybride dreigingen

In de *Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029* die onder coördinatie van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) tot stand is gekomen, worden hybride dreigingen gedefinieerd als 'dreigingen tegen de nationale veiligheid die zich grotendeels manifesteren onder het niveau van een openlijk gewapend conflict'.[3] In de schemerzone tussen oorlog en vrede zetten statelijke (bijv. inlichtingen- en veiligheidsdiensten) en niet-statelijke (bijv. cybercriminelen) actoren bepaalde middelen en technieken in om specifieke strategische doelstellingen te bereiken.[4] Deze technieken en middelen omvatten niet alleen sabotage, spionage en desinformatiecampagnes maar ook cyberaanvallen en kennisdiefstal en kunnen afzonderlijk of in combinatie met elkaar worden ingezet. De Adviesraad Internationale Vraagstukken (AIV) onderscheidt drie dimensies waarbinnen hybride dreigingen materialiseren, namelijk de fysieke, virtueel-informatieve en cognitieve dimensies.[5] Digitale aanvallen die in deze bijdrage centraal staan, kunnen in principe in de praktijk in al deze dimensies plaatsvinden, namelijk op de niveaus van (1) de hardware van netwerk- en informatiesystemen, (2) de verwerking, verspreiding en bescherming van informatie in deze systemen en (3) de daaruit voortvloeiende psychologische effecten die het bewustzijn en gedragspatronen van mensen kunnen veranderen.

In mijn optiek is het van vitaal belang om voor ons democratische land dat een sterk gedigitaliseerde – maar tegelijkertijd open, vrije en pluriforme – samenleving heeft, de aanpak van hybride dreigingen als een essentiële prioriteit aan te merken en deze op een effectieve en efficiënte wijze vorm te geven. Rekening moet worden gehouden met het feit dat de wereldwijde geopolitieke onrust die hybride dreigingen en digitale risico's beïnvloedt, alleen maar toeneemt en dat de

[1] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, AIVD, Ministerie van Defensie & MIVD, *Dreigingsbeeld militaire en hybride dreigingen,* december 2024, p. 3, https://www.nctv.nl/documenten/publicaties/2024/12/06/dreigingsbeeld-hybride-en-militaire-dreigingen.
[2] E. Moyakine, (2024) 'Bits en sloten vanuit een cybersecurityperspectief: Begrijpen en voorkomen van ransomware-aanvallen met LockBit als voorbeeld van gijzelsoftware van de hoogste orde', *Tijdschrift voor Internetrecht* 17(1), p. 15-21.
[3] NCTV, *De Veiligheidsstrategie voor het Koninkrijk der Nederlanden,* rapport, p. 15, https://www.rijksoverheid.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden.
[4] A. Sari & M. Regan, 'Introduction', in M. Regan & A. Sari (red.), (2024) *Hybrid threats and grey zone conflict: The challenge to liberal democracies,* New York: Oxford University Press, p. 13.
[5] AIV, *Hybride dreigingen en maatschappelijke weerbaarheid,* AIV-advies 126, 4 juni 2024, p. 16-17, https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid.

digitale dreiging tegen Nederland en andere EU-landen uiterst complex en significant is. Elke organisatie, hoe klein of groot ook, en ieder individu kan (en op een gegeven moment waarschijnlijk zal) doelwit worden van kwaadwillende actoren die vanuit het digitale domein opereren. Absolute cyberveiligheid bestaat namelijk niet en kan nooit worden gegarandeerd en het is niet uit te sluiten dat de hoge mate van afhankelijkheid van ons land van digitale technologie in de toekomst in grote schade zal resulteren tenzij men tijdig adequate maatregelen treft en ze voortdurend aan nieuwe dreigingen aanpast.

Gebrek aan cybersecurityprofessionals

Ik ben van mening dat de cyberweerbaarheid van Nederland momenteel verre van optimaal is en bepaalde zwakheden vertoont; toch kunnen enkele oorzaken van deze verzwakte weerbaarheid tegen cyberdreigingen worden vastgesteld. Voor de onderwijs- en onderzoeksector heeft SURF in het *Cyberdreigingsbeeld 2014-2024* een drietal factoren genoemd dat onze weerbaarheid aanzienlijk vermindert.[6] Deze bevindingen zijn ook relevant voor andere sectoren en moeten in aanmerking worden genomen bij het bepalen van de strategie, aanpak en prioriteiten in het kader van het voorkomen en afweren van steeds toenemende cyberdreigingen. Ten eerste is er sprake van een groeiend tekort aan cybersecurity-experts. In de Kamerbrief van de toenmalige demissionair Minister van Economische Zaken en Klimaat (EZK) Micky Adriaansens werd er ingegaan op de krapte op de Nederlandse cybersecurity-arbeidsmarkt en aangegeven dat een adequate beschikbaarheid van goedgeschoolde professionals op het gebied van cybersecurity cruciaal is voor het waarborgen van de digitale weerbaarheid van ons land.[7] Hoewel de vraag naar deze experts in de toekomst alleen maar zal toenemen, is uit het in opdracht van de Minister uitgevoerde onderzoek gebleken dat het niet helder is wat de term 'cybersecurity-expertise' (die in verschillende opleidingen wordt gebruikt) inhoudt en er enkel een beperkte afstemming tussen die opleidingen is. Zoals terecht opgemerkt door de Cyber Security Raad (CSR) in zijn signaalbrief, is het noodzakelijk dat niet alleen het Ministerie van EZK maar ook andere ministeries zoals de Ministeries van Onderwijs, Cultuur en Wetenschap en Justitie en Veiligheid gezamenlijk in actie komen met als doel 'publiek-privaat-wetenschappelijke samenwerking' te realiseren.[8]

Sterke ketenafhankelijkheid

Ten tweede zijn talloze organisaties volgens SURF erg afhankelijk van producten en diensten van toeleveranciers of leveren ze zelf bepaalde producten of diensten. Deze ketenafhankelijkheid kan bij digitale aanvallen ernstige gevolgen hebben voor alle organisaties in de keten oftewel *the supply chain*. Een cyberaanval bij één toeleverancier leidt vaak tot aanzienlijke gevolgen voor alle organisaties in de keten. Het is daarom van wezenlijk belang om regelmatig een keteninventarisatie uit te voeren en ketenrisico's te analyseren en te beheersen. Een opmerkelijke stap voorwaarts is de aandacht van de EU-wetgever voor maatregelen die door organisaties uit de vitale infrastructuur getroffen moeten worden met als doel toeleveringsketens veiliger te maken. Deze verplichting die in de relevante EU-wetgeving is neergelegd, zal later in dit position paper in het kort worden besproken.

De mens als schakel

Als laatste verwijst SURF naar de menselijke factor die ook een bijzonder grote rol speelt bij de beveiliging van netwerk- en informatiesystemen. Het huidige cyberbewustzijn van zowel Nederlandse als Europese burgers en bedrijven laat nog helaas te wensen over, wat een open uitnodiging voor kwaadwillenden is om direct toe te slaan. Het onderzoek van Eurostat heeft aangetoond dat

[6] SURF, *Cyberdreigingsbeeld 2014-2024: Onderwijs en onderzoek*, rapport, speciale editie, oktober 2024, p. 20, https://www.surf.nl/nieuws/lessen-en-actiepunten-na-tien-jaar-cyberdreigingen-in-onderwijs-en-onderzoek.
[7] Aanbiedingsbrief van de Minister van Economische Zaken en Klimaat van 15 mei 2024, p. 1-2, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/05/15/kamerbrief-human-capital-cybersecurity.
[8] CSR, *Signaalbrief in reactie op de Kamerbrief van de minister van EZK over de cybersecuritymarkt*, 4 juli 2024, p. 1, https://www.cybersecurityraad.nl/actueel/nieuws/2024/07/04/csr-signaalbrief-cybersecurity-arbeidsmarkt.

bijna 83% van alle Nederlanders tussen 16 en 74 jaar in 2023 over digitale basisvaardigheden beschikte.[9] Het is dus niet verwonderlijk dat Nederland kooploper van de Europese Unie op dit gebied is (gevolgd door Finland en Ierland). Ons land heeft nu al een belangrijke doelstelling van het Europese beleidsprogramma voor het digitale decennium voor 2030 bereikt: minimaal 80% van de bevolking moet namelijk in 2023 digitale basisvaardigheden bezitten. Blijdschap is gepast maar de noodzaak om aan de vaardigheden van Nederlanders te werken blijft groot. De mens is vaak de zwakste schakel in de cybersecurityketen maar we moeten er juist voor zorgen dat onze burgers die het primaire doelwit van cyber- en hybride dreigingen zijn,[10] in plaats van de kern van het probleem onderdeel van de oplossing worden. Elke medewerker van een publieke of private organisatie die in Nederland gevestigd is, dient zich te realiseren dat hij juist de eerste verdedigingslinie van zijn organisatie vormt en de signalen van cyberdreigingen moet kunnen herkennen om daar adequaat op te reageren. Awarenesscampagnes en -trainingen zijn onontbeerlijk om mensen te informeren en bewustwording over online veiligheid te vergroten.

Vooruitgang in technologie

Daarnaast is het essentieel te beseffen dat veel bedrijven, andere organisaties en processen binnen die organisaties digitaal met elkaar verbonden zijn en dat technologische ontwikkelingen een aanzienlijke invloed op de digitale component van hybride dreigingen hebben. Te denken valt aan onder andere het toegenomen gebruik van *Internet of Things*- oftewel IoT-apparaten, *quantum computing* en artificiële intelligentie (AI). Hieronder wil ik vooral stilstaan bij de laatstgenoemde ontwikkeling. Tegenwoordig fungeert AI als hulpmiddel voor kwaadwillenden en wordt gebruikt om geavanceerde aanvalstechnieken te ontwikkelen en te verfijnen. Het transformerende potentieel van kunstmatige intelligentie moet echter ook worden benut om ons tegen digitale dreigingen te beschermen. In zijn eerste grote speech als secretaris-generaal van de NAVO heeft Mark Rutte op 12 december 2024 aangegeven dat er vijandige landen zijn die enorm investeren in de ontwrichtende technologieën waaronder AI, kwantumtechnologie en ruimtevaart.[11] Hij heeft in zijn antwoord op de vraag van Rosa Balfour, directeur van Carnegie Europe, erop gewezen dat de NAVO-landen ook de nieuwste technologie nodig hebben, inclusief datgene wat we kunnen leren van AI en kwantumtechnologie, om zich effectief te kunnen verdedigen tegen een breed spectrum aan dreigingen.

Wat de nieuwste technologieën betreft, zijn onze inspanningen als onderzoekers aan de Rijksuniversiteit Groningen erop gericht om innovatieve AI-toepassingen voor het verbeteren van de cyberweerbaarheid te ontwerpen. Mijn collega's van de sectie IT-recht en ik werken nauw samen met interne en externe technisch experts aan onderzoeksvoorstellen en -projecten om de veiligheid van netwerk- en informatiesystemen van publieke en private organisaties met behulp van nieuwe technologieën zoals generatieve AI (GenAI) conform de geldende wet- en regelgeving te waarborgen. In het onderwijs dat op onze faculteiten wordt verzorgd, delen wetenschappers hun inzichten met betrekking tot onder andere de inzet van offensieve en defensieve AI en beveiligingsmaatregelen met studenten die tot IT-juristen en cybersecurity-experts worden opgeleid, en wordt gezamenlijk nagedacht over innovatieve oplossingen voor de uitdagingen van digitale dreigingen om de cyberveiligheid van Nederland naar een hoger niveau te tillen. De CSR stelt dat het aantal docenten moet worden verhoogd en dat daar voldoende financiële middelen voor

[9] Eurostat, '56% of EU people have basic digital skills', 15 december 2023, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20231215-3; Eurostat, 'Individuals' level of digital skills (from 2021 onwards)', laatste update: 16 juni 2024, https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/bookmark/table?lang=en&bookmarkId=8154ff68-4fdd-4681-ac60-0197cb3d06af&page=time:2023.

[10] V. Shalamanov & B. Bankov, 'NATO Cyber Defence Policy and hybrid threats: The way to enhance our resilience', in M. Bogdanoski (red.), (2022) *Building cyber resilience against hybrid threats,* NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 61, Amsterdam: IOS Press, p. 1.

[11] NATO, 'To prevent war, NATO must spend more': Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels', 12 december 2024, laatste update: 13 december 2024, https://www.nato.int/cps/en/natohq/opinions_231348.htm.

beschikbaar gemaakt moeten worden.[12] Daarnaast wordt er door mij gepleit voor nauwe samenwerking met onderwijsinstellingen van verschillende niveaus binnen en buiten de EU die onmisbaar is voor het uitwisselen van kennis en expertise en het toepassen daarvan in de praktijk. Persoonlijk zie ik een dringende noodzaak om meer interdisciplinair en transdisciplinair wetenschappelijk onderzoek op het vlak van cybersecurity uit te voeren en meer studenten te inspireren en op te leiden in dit cruciale vakgebied om ervoor te zorgen dat onze maatschappij beter voorbereid is op haar toekomst vol onzekerheden, veranderingen en nieuwe uitdagingen. De huidige bezuinigingsplannen van het kabinet staan echter haaks op deze noodzaak en zullen helaas de kwaliteit van ons onderzoek en onderwijs in gevaar brengen.

Cyberattributie

Vervolgens wil ik in mijn position paper de eerdergenoemde complexiteit van hybride dreigingen in de vorm van cyberaanvallen aansnijden en de uitdagingen rondom het attribueren daarvan onder de aandacht brengen. Fysieke aanvallen zijn vaak duidelijk waarneembaar en kunnen in de meeste gevallen moeiteloos worden gedetecteerd. In contrast daarmee zijn digitale aanvallen minder zichtbaar of de effecten daarvan kunnen zich pas in een later stadium openbaren. Ze kunnen niet altijd worden gekoppeld aan personen en/of entiteiten die ze uitvoeren en er zijn beperkte mogelijkheden voor de toerekening van deze aanvallen aan staten die erbij betrokken kunnen zijn. Hybride dreigingen gaan vaak gepaard met dit attributieprobleem.[13] Het jaarlijks gepubliceerde rapport van de NCTV *Cybersecuritybeeld Nederland 2022* wijst er terecht op dat cyberaanvallen door statelijke actoren niet meer zeldzaam zijn en 'het nieuwe normaal' zijn geworden.[14] Attributie van offensieve cyberoperaties die het internationaal recht (bijv. het VN-Handvest of het internationaal humanitair recht vastgelegd in onder andere de Geneefse Conventies) schenden, is cruciaal om vast te stellen welke rechtsgevolgen de schendingen in kwestie met zich meebrengen en of de aangevallen staten daarop kunnen reageren door staatsaansprakelijkheid in te roepen, tegenmaatregelen te nemen en een beroep op het recht op zelfverdediging van artikel 51 VN-Handvest tegen een mogelijke gewapende aanval te doen. Derhalve vormt cyberattributie een essentieel aandachtsgebied dat, naar mijn inzicht, meer (wetenschappelijke) verdieping vereist en verder op het nationale en internationale niveau moet worden uitgewerkt.

Als zodanig is attributie of toerekening een proces dat uit meerdere lagen bestaat en een drietal specifieke dimensies omvat.[15] Technische attributie richt zich op het identificeren van de daders achter bepaalde cyberoperaties waarbij gebruik wordt gemaakt van technisch/forensisch onderzoek. Daarnaast is politieke of publieke attributie ervoor bedoeld om de bovengenoemde operaties aan de betrokken kwaadwillende staten en/of entiteiten op het politieke niveau te koppelen. Denkt u aan de recente onthullingen van de MIVD met betrekking tot de digitale spionageactiviteiten van China.[16] Nederland is een grote voorstander van effectieve politieke attributie en in de *Defensie Cyber Strategie 2018* staat het volgende expliciet vermeld: 'Een actief politiek attributiebeleid draagt bij aan het afschrikkend vermogen en het minder aantrekkelijk maken van Nederland als doelwit van cyberaanvallen… Zo draagt Nederland bij aan het tegengaan van straffeloosheid in het digitale domein.'[17] Bij deze vorm van toerekening moet er onder andere worden

[12] CSR, *Signaalbrief in reactie op de Kamerbrief van de minister van EZK over de cybersecuritymarkt*, 4 juli 2024, p. 2, https://www.cybersecurityraad.nl/actueel/nieuws/2024/07/04/csr-signaalbrief-cybersecurity-arbeidsmarkt.
[13] N. Downes & L. Maglaras, 'From rules to retribution: The problem of attribution and regulation in the age of cyberwarfare', in M. A. Ferrag, I. Kantzavelou, L. Maglaras & H. Janicke (red.), (2024) *Hybrid threats, cyberterrorism and cyberwarfare,* Boca Raton: CRC Press, p. 41; J. Wiseman, 'EU-NATO hybrid warfare', in M. Bogdanoski (red.), (2022) *Building cyber resilience against hybrid threats,* NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 61, Amsterdam: IOS Press, p. 19.
[14] NCTV, *Cybersecuritybeeld Nederland 2022,* rapport, 4 juli 2022, p. 7, 14, 16, https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022.
[15] Nicholas Tsagourias, (2012) 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict and Security Law* 17(2), p. 233.
[16] Rijksoverheid, 'MIVD onthult werkwijze Chinese spionage in Nederland', 6 februari 2024, https://www.rijksoverheid.nl/actueel/nieuws/2024/02/06/mivd-onthult-werkwijze-chinese-spionage-in-nederland.
[17] Ministerie van Defensie, *Defensie Cyber Strategie 2018: Investeren in digitale slagkracht voor Nederland,* 12 november 2018, p. 7, https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018.

voorkomen dat er te veel informatie wordt vrijgegeven over de specifieke aanvalstechnieken en -middelen van je tegenstanders die door anderen kunnen worden gebruikt, en worden staten niet verantwoordelijk gehouden voor mogelijke schendingen van het internationaal recht. Staten die deze schendingen als internationale onrechtmatige daden begaan, zijn alleen internationaalrechtelijk aansprakelijk mits juridische attributie mogelijk is. Dit laatste type attributie is natuurlijk sterk afhankelijk van de uitkomst van technische attributie en is nauw verbonden met politieke attributie. Het is echter ook één van de meest uitdagende en complexe thema's dat ik in mijn onderzoek probeer te doorgronden.

In het *Cybersecuritybeeld Nederland 2024* wordt er gesteld dat niet alleen criminelen maar ook statelijke actoren de grootste cyberdreiging tegen ons land vormen.[18] Er zijn landen die offensieve cyberprogramma's hebben en hun activiteiten in het digitale domein intensiveren; steeds vaker worden niet-statelijke actoren, zoals 'hacktivisten', ingezet bij het uitvoeren van offensieve cyberoperaties die door staten worden gesponsord. Ik ben van mening dat het internationaal recht dat op zowel cyberspace als cyberdreigingen van toepassing is, verder dient te worden ontwikkeld. Meer duidelijkheid moet worden verschaft over de vraag of en in hoeverre offensieve cyberoperaties die door niet-statelijke actoren met de betrokkenheid van staten als hybride aanvallen worden uitgevoerd, aan die staten toegerekend kunnen worden. Één van de meest relevante gronden voor deze toerekening vindt men in artikel 8 van de zogenoemde 'Articles on the Responsibility of States for Internationally Wrongful Acts' (ARSIWA) oftewel de artikelen inzake de aansprakelijkheid van staten voor internationale onrechtmatige daden van *the International Law Commission* of de Commissie voor het Internationaal Recht van de Verenigde Naties.[19] Deze bepaling geldt indien individuen of groepen van individuen onder instructies, leiding of controle van staten handelen. Het komt niet vaak voor dat er voldoende bewijs is voor duidelijke en specifieke instructies en leiding van staten; wat kwaadwillende staten echter wel regelmatig doen, is het uitoefenen van controle over personen en entiteiten die in het cyberdomein actief zijn en tot cyberaanvallen overgaan. De vraag rijst wat de mate van controle is die door een vijandige staat moet worden uitgeoefend, om offensieve cyberoperaties aan die staat volgens de criteria van artikel 8 ARSIWA toe te rekenen. Naast de door het Internationaal Gerechtshof (IGH) in 1986 geformuleerde theorie van effectieve controle[20] zijn er controletests die door anderen zijn ontwikkeld,[21] maar is het noodzakelijk om gezien de huidige technologische ontwikkelingen een nieuwe controletheorie te formuleren en, zo ja, hoe moet die luiden? Onder welke omstandigheden kunnen cyber- en hybride dreigingen als geweldgebruik in strijd met artikel 2 lid 4 van het VN-Handvest worden beschouwd? Zijn deze dreigingen ook aan te merken als gewapende aanvallen waartegen het recht op zelfverdediging kan worden uitgeoefend, en onder welke voorwaarden zijn ze als zodanig te kwalificeren?

Bescherming van de kritieke infrastructuur

De vitale infrastructuur van Nederland is een gewild doelwit voor kwaadwillenden. De uitval of verstoring van deze vitale processen en diensten, zoals drinkwatervoorziening, productie van elektriciteit en Internettoegang, kan tot grote maatschappelijke en economische gevolgen leiden en onze nationale veiligheid bedreigen maar de digitale beveiliging van deze infrastructuur is niet altijd optimaal. Het is toch enigszins geruststellend dat een breed scala aan wet- en regelgeving

[18] NCTV, *Cybersecuritybeeld Nederland 2024,* rapport, 28 oktober 2024, p. 6, https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024.
[19] International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts*, Yearbook of the International Law Commission, 2001, vol. II(2), UN Doc. A/56/10, https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf.
[20] IGH 27 juni 1986, *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua/United States of America),* r.o. 115.
[21] Joegoslaviëtribunaal 15 juli 1999, *Prosecutor v. Tadić*, r.o. 137; C. Allan, (2013) 'Attribution issues in cyberspace', *Chicago-Kent Journal of International and Comparative Law* 13(2), p. 81; N. Tsagourias & M. Farrell, (2020) 'Cyber attribution: technical and legal approaches and challenges', *European Journal of International Law* 31(3), p. 965; E. Moyakine (2023), 'Pulling the strings in cyberspace: Legal attribution of cyber operations based on state control', in F. Delerue, A. Sukumar & D. Broeders (red.), *Responsible behaviour in cyberspace: Global narratives and practice*, Luxembourg: Publications Office of the European Union, p. 200-218.

voor het tegengaan van digitale dreigingen al bestaat of in de maak is. Deze loopt helaas soms achter op de relevante technologische ontwikkelingen en dient voortdurend te worden aangepast om effectief te blijven en dynamisch te kunnen inspelen op de realiteit van deze dreigingen en nieuwe technologische trends. Daarbij is het beschermen van onze vitale infrastructuur tegen fysieke dreigingen, zoals natuurrampen en terroristische aanvallen, onontbeerlijk. Als voorbeeld kunt u denken aan de EU-brede wetgeving, namelijk de *Critical Entities Resilience* (CER)-richtlijn en de *Network and Information systems Security 2* (NIS2)-richtlijn, de opvolger van de eerste inmiddels verouderde NIS-richtlijn die minder sectoren omvatte en minder strenge beveiligingseisen aan netwerk- en informatiesystemen stelde. In Nederland zijn deze richtlijnen geïmplementeerd in respectievelijk de Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (Cbw) die op 2 december aan de Afdeling advisering van de Raad van State ter advies zijn voorgelegd.[22] De verwachting is dat ze in het derde kwartaal van 2025 in werking zullen treden. Helaas heeft maar een klein aantal EU-landen de twee bovengenoemde richtlijnen tot nu toe volledig geïmplementeerd en de Europese Commissie is inbreukprocedures begonnen tegen meer dan 20 lidstaten, waaronder Nederland, die dat nog niet hebben gedaan.[23]

Wat de Cbw betreft, is het niet altijd even helder of bepaalde organisaties onder de reikwijdte van de nieuwe wet vallen en aan de daarin opgenomen verplichtingen moeten voldoen. Zo kunnen onderwijsinstellingen op grond van artikelen 11 en 13 als essentiële of belangrijke entiteiten worden aangewezen bij regeling of besluit van de Minister van Onderwijs, Cultuur en Wetenschap na overleg met de Minister van Justitie en Veiligheid. Deze lagere regelgeving is, voor zover ik weet, nog niet tot stand gekomen en onderwijsinstellingen verkeren in onzekerheid over de inhoud daarvan. Bovendien valt het nog te bezien of aanbieders van openbare elektronische communicatienetwerken en -diensten die als kleine of micro-ondernemingen zijn aan te merken, zich aan de vergaande verplichtingen uit de Cbw zullen kunnen houden en niet zullen worden gedwongen om met hun activiteiten in de telecomsector te stoppen.[24] Volgens artikel 12 lid 1 onderdelen c en d van het wetsvoorstel behoren ze namelijk nu tot de categorie 'belangrijke entiteit van rechtswege'. Verder bepaalt artikel 21 lid 3 onderdeel d van de voorgestelde wet dat de beveiliging van de toeleveringsketen, waar in het bovenstaande naar verwezen is, door essentiële en belangrijke entiteiten dient te worden gewaarborgd. In de praktijk betekent dit dat de cyberveiligheid van toeleveringsketens in kaart moet worden gebracht en dat rechtstreekse leveranciers of dienstverleners van de entiteiten indirect door de nieuwe wet zullen worden geraakt: het moet nog blijken aan welke eisen toeleveranciers van organisaties uit verschillende sectoren uiteindelijk zullen moeten voldoen en of die bedrijven niet zullen verdrinken in een wirwar van verschillende raamwerken en formulieren. Ook al zijn er veel vragen en onduidelijkheden, kunnen bedrijven en andere organisaties die onder de reikwijdte van de twee bovengenoemde wetten vallen, nu alvast beginnen met het nemen van maatregelen om zich te beschermen tegen fysieke en digitale dreigingen en hoeven ze niet te wachten totdat de wetgeving in kwestie eindelijk in werking is getreden.

Conclusie

In zijn advies pleit de AIV voor zowel de *whole-of-government*- als *whole-of-society*-benadering waarbij de overheid en de Nederlandse samenleving volledig worden betrokken bij het bestrijden van hybride dreigingen.[25] Daar sta ik natuurlijk volledig achter en benadruk het belang van deze aanpak in mijn onderwijs- en onderzoeksactiviteiten want 'publiek, privaat en wetenschap hebben

[22] NCTV, 'Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten: uitkomsten consultatie verwerkt', 12 december 2024, https://www.nctv.nl/actueel/nieuws/2024/12/12/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-uitkomsten-consultatie-verwerkt.
[23] Europese Commissie, 'Commission takes action to ensure complete and timely transposition of EU directives', 28 november 2024, https://ec.europa.eu/commission/presscorner/detail/en/inf_24_5988.
[24] Andreas Gruber & Natalie Ségur-Cabanac, (2021) 'Necessary or premature? The NIS 2 Directive from the perspective of the telecommunications sector', *International Cybersecurity Law Review* 2, p. 238.
[25] AIV, *Hybride dreigingen en maatschappelijke weerbaarheid,* AIV-advies 126, 4 juni 2024, p. 7-10, 46, https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid.

elkaar nodig om tot oplossingen te komen'[26]. Tevens is intensieve internationale samenwerking met gelijkgestemde landen binnen de EU en de NAVO, als ook tussen de EU en de NAVO, zeer wenselijk. Het spreekt voor zich dat cybersecurity niet als einddoel kan worden beschouwd maar is en blijft een continu proces. Door gezamenlijk als Nederland en de EU tegen cyberdreigingen op te treden en ze effectief aan te pakken, kunnen hybride dreigingen als fenomeen minder impactvol en beter beheersbaar worden.

Zijn we nu eindelijk bereid om de benodigde stappen te zetten en te blijven zetten voordat het te laat is? Zo ja, laten we dan het tijdloze Latijnse adagium niet vergeten: *'Si vis pacem, para bellum'*... als je vrede wilt, bereid je dan voor op oorlog.

Hoogachtend,

Evgeni Moyakine

[26] CSR, *Integrale aanpak cyberweerbaarheid: Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren,* adviesrapport, 6 april 2021, p. 11, 20, https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid.